BAB III

ANALISIS KEBUTUHAN DAN PERANCANGAN

3.1 Analisis Kebutuhan

Analisis kebutuhan yang digunakan dalam sistem yang dibangun yaitu analisis kebutuhan masukan *(input),* kebutuhan keluaran *(output),* dan kebutuhan proses.

3.1.1 Analisis Kebutuhan Masukan (*input)* sistem

Kebutuhan masukan *(input)* yang digunakan dalam mengimplementasikan algoritma Rijndael dalam steganografi citra digital menggunakan metode *Least Significant Bit* adalah sebagai berikut :

a. Pesan atau *file* yang akan dienkripsi berupa *file* teks (.txt) yang telah dibuat secara manual.
b. Kunci yang digunakan untuk enkripsi dan dekripsi *file* pesan rahasia.
c. *File* chiperteks berupa *file* chiperteks dengan ekstensi .enc yang disisipkan ke dalam gambar.
d. Media yang digunakan dalam penyisipan adalah citra gambar bitmap (.bmp) dengan dua jenis yaitu bertipe RGB dan grayscale untuk dilakukan pengujian hasil stegoimagenya.
e. *File* stegoimage yang berisi pesan rahasia yang digunakan untuk ekstraksi pesan rahasia di dalamnya.

3.1.2 Analisis Kebutuhan Keluaran *(output)*

Kebutuhan keluaran yang ada dalam sistem yang dibangun adalah sebagai berikut :

a. Kunci enkripsi yang disimpan dalam format *file* teks (.txt).
b. *File* chiperteks (.enc) yang dihasilkan dari proses enkripsi *file* plainteks atau pesan asli.

c. *File* gambar bertipe bitmap (.bmp) yang dihasilkan dari proses penyisipan pesan rahasia.
d. Pesan asli atau plainteks berformat .txt yang dihasilkan dari proses dekripsi pesan yang ada di dalam gambar yang sebelumnya sudah diestrak.

3.1.3 Analisis Kebutuhan Proses

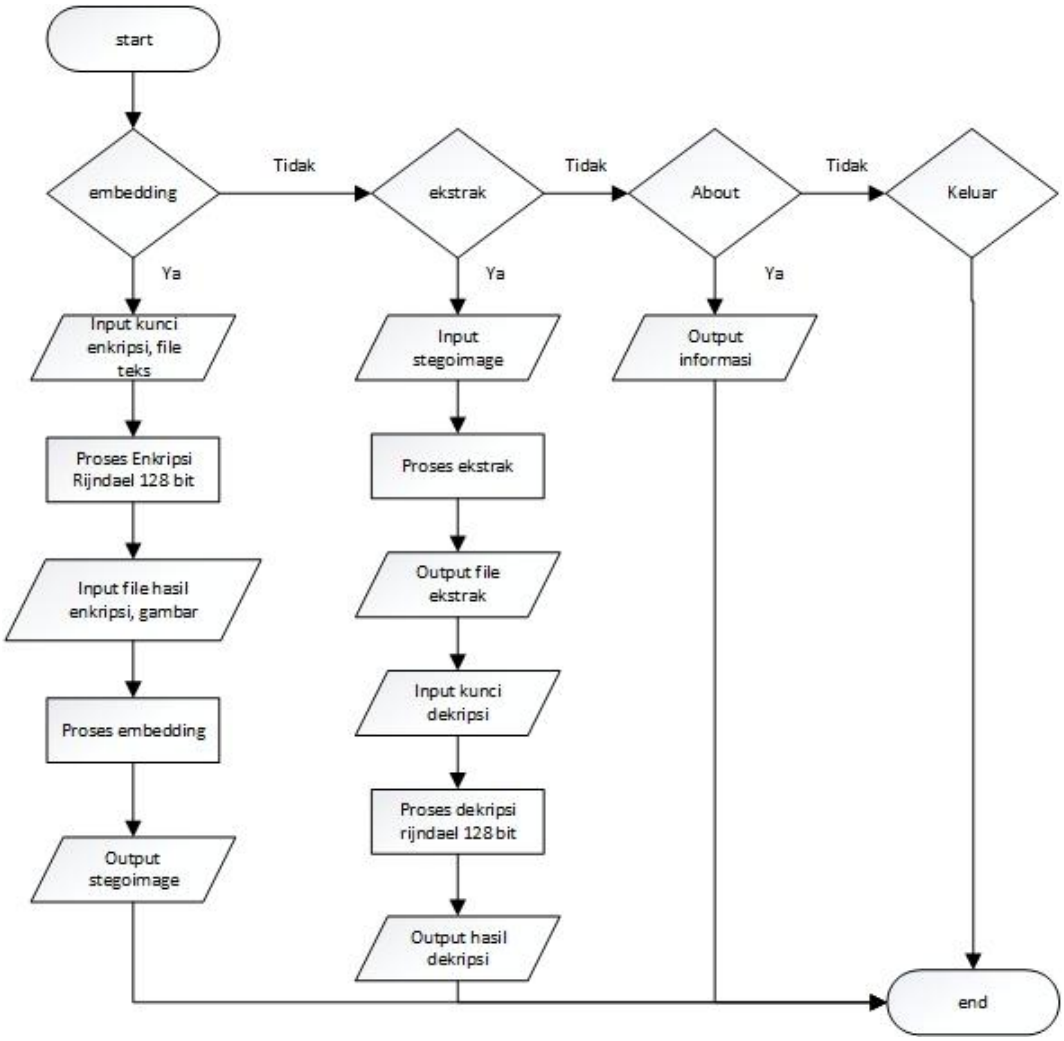
Kebutuhan proses yang ada dalam sistem yang akan dibangun adalah sebagai berikut :

