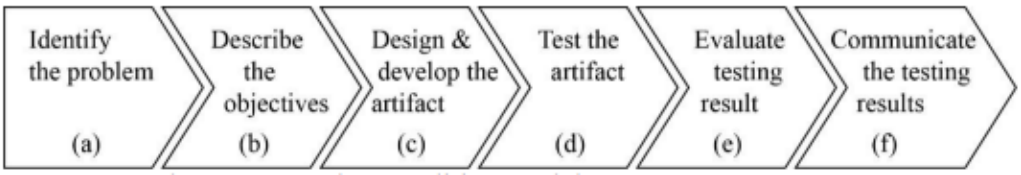
BAB III
METODE PENELITIAN

3.1 Desain Penelitian

Metode penelitian yang akan digunakan selama penelitian ini berlangsung adalah Model *Design and Development* (D&D) atau riset desain dan pengembangan, (Richey dan Klein, 2007) memaparkan bawasanya model ini merupakan, "*the systematic study of design, development, and evaluation processes with the aim of establishing an empirical basis for the creation of instructional and non-instructional product and tools and new or enhanced models that govern their development*". Berdasarkan pendapat tersebut didapat kesimpulan model D&D merupakan studi yang sistematis terhadap proses desain, pengembangan, dan evaluasi dengan tujuan untuk menetapkan dasar empiris dalam penciptaan produk dan alat instruksional dan non-instruksional serta model baru atau yang disempurnakan.. Adapun ilustrasi skema yang dilakukan pada penelitian ini berdasarkan prinsip desain D&D dapat dilihat pada gambar 3.1



Gambar 3. 1 Prosedur penelitian model D&D (Ellis dan Levy, 2010)

3.2 Identifikasi Masalah (*Identify the problem*)

Badan Siber dan Sandi Negara (BSSN) mencatat, Indonesia kembali mendapatkan 279,84 juta serangan siber pada 2023. Walaupun demikian, jumlah tersebut menurun 24,4% dari tahun sebelumnya yang sebanyak 370,02 juta serangan. Dengan banyaknya serangan siber dan juga Undang-Undang terkait yang mewajibkan kerahasiaan data medis, diperlukan sebuah aplikasi yang dapat mengamankan data medis guna meminimalisir serangan siber pada waktu atau tahun yang akan datang. Penelitian ini berfokus pada keamanan rekam medis yang memuat catatan lengkap mengenai identitas, pemeriksaan, pengobatan, dan layanan medis yang telah diterima pasien. Sesuai dengan PERMENKES RI No. 24 tahun 2022, semua fasilitas kesehatan di Indonesia diwajibkan untuk mengimplementasikan sistem rekam medis elektronik sebelum akhir Desember

2023. Penelitian ini bertujuan untuk merancang dan mengembangkan sebuah aplikasi yang mampu mengamankan data medis elektronik, yang mana sangat penting untuk menjaga kerahasiaan dan integritas data medis dalam menghadapi ancaman serangan siber.

3.3 Mendeskripsikan Tujuan (*Describe the objectives*)

Untuk mengatasi masalah keamanan data medis yang telah diuraikan, merancang dan mengembangkan sebuah aplikasi pengamanan data medis. Aplikasi ini menggunakan Algoritma *Vigenere Cipher* dan LSB berbasis web, yang dirancang khusus untuk meningkatkan keamanan data medis sesuai dengan kebutuhan regulasi dan menghindari risiko kebocoran data yang telah menjadi perhatian serius dalam beberapa tahun terakhir.

