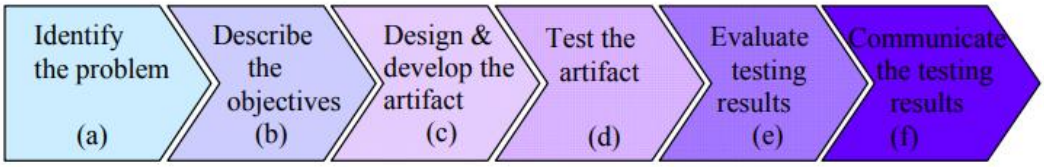
BAB III
METODE PENELITIAN

3.1. Desain Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah model *design and development* (D&D) atau dapat disebut dengan model desain dan pengembangan. (Richey & Klein, 2014) menjelaskan bahwa pendekatan model ini memiliki tiga buah unsur utama yaitu desain, pengembangan dan evaluasi yang seluruhnya terintegrasi dengan tujuan dalam menciptakan sebuah produk baru atau melakukan pengembangan pada produk yang sudah ada sehingga mampu mengembangkannya menjadi lebih baik lagi. Melalui definisi diatas, dapat diketahui bahwa model *design and development* (D&D) merupakan sebuah pendekatan yang melakukan penekanan dan studi yang sistemastis terhadap desain, pengembangan dan evaluasi dalam menciptakan produk baru atau memperbaiki produk yang sudah ada menjadi lebih baik lagi. Hal ini selaras dengan penelitian yang akan dibuat dimana perancangan aplikasi akan dimulai dengan tahapan desain, lalu pengembangan dan terakhir melakukan evaluasi.



Gambar 3.1 Prosedur penelitian design and development *(Ellis & Levy, 2010).*

Gambar 3.1 merupakan sebuah tahapan dari metode penelitian D&D dimana proses diawali dengan identifikasi masalah yang akan dijadikan latar belakang serta urgensi penelitian. Selanjutnya penjabaran tujuan penelitian yang akan menjadi solusi dalam menyelesaikan permasalahan yang ada. Lalu perancangan dan pengembangan sistem yang dimulai dari perancangan antarmuka dan sistem yang akan dibuat. Kemudian ada pengujian sistem yang dibuat mulai dari sistem secara menyeluruh hingga kebagian detailnya. Setelahnya adalah evaluasi hasil pengujian

Wesly Hugo Tamba, 2025
PERANCANGAN APLIKASI WEB UNTUK KEAMANAN DATA MENGGUNAKAN LSB DAN RAIL FENCE CIPHER PADA AUDIO
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

yang dilakukan dengan mengolah data hasil pengujian dan terakhir adalah mempresentasikan hasil penelitian yang telah diperoleh

3.2. Identifikasi Masalah (*Identify the problem*)

Badan Siber dan Sandi Negara (BSSN) mencatat bahwa setiap tahunnya Indonesia mengalami banyak sekali serangan siber. Aktivitas kejahatan siber di Indonesia juga menunjukan bahwa Indonesia merupakan salah satu negara dengan tujuan kejahatan siber tertinggi di dunia dimana pada 2023, Indonesia menempati urutan pertama dari top 10 tujuan anomali dengan total 208.612.734 anomali. Dengan banyaknya kejahatan siber yang banyak terjadi di Indonesia, tentu keberadaan data yang dimiliki dalam kondisi terancam karena sewaktu-waktu data tersebut dapat menjadi target penyerangan oleh para penjahat siber. Oleh karena itu, diperlukan sebuah sistem keamanan yang dapat mengamankan data yang dinilai berharga serta meminimalisir serangan siber. Penelitian ini berfokus pada keamanan data dengan memanfaatkan metode steganografi sebagai metode dalam menyembunyikan data yang berharga dengan menggunakan *file* audio sebagai media penyisipan. Pemilihan audio sebagai media sendiri didasarkan karena audio merupakan salah satu bentuk media yang saat ini sering kita jumpai dimanapun. Audio sendiri memiliki kapasitas yang cukup besar dan fleksibilitas yang cukup tinggi sehingga dapat dimanfaatkan sebagai salah satu media penampung dalam penerapan sistem keamanan steganografi.