a. Proses enkripsi pesan dengan memasukkan kunci enkripsi oleh pengguna kemudian memilih *file* pesan rahasia yang kemudian dilakukan enkripsi pesan tersebut.
b. Proses penyisipan pesan yang dilakukan dengan memilih pesan yang terenkripsi dan memilih gambar yang akan dijadikan media penyisipan pesan kemudian dilakukan proses penyisipan dari pesan terenkripsi ke dalam gambar.
c. Proses ekstraksi pesan yaitu dengan memilih gambar yang berisi pesan tersembunyi di dalamnya kemudian diekstrak isi pesan yang terdapat di dalamnya hingga dimukan pesan yang dienkripsi dan belum bisa terbaca.
d. Proses dekripsi pesan dengan menggunakan *file* kunci yang sama seperti yang digunakan mendekripsi pesan yang sebelumnya sudah diekstrak dari sebuah gambar agar pesan tersebut dapat dibaca oleh penerima.

3.2 Perancangan Diagram alir *(Flowchart)*

Perancangan diagram alir ini merupakan salah satu yang akan dibutuhkan dalam pembuatan sebuah sistem. Diagram alir atau juga disebut *flowchart* ini menjelaskan bagaimana alur jalannya sebuah program yang digambarkan oleh bagan – bagan yang memiliki ketentuan berbeda misal bagan *input/output*, bagan proses dan sebagainya. Bagan – bagan tersebut dihubungkan oleh garis panah yang menandakan urutan dari jalannya sebuah sistem.

3.2.1 *Flowchart* utama sistem



Gambar 3.1 *Flowchart* utama sistem

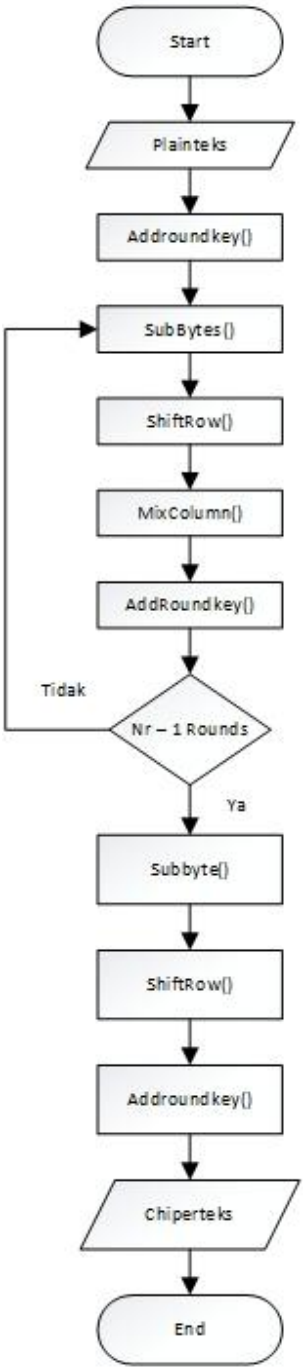
Flowchart utama sistem di sini menggambarkan alur dari sistem aplikasi yang akan dibangun. *Flowchart* menjelaskan tahapan dari berjalanya sistem secara runtut dari *input, output,* proses dan sebagainya. Di bawah ini adalah *flowchart* dari aplikasi stegorijndael yang akan dibangun. Tersedia empat buah menu yaitu embedding, ekstrak, about dan keluar. Apabila memilih embedding maka alurnya adalah menginput kunci dan file pesan rahasia kemudian kedua input tersebut dienkripsi oleh rijndael 128 bit. Untuk menyisipkan pesan maka dibutuhkan input file chiperteks dan media cover nya kemudian akan dilakukan

proses embbeding dari kedua file yang diinputkan tadi. Output yang dikeluarkan berupa gambar stegoimage.

Apabila memilih menu ekstrak maka alurnya adalah Input stegoimage kemudian dilakukan proses ekstraksi pesan. Sebelum dilakukan proses dekripsi Rijndael maka dibutuhkan input yaitu sebuah kunci. Maka hasil output yang dikeluarkan adalah hasil dekripsi. Menu about akan menunjukkan output berupa informasi penggunaan aplikasi. Keluar untuk menutup aplikasi.

3.2.2 *Flowchart* Enkripsi Algoritma Rijndael

Flowchart pada gambar 3.2 adalah *flowchart* yang menggambarkan alur dari tahap – tahap proses enkripsi mengubah plainteks menjadi chiperteks dari algoritma Rijndael secara urut. Pertama plainteks dan key akan diubah ke blok – blok kemudian akan dilakukan proses add roundkey untuk yang pertama, kemudian dilakukan proses subbytes, shiftrow, mix column dan add round key sebanyak putaran pada jenis Rijndael yan digunakan. Disini menggunakan 128 bit sehingga banyak putaran yang digunakan adalah 10 putaran. Untuk tahap putaran terakhir melakukan proses - proses seperti sebelumnya namun tanpa melewati proses mix column hanya subbytes, shiftrow, dan addroundkey kemudian akan dihasilkan chiperteks.



Gambar 3.2 *Flowchart* enkripsi algoritma rijndael

3.2.3 Flowchart proses embedding metode Least Significant Bit

Flowchart ini adalah gambaran dari alur proses penyisipan pesan dengan metode LSB *(Least Significant Bit).* Pertama dengan menginisialisasi gambar yang diambil terlebih dahulu, gambar tersebut diubah dengan cara mengubah piksel gambar menjadi heksadesimal kemudian diubah lagi menjadi biner. Setelah itu bit – bit yan ada pada chiperteks disisipkan ke dalam bit – bit gambar. Ubah kembali bit – bit gambar menjadi heksadesimal dan menghasilkan sebuah gambar yang disebut *stegoimage. Flowchart* proses *embedding* ditunjukkan pada gambar 3.3.

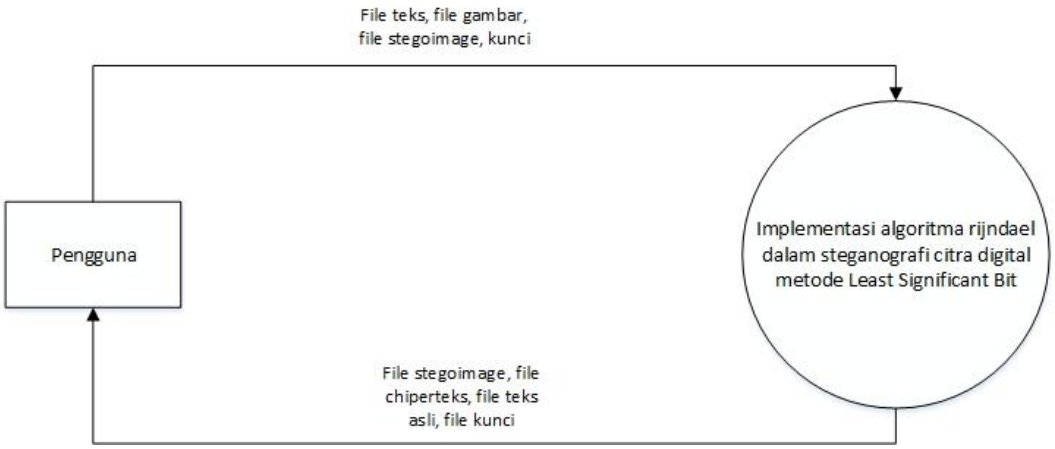
Gambar 3.3 *Flowchart* proses *embedding* metode *Least Significant Bit*