3.3. Mendeskripsikan Tujuan (*Describe the objectives*)

Sebagai upaya dalam mengatasi permasalahan keamanan data yang telah diuraikan diatas, maka pembuatan aplikasi sebagai sistem keamanan dapat mengatasi permasalahan tersebut. Aplikasi ini menerapkan teknik steganografi sebagai metode mengamankan data dengan menyembunyikan data pada sebuah media audio. Aplikasi ini menggunakan algoritma *Least significant Bit* dan *Rail fence cipher* berbasis web yang dirancang khusus dalam meningkatkan keamanan data sesuai dengan kebutuhan dan menghindari risiko pencurian dan kebocoran data yang telah menjadi permasalahan serius dalam beberapa tahun terakhir. Dengan

demikian, aplikasi ini dapat menjadi salah satu solusi dalam memastikan data berharga yang dimiliki tidak mudah diketahui oleh orang lain

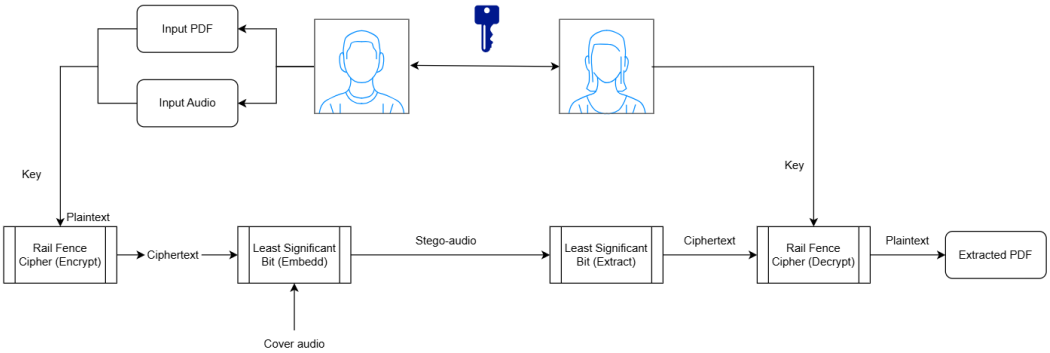
3.4. Desain dan Pengembangan Sistem (*Design and develop the artifact*)

Tahapan selanjutnya adalah tahapan desain dan pengembangan sistem dimana bagian ini menjelaskan dan membahas terkait rancangan desain dan pengembangan sistem yang akan dilaksanakan pada penelitian ini. Pengembangan sistem yang digunakan adalah metode *Agile.* Metode ini dipilih sebagai metode pengembangan sistem pada perancangan aplikasi website pengamanan data karena kelebihan metode ini memiliki kelebihan dalam menangani perubahan kebutuhan secara fleksibel. Metode Agile adalah sebuah metode ekspansi perangkat lunak yang didasarkan pada pengembangan sistem dalam kurun waktu singkat dengan mendahulukan adanya interaksi cepat dari sisi pengembangan ketika terjadi sebuah perubahan atau perbedaan dalam bentuk apapun (Handayani dkk., 2023).

1. Diagram Arsitektur

   Diagram arsitektur berikut menggambarkan keseluruhan proses yang terjadi dalam sistem yang dikembangkan. Dalam perancangan sistem ini, terdapat beberapa modul yang dapat digunakan yaitu modul menu, enkripsi dan dekripsi. Diagram arsitektur berfungsi dalam menjelaskan bagaimana cara kerja dari sistem yang dibangun dan interaksi dari setiap fungsi yang ada didalamnya.

   Pada gambar 3.2 menjelaskan bagaimana alur dari seluruh sistem dalam menjalankan sistem yang dikembangkan dengan menggunakan kombinasi *rail fence cipher* dan *Least significant Bit* dalam menjalankan proses enkripsi dan dekripsi. Proses diawali dengan menggunggah *file* PDF sebagai *file* yang akan disembunyikan dan *file* audio yang akan digunakan sebagai cover dalam menjalankan proses enkripsi. Setelahnya, maka key dimasukan sebagai bagian dalam menjalankan proses enkripsi dan dekripsi.