3.3 Perancangan DFD (Data Flow Diagram)

Perancangan DFD (*Data Flow Diagram)* dibutuhkan dalam perancangan sebuah sistem. Diagram tersebut menjelaskan tentang bagaimana aliran data masukan (*input*) dan data keluaran (*output*) yang terdapat dalam suatu sistem. DFD terdiri dari beberapa level yaitu level 0, level 1, dan level 2 sesuai dengan yang diperlukan.

3.3.1 DFD Level 0

DFD Level 0 dari sistem yang akan digunakan dalam penelitian implementasi algoritma rijndael dalam steganografi citra digital dengan metode LSB ini dijelaskan pada gambar 3.4. Sistem ini hanya memiliki satu jenis pengguna. Data yang menjadi masukan (*input*) yaitu *file* yang akan disisipkan berupa file .txt, kemudian yang akan menjadi media penyisipan berupa gambar berformat bitmap .bmp. Kunci enkripsi digunakan untuk keperluan enkripsi dan dekripsi. Stegoimage untuk keperluan proses ekstrak. Data yang menjadi keluaran yaitu *stegoimage*, *file* chiperteks, *file* kunci, *file* teks asli.



Gambar 3.4 DFD Level 0

3.3.2 DFD Level 1

DFD level 1 menguraikan DFD level 0 menjadi beberapa bagian lebih rinci dengan membagi menjadi beberapa proses. Sistem yang akan dibangun memiliki empat proses yaitu proses enkripsi, proses dekripsi, proses penyisipan, dan proses ekstraksi. Setiap proses memiliki penyimpanan, data masukan dan data keluaran sebagai berikut :

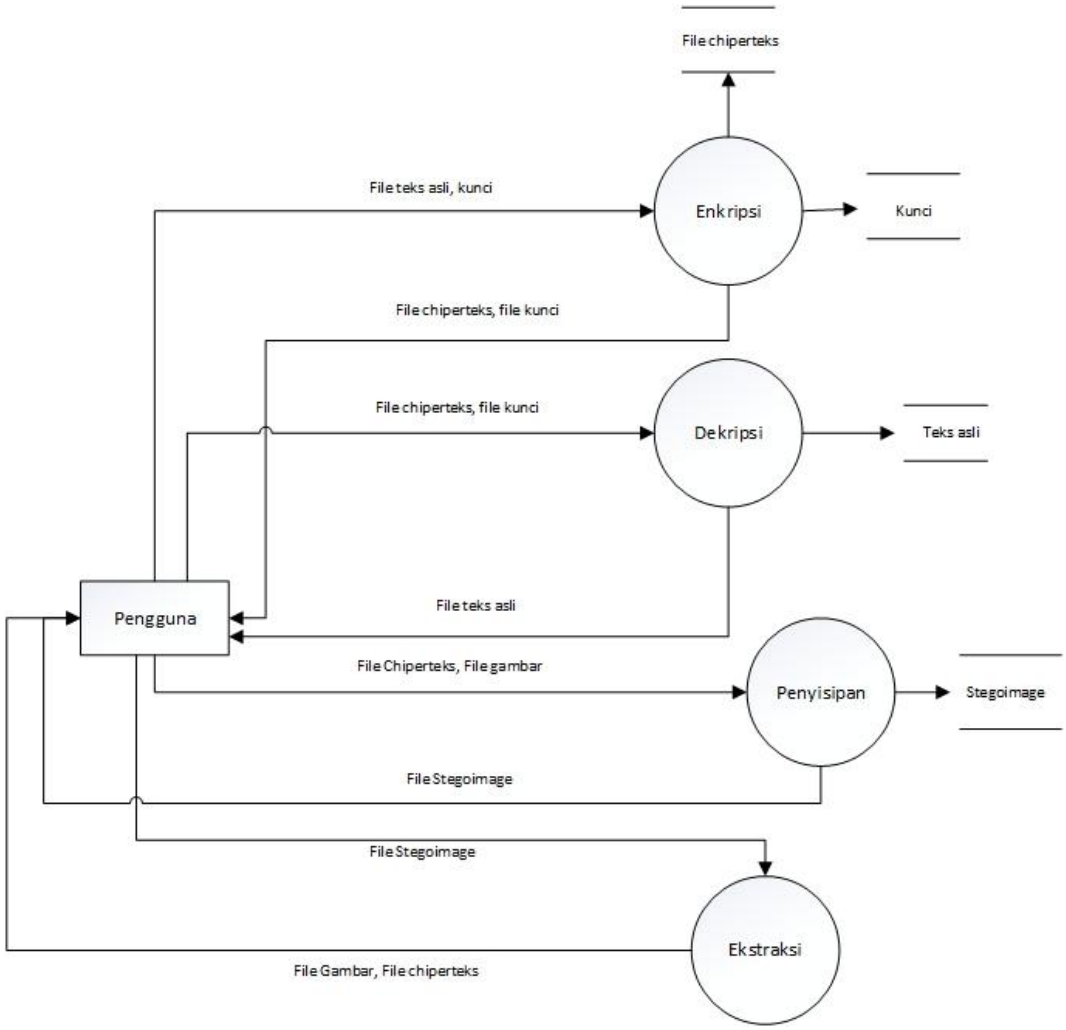
a. Proses enkripsi
   - Data masukan : File plainteks dan kunci.
   - Data keluaran : File chiperteks.
   - Penyimpanan : Kunci dan file chiperteks.

b. Proses dekripsi
   - Data masukan : File chiperteks, file kunci.
   - Data keluaran : File plainteks.
   - Penyimpanan : File teks asli.

c. Proses penyisipan
   - Data masukan : File chiperteks, file gambar.
   - Data keluaran : Stegoimage.
   - Penyimpanan : Stegoimage

d. Proses Ekstraksi
   - Data masukan : Stegoimage.
   - Data keluaran : File chiperteks, gambar.

Alur dan gambaran DFD level 1 ini akan ditunjukan pada gambar 3.5 berikut ini.



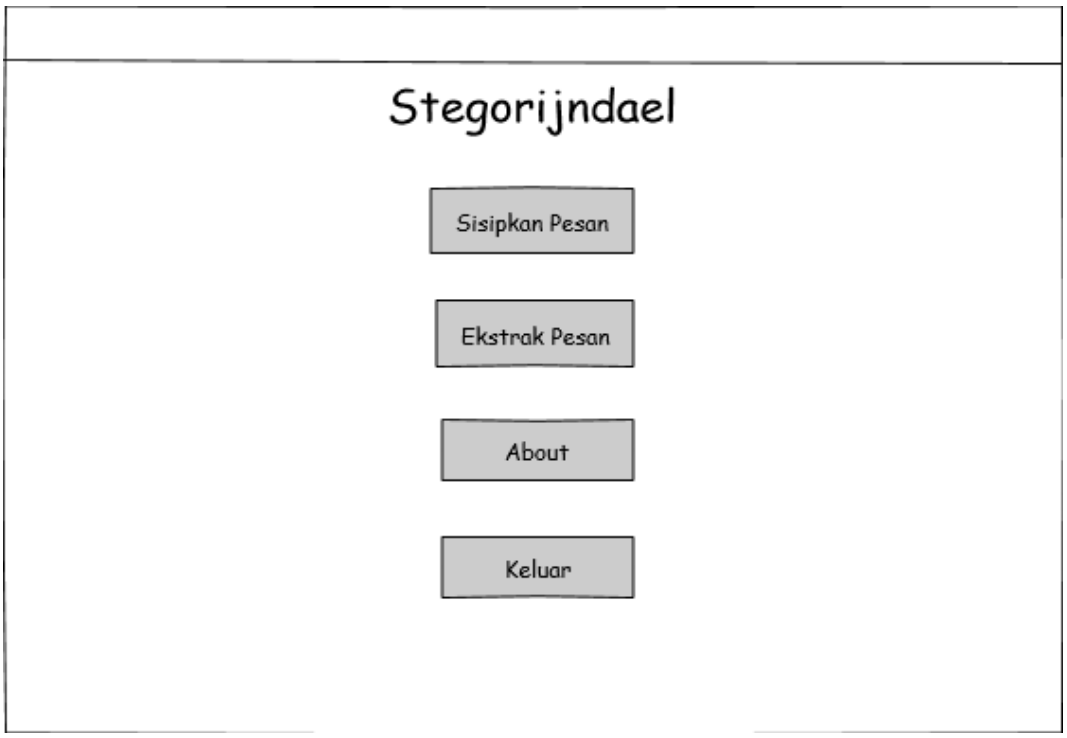
Gambar 3.5 DFD Level 1

3.4 Perancangan Antarmuka

Perancangan antarmuka merupakan rancangan antarmuka (*interface*) yang menjadi perantara antara sistem dengan pengguna (*user*). Tujuan dari perancangan antarmuka ini yaitu merancang antarmuka aplikasi yang akan dibangun dapat mudah dimengerti oleh pengguna.