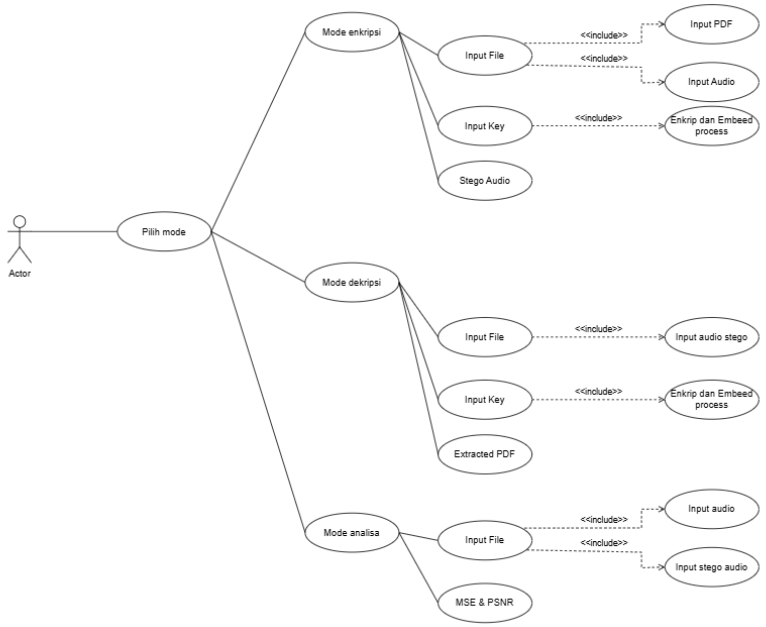


Gambar 3.2 Arsitektur Diagram Aplikasi Keamanan Data Pada Audio

Proses enkripsi akan membuat teks yang didalam PDF mengalami proses acak yang akan sulit dibaca oleh manusia dan akan menghasilkan sebuah *ciphertext* yang nantinya akan disisipkan kedalam sebuah audio dengan menggunakan steganografi *Least significant Bit*. Setelahnya maka akan dihasilkan sebuah *stego-audio*. Setelahnya, *stego-audio* dapat melakukan dekripsi dan ekstraksi dimana hal ini pertama dilakukan dengan menginputkan kunci sebelumnya. Lalu sistem akan melakukan ekstraksi dengan memishkan ciphertext dari audio dengan steganografi *Least significant Bit*. Setelahnya, dekrispi akan dilakuan berdasarkan kunci yang digunakan sebelumnya untuk mendapatkan kembali teks asli yang sudah disisipkan sebelumnya.

2. Desain Use Case Diagram

Bagian ini menjelaskan gambaran use case diagram pada sebuah sistem keamanan steganografi dalam mengamankan *file* PDF. Use case diagram adalah sebuah pemodelan pada sistem yang akan dibuat dengan melakukan pendeskripsian pada korelasi antara satu peran dengan peran lainnya. Penggunaan use case diagram juga dapat menggambarkan mengenai fungsi apa saja yang terdapat pada sistem dan siapa saja yang memiliki hak dalam menggunakan fungsi-fungsi tersebut (Hafsari dkk., 2023). Use case diagram dapat dilihat pada gambar 3.3



Gambar 3.3 Desain Use Case Diagram Keamanan Data Pada Audio

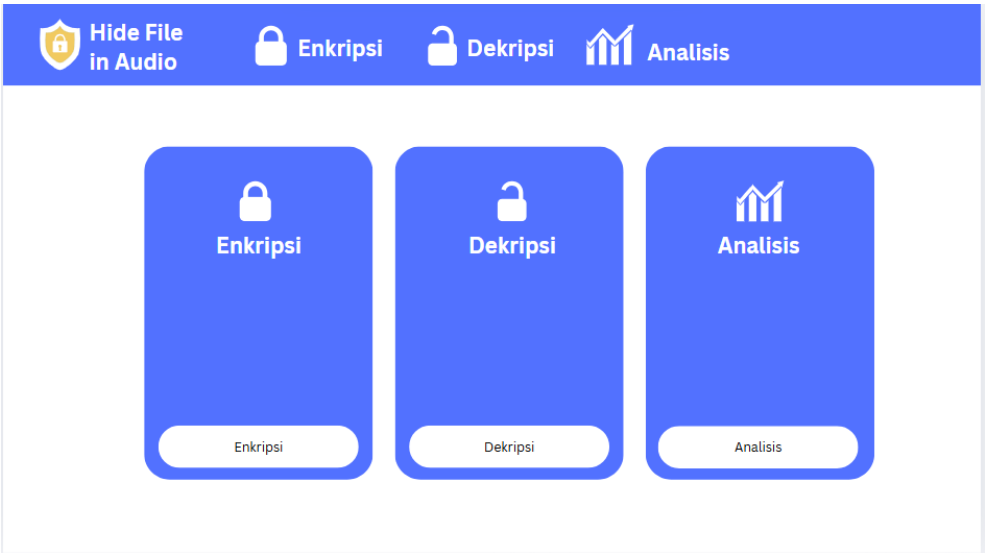
Pada gambar 3.3, terdapat 3 mode yang dapat digunakan dalam aplikasi *website* dengan pengamanan LSB dan *rail fence cipher* yang dirancang yakni mode enkripsi, mode dekripsi dan mode analisis. Pada mode enkripsi 2 fungsi yang terdiri fungsi input audio, *file* PDF dan *key* serta fungsi menjalankan enkripsi yang akan menghasilkan sebuah stego audio. Mode dekripsi memiliki 2 fungsi yakni fungsi input stego audio dan *key* serta fungsi menjalankan proses dekripsi yang akan menghasilkan sebuah *extracted* PDF. Mode analisis memiliki 2 fungsi yakni input audio dan stego audio serta proses menjalankan analisis yang akan menghasilkan informasi MSE dan PSNR.

3. Desain Website

Perencanaan desain website yang digunakan adalah website yang dikembangkan dengan memanfaatkan Flask, yang akan menjadi berfungsi sebagai server backend atau sebagai penyimpanan lokal. Tampilan antarmuka akan memanfaatkan penggunaan HTML, CSS dan Javascript. Penggunaan ketiganya berfungsi agar website yang diciptakan menjadi lebih interaktif dan responsif sehingga mudah untuk digunakan.

HTML akan berfungsi sebagai dasar dari pembentukan website, CSS berfungsi sebagai alat dalam melakukan *styling* pada website serta Javascript yang berfungsi dalam menciptakan sisi interaktivitas pada website yang memungkinkan pengguna dalam melakukan interaksi dengan website secara dinamis. Flask sebagai server backend akan mengelola data yang masuk pada halaman website serta melakukan interaksi dengan database sehingga data yang disimpan didalamnya dapat tersimpan dengan aman. Terakhir, pemanfaatan python sebagai bahasa pemrograman sebagai pengimplementasian algoritma *Least significant Bit* dan *reil fence cipher* yang menjadi fitur utama dalam website ini. Penggabungan seluruh teknologi ini akan memberikan solusi dalam menciptakan sistem keamanan berupa website yang dapat memenuhi kebutuhan fungsionalitas dan pengalaman penggunan yang maksimal.

Gambar 3.4, gambar 3.5, gambar 3.6 dan gambar 3.7 merupakan tampilan antarmuka yang dirancang sesuai dengan diagram arsitektur dan diagram alir yang dibuat. Pembuatan tampilan antarmuka juga disesuaikan agar pengguna lebih mudah untuk menggunakannya.



Gambar 3.4 Tampilan Antarmuka Awal Aplikasi

Pada gambar 3.4 menampilkan *mock-up* tampilan antarmuka aplikasi yang memiliki *navigation bar* dengan 4 menu yakni *home*, enkripsi, dekripsi dan analisis.

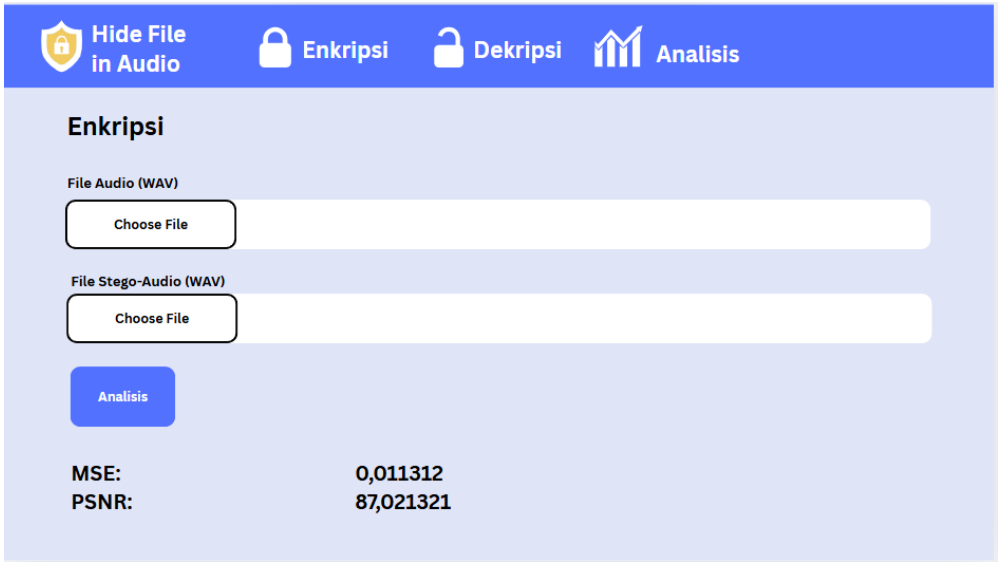
Pada bagian *body* terdapat 3 *card* yang masing-masing mewakili fitur tertentu yakni fitur enkripsi, dekripsi dan analisis.

Gambar 3.5 Tampilan Antarmuka Fitur Enkripsi

Pada gambar 3.5 menampilkan *mock-up* tampilan antarmuka yang memiliki *navigation bar* dengan 4 menu yakni *home*, enkripsi, dekripsi dan analisis. Pada bagian *body* terdapat beberapa hal yang memiliki beberapa *input bar* dengan 3 input bar yakni *input file* audio WAV, *input file* PDF, *input text key* dan tombol menjalankan enkripsi.

Gambar 3.6 Tampilan Antarmuka Fitur Dekripsi

Pada gambar 3.6 menampilkan *mock-up* tampilan antarmuka yang memiliki *navigation bar* dengan 4 menu yakni *home*, enkripsi, dekripsi dan analisis. Halaman antarmuka yang memiliki *input bar* dengan 3 input bar yakni *input file* stego audio WAV, *input text key* dan tombol menjalankan dekripsi.