3.4.1 Antarmuka Menu Utama

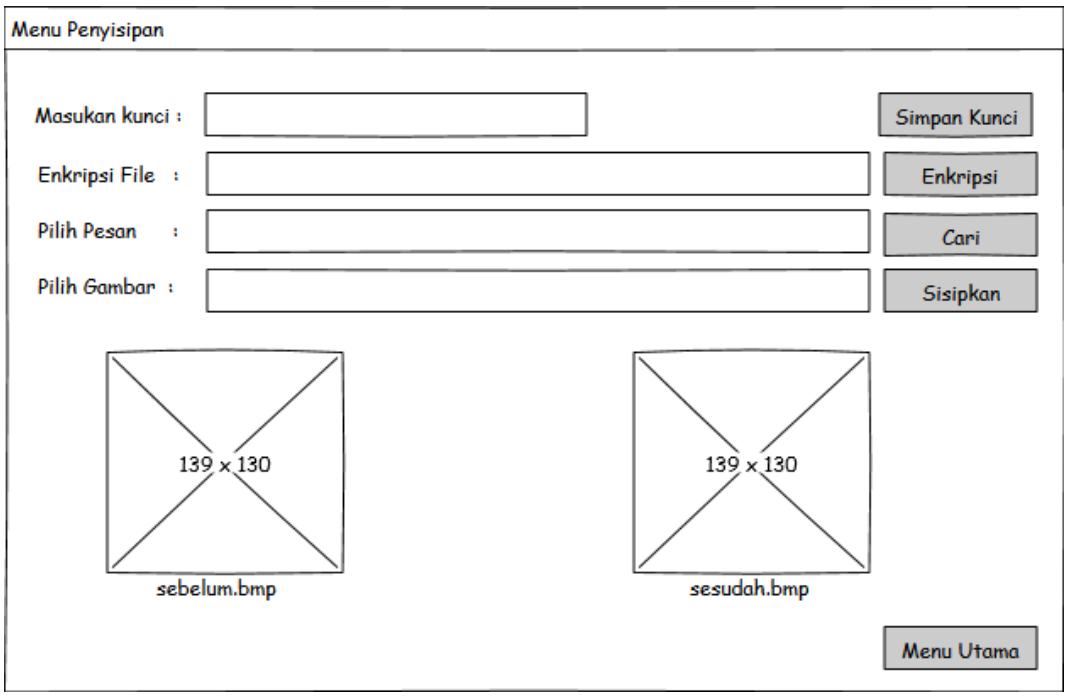
Desain antarmuka menu utama terdapat empat tombol yaitu tombol sisipkan pesan, tombol ekstrak pesan, tombol *about* dan tombol keluar. Tombol sisipkan pesan digunakan untuk mengarahkan pengguna ke jendela menu penyisipan untuk melakukan enkripsi pesan rahasia dan kemudian disisipkan ke media gambar. Tombol ekstrak pesan digunakan untuk mengarahkan ke jendela menu ekstrak untuk melakukan ekstrak pesan dan dekripsi pesan rahasia. Tombol keluar digunakan untuk menutup aplikasi. Gambar di bawah ini gambaran tentang desain antarmuka pengguna menu utama.



Gambar 3.6 Antarmuka menu utama

3.4.2 Antarmuka Menu Penyisipan *(Embedding)*

Pada rancangan antarmuka menu penyisipan kolom untuk memasukkan kunci dan tombol simpan kunci untuk menyimpan kunci. Tombol enkripsi untuk mengenkripsi pesan rahasia. Tombol cari pada pilih pesan untuk mengambil pesan rahasia yang sudah dienkripsi dan tombol sisipkan pada pilih gambar untuk memilih gambar yang akan disisipi kemudian proses dekripsi. Rancangan dari menu penyisipan ini dijelaskan pada gambar berikut.

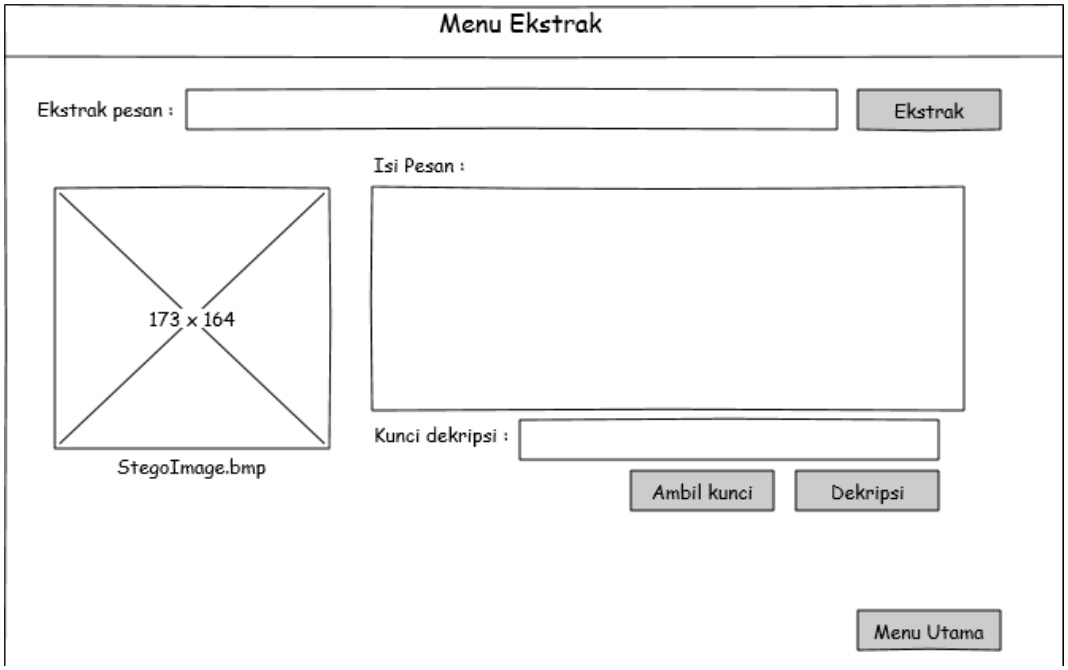


Gambar 3.7 Antarmuka menu penyisipan *(embedding)*

3.4.3 Antarmuka Menu Ekstrak

Rancangan antarmuka menu ekstrak yaitu rancangan untuk bagian menu ekstrak yang digunakan untuk ekstrak pesan. Pada bagian atas terdapat kolom masukkan stegoimage untuk untuk memilih stegoimage yang ingin diekstrak. Tombol ekstrak berfungsi untuk mengekstrak stegoimage. Pada bagian kiri terdapat tampilan gambar stegoimage, pada bagian kanan terdapat *textfield* yang berisi isi dari pesan rahasia. Di bawah *textfield* terdapat tombol ambil kunci yang berfungsi untuk mengambil file kunci. Tombol dekripsi untuk mendekripsi

pesan yang menggunakan kunci dekripsi. Tampilan menu ekstrak ada pada gambar 3.8 berikut.



Gambar 3.8 Antarmuka menu ekstrak

3.5 Rancangan Pengujian

Pada tugas akhir ini, akan dilakukan pengujian perangkat lunak yang mencakup proses penyisipan pesan, proses pengenkripsian isi pesan, ekstraksi pesan dan pengujian kinerja perangkat lunak. Adapun tujuan pengujian yang akan dilakukan mencakup :

1. Menguji kebenaran proses penyisipan dan ekstraksi pesan pada file gambar.
2. Mengukur kualitas dari stegoimage dilihat dari kriteria steganografi yang baik yaitu secara *fidelity, robustness, Recovery, Security.*
3. Menguji proses enkripsi dan dekripsi pesan.