Gambar 3.7 Tampilan Antarmuka Fitur Analisis

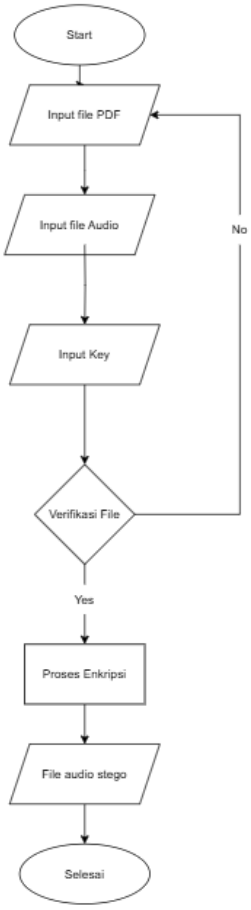
Pada gambar 3.7 menampilkan *mock-up* tampilan antarmuka yang memiliki *navigation bar* dengan 4 menu yakni *home*, enkripsi, dekripsi dan analisis. Pada bagian *body* terdapat beberapa hal yang memiliki beberapa *input bar* dengan 2 *input* bar yakni *input file* audio WAV, *input file* stego audio WAV, dan tombol menjalankan analisis yang akan menghasilkan nilai MSE dan PSNR

4. Flowchart Sistem

Diagram Flowchart atau diagram alir merupakan sebuah metode analitis gambar dalam menjelaskan beberapa aspek secara jelas, ringkas, dan logis dimana didalamnya terdapat sebuah grafik yang berisi langkah-langkah atau procedural dalam menjalankan suatu program atau sistem sehingga akan mempermudah orang lain dalam memahami sebuah program atau sistem yang akan dirancang (Tuasamu dkk., 2023).

Penggunaan flowchart akan menggunakan simbol-simbol grafis yang dapat menjadi representasi dari tahapan, keputusan atau operasi yang terjadi dalam sebuah sistem. Tujuannya agar mampu memberikan gambaran yang jelas dan mudah dipahami tentang bagaimana sebuah sistem nantinya berjalan atau beroperasi.

a. Proses Enkripsi dan Embedding

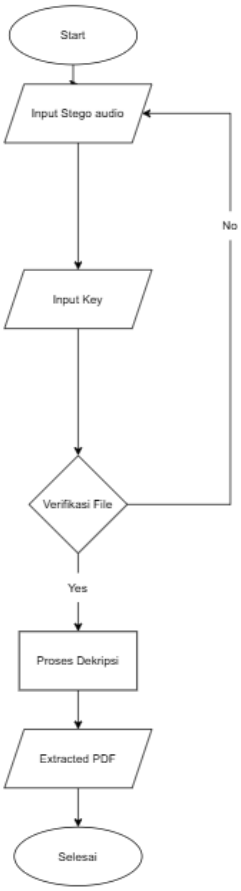


Gambar 3.8 Flowchart Enkripsi dan Embedding Keamanan Data Pada Audio

Pada gambar 3.8 dijelaskan proses enkripsi dan *embedding* (penyisipan) dimana dalam aplikasi ini dilakukan dalam menentukan *file* PDF sebagai data yang akan disisipkan serta audio dengan format WAV yang akan digunakan sebagai media penampung. Setelah kedua *file* dimasukan, maka sistem akan melakukan validasi terlebih dahulu apakah kedua *file* telah dimasukan kedalam kolom. Jika belum, maka sistem akan memunculkan sebuah *alert* yang

memberitahu jika masih ada kolom yang kosong dan harus mengisikannya terlebih dahulu. Selanjutnya sistem akan meminta *key* sebagai alat untuk melakukan enkripsi pada *file*. Jika kedua *file* sudah dimasukan dan key sudah ditentukan, maka sistem akan melakukan proses *encryption* dan *embedding* pada audio yang telah diinputkan. Nantinya, sistem akan menghasilkan sebuah *file* berupa sebuah audio yang nantinya dapat diekstraksi kembali untuk mendapatkan kembali *file* yang telah disisipkan sebelumnya.

b. Proses Dekripsi dan Extracing



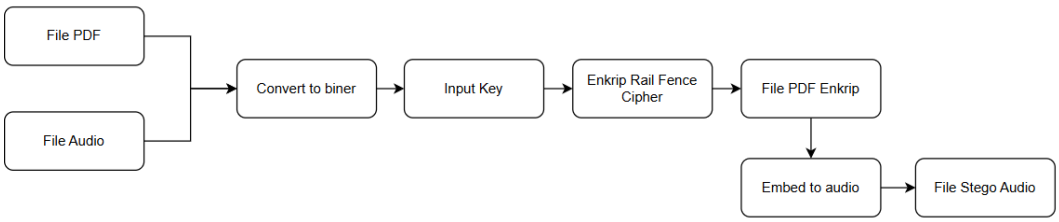
Gambar 3.9 Flowchart *Extracting* (Ekstraksi) Keamanan Data Pada Audio

Pada gambar 3.9 dijelaskan roses *extracting* (ekstraksi) dimana dalam aplikasi ini dilakukan untuk kembali memisahkan *file* yang sudah disisipkan dengan audio sebagai media penampung. Proses ini dilakukan dengan

memasukkan *file* audio stego yang telah didapatkan sebelumnya dan memasukan key yang sebelumnya digunakan. Setelahnya, sistem akan melakukan validasi apakah *file* audio stego tersebut mengandung sebuah *file* yang disisipkan atau tidak dan key yang dimasukan sudah benar atau belum. Jika tidak, maka sistem akan memberikan *alert* bahwa *file* yang diinputkan tidak sesuai. Jika sesuai, maka sistem akan mulai melakukan proses ekstraksi. Nantinya, sistem akan menghasilkan *output* yaitu kondisi *file* akan dikembalikan kesedia awal dimana *file* PDF dan *file* audio akan dipisahkan sehingga pengguna dapat membuka *file* PDF tersebut.