3.5.1 Rancangan Pengujian Kinerja Perangkat Lunak

Rancangan pengujian kinerja perangkat lunak yang akan dilakukan adalah sebagai berikut :

1. Pengenkripsian isi pesan rahasia.
2. Penyisipan pesan rahasia ke dalam *file* gambar.
3. Ekstraksi sebuah *stegoimage* berupa *file* gambar yang telah disisipi pesan rahasia.
4. Pendekripsian isi pesan rahasia.
5. Memuat isi pesan rahasia sebelum dan sesudah dilakukannya proses penyisipan pesan.

3.5.2 Rancangan Pengujian Kebenaran Perangkat Lunak

Ada beberapa langkah yang dilakukan dalam pengujian kebenaran perangkat lunak yang dibangun. Langkah pengujian yang dilakukan sebelum penyisipan pesan rahasia pada *file* gambar yaitu:

1. Membuka *file* gambar berformat bitmap yang akan disisipi pesan rahasia.
2. Membuka isi pesan rahasia yang berupa *file* teks.

Langkah untk melakukan proses penyisipan pesan rahasia adalah sebagai berikut :

1. Masukkan kunci untuk enkripsi pesan rahasia.
2. Masukkan pesan rahasia berupa *file* teks (.txt).
3. Lakukan proses Enkripsi.
4. Masukkan *file* hasil enkripsi yang akan disisipkan.
5. Masukkan *file* gambar yang akan menjadi media proses penyisipan berupa gambar bitmap.

Untuk langkah proses pengekstraksian adalah sebagai berikut :

1. Masukan *stegoimage* berupa *file* gambar berformat bitmap.
2. Lakukan proses ekstraksi.
3. Masukkan kunci dekripsi.
4. Lakukan proses dekripsi pesan rahasia.

Keberhasilan proses penyisipan dinilai dari berubah tidaknya gambar yang menjadi media penyisipan pesan rahasia. Keberhasilan dari proses ekstraksi adalah ditemukannya sebuah pesan rahasia di dalam gambar kemudian hasil ekstrak akan didekripsi dan disimpan.

3.5.3 Metode Pengujian Kualitas Steganografi

Dalam subbab ini akan dijelaskan metode pengujian untuk mengetahui apakah algoritma Rindael ini mempengaruhi kualitas stegoimage hasil penyisipan menggunakan metode *Least Significant Bit*. Pengujian akan dilakukan setiap kriteria steganografi yaitu :

a. Pengujian *Fidelity*

   Metode yang digunakan untuk pengujian sesuai dengan kriteria *fidelity* adalah dengan mengukur nilai PSNR *(Peak Signal Noise to Ratio)* dari kedua gambar sebelum dan sesudah dilakukan proses penyisipan pesan. Nilai PSNR ini dapat dihitung dengan menggunakan *software* penghitung PSNR. Apabila nilai PSNR diatas 40 dB maka kualitas stegoimage tersebut tergolong baik. Namun apabila nilai PSNR tersebut berada di bawah angka 30 dB maka kualitas stegoimage tergolong rendah.

b. Pengujian *Robustness*

   Pengujian pada kriteria ini menguji ketahanan file stegoimage yang dihasilkan. Pengujian ini dilakukan dengan cara melakukan penyisipan pesan pada beberapa gambar media cover kemudian hasilnya dilakukan manipulasi gambar seperti crop, manipulasi brigthness, contrast dan sebagainya. Setelah dilakukan manipulasi stegoimage, kemudian dari setiap gambar dilakukan proses ekstraksi untuk mengetahui apakah stegoimage tersebut masih bisa diambil pesan yang disisipkan sebelumnya atau tidak.

c. Pengujian *Recovery*

   Pengujian pada kriteria ini dilakukan dengan menyisipkan pesan rahasia ke dalam beberapa jenis gambar kemudian dilakukan ekstraksi dan perbandingan antara pesan yang sebelum disisipkan dan pesan sesudah diekstrak.

d. Pengujian *Security*

Pengujian ini dilakukan dengan cara memastikan apakah pesan yang disisipkan sudah berhasil dienkripsi dengan baik atau belum. Dilakukan perbandingan antara pesan rahasia sebelum dan sesudah dilakukan enkripsi.