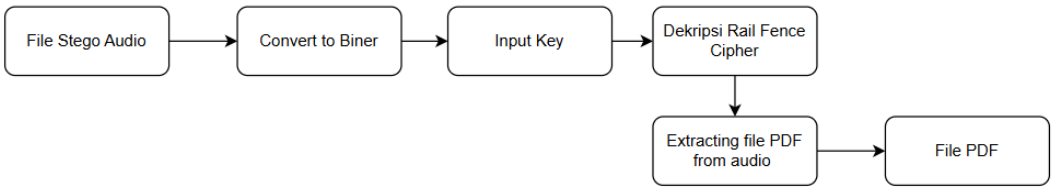
5. Diagram Blok Sistem

Diagram blok sistem merupakan suatu perancangan sistem yang memberikan visualisasi tentang bagaimana prinsip kerja sebuah rangkaian sistem bekerja secara keseluruhan. Blok-blok tersebut disusun hingga membentuk sebuah sistem agar dapat membentuk sistem yang dapat difungsikan sesuai dengan perencanaan.



Gambar 3.10 Diagram Blok Enkripsi-Embedding Keamanan Data Pada Audio

Pada gambar 3.10 menjelaskan proses dari enkripsi dan embedding dimana proses dilakukan dengan menentukan *file* PDF dan audio yang akan digunakan. Selanjutnya adalah menentukan *key* yang berfungsi sebagai acuan dalam melakukan enkripsi dengan base64. Setelah *file* PDF terenkrip, maka tahapan selanjutnya adalah melakukan proses embedding dengan menyisipkan *file* PDF kedalam audio dengan menggunakan *Discrete Wavelet Transform* sehingga pada proses akhir PDF telah disispkan kedalam audio dan diperoleh sebuah *file* stego dalam format audio.



Gambar 3.11 Diagram Blok Dekripsi-Extracting Keamanan Data Pada Audio

Selanjutnya pada gambar 3.11 dijelaskan blok diagram dalam proses dekripsi dan *extracting.* Proses ini nantinya dilakukan dengan memasukan audio stego yang telah diperoleh sebelumnya. Selanjutnya memasukkan *key* yang digunakan untuk melakukan dekripsi pada *file* PDF agar teks didalamnya dikembalikan dalam bentuk semula. Setelah semuanya selesai diisi maka sistem akan memulai proses extracting terlebih dahulu, setelah itu *file* PDF dilakukan metode dekripsi sehingga *file* sebelumnya kembali seperti semula.

3.5. Desain Uji Coba Sistem (*Test the artifact*)

Design uji coba dilakukan dengan menggunakan *Black Box Testing* dimana metode ini digunakan dengan melakukan pengamatan pada *input* dan *output* pada *software* yang dibuat tanpa membuka baris kode pada *software* tersebut (Fahrezi dkk., 2022). *Black Box Testing* adalah sebuah pengujian dimana pengujian teknologi tidak melibatkan struktur interior dan baris logika perangkat lunak sehingga pengujian didasarkan pada spesifikasi kebutuhan yang sudah dirancang dan tidak memerlukan analisa terhadap baris kode. Salah satu kelebihan dari *Black Box Testing* adalah kemampuannya dalam menemukan aspek-aspek yang bermasalah atau tidak terpenuhi yang diberikan dalam pengembangan perangkat lunak (Praniffa dkk., 2023).

Dalam penggunaan metode pengujian ini, pengujian akan dilakukan pada tahap akhir perancangan yang memberikan kesempatan dalam melakukan identifikasi *error* atau kekurangan yang mungkin saja tidak terdeteksi pada saat perancangan yang mampu memastikan kualitas dan fungsionalitas aplikasi berjalan sesuai perencanaan. Tahapan pengujian perangkat lunak dengan menggunakan metode *black box testing* dapat dilihat pada tabel 3.1. Proses ini melibatkan

berbagai macam skenario pengujian dalam mengidentifikasi *bug* atau *error* dalam perangkat lunak.

Tabel 3.1 Skenario Uji Coba Sistem *Website*

Fitur yang Diuji	**Jenis Fitur**	**Kebutuhan**	**Hasil yang Diharapkan**
Embedding dan enkripsi	1. Tampilan Input *file* PDF 2. Tampilan Input *File* Audio 3. Tampilan Input Key	Pengguna dapat melakukan *input file* PDF dan *file* audio. Setelah itu Pengguna dapat memasukan key untuk melakukan enkripsi. Selanjutnya sistem akan melakukan verifikasi apakah format yang dimasukan sudah sesuai dengan aturan yang dibuat	1. *File* PDF dan Audio dapat dimasukan kedalam sistem 2. Proses enkripsi dengan *rail fence cipher* dapat dilakukan pada *file* PDF 3. *File* PDF akan disisipkan pada *file* audio menggunakan teknik steganografi LSB tanpa mengubah audio secara signifikan 4. *File* audio dengan *file* PDF yang sudah tersembunyi siap untuk disimpan
Extraction dan dekripsi	1. Tampilan input *file* audio hasil stego	Pengguna dapat melakukan *input file* audio stego. Sistem melakukan validasi bahwa	1. *File* audio stego dapat dimasukan kedalam sistem 2. Key yang sebelumnya

Fitur yang Diuji	Jenis Fitur	Kebutuhan	Hasil yang Diharapkan
		format yang diinputkan sudah sesuai dengan aturan yang dibuat	digunakan dimasukan kembali 3. *File* audio stego yang diterapkan metode steganografi LSB akan diekstraksi 4. *File* PDF yang telah diekstraksi dapat diakses kembali oleh pengguna dengan memastikan data dalam kondisi yang sempurna
Analisis	1. Tampilan input file audio 2. Tampilan input stego-audio	Pengguna dapat melakukan *input file* audio dan audio stego. Sistem melakukan validasi bahwa format yang diinputkan sudah sesuai dengan aturan yang dibuat	1. *File* audio dapat dimasukan kedalam sistem 2. *File* audio stego dapat dimasukan kedalam sistem *3.* Proses perhitungan MSE dan PSNR dapat dilakukan

Pada tabel 3.1 dipaparkan bagaimana perancangan untuk pengujian *black box.* Pengujian *black box* dilakukan pada 3 fitur utama yaitu enkripsi, dekripsi dan analisis. Setiap fitur memiliki masing-masing fungsinya dimana nantinya pengujian dilakukan untuk memastikan setiap fungsi dapat berjalan saling terhubung untuk menjalankan 3 fitur utama

3.6. Desain Evaluasi Hasil Uji (*Evaluate testing result*)

Evaluasi dilakukan dengan melakukan analisa data terhadap hasil yang telah diperoleh setelah melalui serangkaian percobaan yang telah dilakukan. Proses ini dilakukan dalam membentuk kesimpulan mengenai kesesuaian hasil produk yang dikembangkan dengan tujuan penelitian yang telah ditentukan diawal. Dalam konteks penelitian yang dilakukan, evaluasi bertindak sebagai parameter dalam memastikan bahwa solusi yang dikembangkan dan dibuat benar-benar bekerja dengan baik dalam melindungi data pada media audio. Hasil pengujian akan dievaluasi berdasarkan kuisoner, korelasi pearson, serta nilai MSE dan PSNR sebagai penentu keberhasilan algoritma yang diterapkan dalam menjaga data yang disisipkan pada media audio.

Pengujian pertama dilakukan dengan melihat kinerja algoritma secara langsung. Hal ini untuk memastikan bahwa setiap algoritma dapat menjalankan tugasnya masing-masing sehingga ketika nantinya dikombinasikan akan meningkat tingkat pengamanan data yang akan dilakukan. Pengujian *rail fence cipher* dilakukan dengan mengujikannya kepada salah satu dokumen yang berisi teks dan melihat secara langsung antara bentuk awal, hasil enkripsi dan hasil dekripsi. Lalu pengujian *least significant bit* dilakukan dengan menguji 4 buah audio dengan durasi yang berbeda-beda dan disisipkan dengan sebuah PDF dengan ukuran yang berbeda-beda. Hasil yang diperoleh nantinya akan ditampilkan dalam bentuk tabel dan dilakukan penjelasan mengenai hasil proses penyisipan dan ekstraksi serta penjelasan mengenai jika adanya kegagalan dalam proses didalamnya.

Korelasi pearson digunakan dalam mengukur korelasi antara 2 variabel. Dalam konteks kriptografi, korelasi pearson digunakan dalam mengukur kekuatan kriptografi sebagai metode enkripsi dimana pendekatan ini menguji korealasi antara *plaintext* dan *ciphertext.* Pengukuran nilai korelasi pearson sendiri dibagi menjadi dua yaitu 0 untuk menggambarkan tidak ada korelasi dan 1 maupun -1 untuk menggambarkan adanya korelasi. Oleh karena itu, pengujian korelasi pearson yang dicari pada penelitian ini adalah nilai korelasi pearson yang mendekati angka 0 yang dapat menggambarkan bahwa tidak ada korelasi antara *plaintext* dan *ciphertext.*

Sebaliknya Nilai korelasi pearson yang mendekati angka 1 dapat menggambarkan bahwa terdapat korelasi antara *plaintext* dan *ciphertext.* Pengujian korelasi pearson dilakukan dengan dua kali percobaan yaitu dalam bentuk teks dan dalam bentuk biner dengan tujuan untuk memastikan bahwa teks berhasil dienkripsi dan sulit untuk dipahami hingga pada tingkatan nilai bit.

MSE (Mean Squared Error) digunakan untuk mengukur perbedaan rata-rata antara sinyal audio asli dan sinyal audio hasil penyisipan data. Nilai MSE yang lebih kecil menunjukkan bahwa perubahan yang terjadi pada media audio akibat proses steganografi relatif kecil, sehingga kualitas audio tetap terjaga. Sebaliknya, nilai MSE yang besar menunjukkan adanya distorsi yang signifikan pada audio yang telah dimodifikasi, yang dapat mengurangi keefektifan metode yang digunakan. Pengujian ini dilakukan dengan membandingkan dua buah audio yaitu audio original serta audio yang telah mengalami modifikasi dengan memastikan bahwa nilai MSE yang diperoleh adalah nilai yang mendekati 0.

Sementara itu, PSNR (Peak Signal-to-Noise Ratio) berfungsi untuk mengukur kualitas audio yang telah dimodifikasi dengan membandingkan tingkat sinyal asli terhadap tingkat noise yang diperkenalkan oleh proses steganografi. PSNR dinyatakan dalam satuan desibel (dB), di mana nilai PSNR yang lebih tinggi menandakan bahwa kualitas audio hasil steganografi masih mendekati kualitas audio asli. Umumnya, nilai PSNR di atas 30 dB menunjukkan bahwa perubahan yang terjadi sulit dideteksi oleh pendengaran manusia, sehingga metode yang digunakan dianggap berhasil dalam menjaga kualitas audio sambil tetap menyisipkan informasi secara aman. Pengujian ini dilakukan dengan membandingkan dua buah audio yaitu audio original serta audio yang telah mengalami modifikasi dengan memastikan bahwa nilai PSNR yang diperoleh adalah nilai yang mampu diatas 30 dB.

Pengujian dengan melakukan kuisoner dilakukan dengan memberikan dua buah jenis audio dimana audio A adalah audio original dan audio B adalah audio hasil modifikasi. Pengujian ini dilakukan dengan menilai bagaimana seseorang

dapat merasakan perbedaan antara audio original dengan audio hasil modifikasi. Kuisoner dilakukan dengan metode kombinasi yaitu *random sampling* dimana pengambilan sampel diambil secara acak tanpa memandang strata yang ada dalam populasi dan purposive sampling dengan memilih beberapa orang yang cukup ahli dibidangnya. Setelahnya, setiap hasil yang diperoleh nanti akan dibandingkan dengan melihat perbandingan antara orang yang dapat merasakan perbedaan antara kedua audio tersebut dengan orang yang tidak dapat merasakan perbedaan antara kedua audio tersebut. Beberapa pertanyaan yang diujikan yaitu:

"Manakah Audio yang menurut anda lebih baik kualitasnya"

"Jika menjawab A atau B, jelaskan perbedaan yang anda dengar"

Melalui pengujian dengan menggunakan kuisoner, korelasi pearson serta MSE & PSNR diharapkan dapat menghasilkan hasil evaluasi yang dapat digunakan sebagai parameter keberhasilan penelitian ini. Kuisoner sebagai pengujian penyamaran audio pada kehidupan nyata, korelasi pearson sebagai parameter dalam menilai korelasi dari *plaitext* dan *ciphertext* yang dihasilkan algoritma *rail fence cipher*, serta MSE dan PSNR sebagai parameter menilai hasil modifikasi audio oleh *least significant bit.* Hasil evaluasi ini akan menjadi dasar dalam menilai keberhasilan metode yang diusulkan dalam penelitian ini.

3.7. Pemaparan Hasil Uji (Comunicating the testing result)

Tahapan ini merupakan tahap akhir dalam metode penelitian D&D yaitu tahap '*comunicating the testing result'*. Data yang diperoleh melalui analisa hasil kemudian disimpulkan untuk selanjutnya dilaporkan sebagai laporan tertulis skripsi dan dilakukan komunikasi melalui bimbingan skripsi dihadapan dosen pembimbing. Melalui proses komunikasi pada bimbingan skripsi maka hasil analisa data akan mengandung banyak informasi seperti proses dari desain dan perancangan sistem, kontribusi sistem yang dikembangkan terhadap perkembangan teknologi keamanan data, keterkaitan antara penelitian sebelumnya dengan penelitian yang dilakukan serta pengembangan selanjutnya bagi para peneliti dimasa depan.