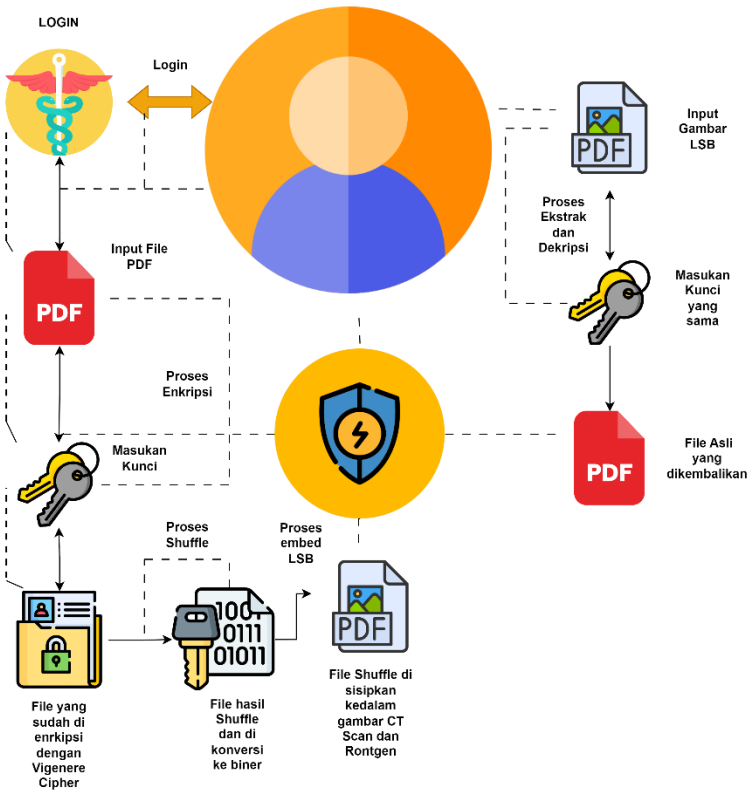
Aplikasi ini menggunakan kombinasi Algoritma *Vigenere Cipher* dan teknik LSB dalam sebuah platform berbasis web yang dirancang untuk memastikan integritas dan kerahasiaan data medis. Dengan demikian, aplikasi ini tidak hanya akan membantu fasilitas kesehatan mematuhi regulasi yang ketat, tetapi juga melindungi hak privasi pasien dari ancaman kebocoran data.

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

Kemudian selanjutnya masuk ke dalam tahapan desain dan pengembangan sistem. Dimana pada bagian ini akan membahas terkait rancangan desain dan pengembangan sistem untuk dilaksanakan pada penelitian ini. Adapun hal-hal tersebut sebagai berikut :

1. Desain *Use Case Diagram*

   Dalam bagian ini menggambarkan use case diagram untuk sebuah sistem keamanan informasi dalam konteks medis, khususnya dalam penanganan dokumen PDF. *Use Case Diagram* untuk aplikasi pengamanan data medis ini dapat dilihat pada gambar 3.2



Gambar 3. 2 *Desain Use Case Diagram*

Dalam sistem ini, hanya dokter dan perawat yang diberi wewenang untuk mengakses dan mengelola dokumen. User ini memiliki kemampuan untuk membuka, mengedit, dan mengenkripsi dokumen medis untuk menjaga keamanan data pasien.

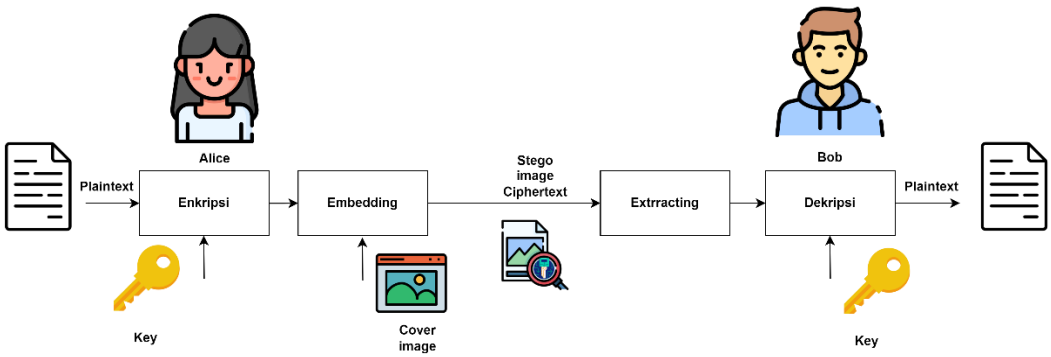
2. Desain Web

Desain web yang direncanakan akan dikembangkan menggunakan bahasa pemrograman PHP, yang akan berfungsi sebagai server back-end atau sebagai sistem penyimpanan lokal. Untuk tampilan antarmuka pengguna, pengembangan akan menggunakan HTML, CSS, dan JavaScript, yang merupakan teknologi standar untuk membangun tampilan web yang interaktif dan responsif. HTML akan digunakan untuk struktur dasar halaman web, sementara CSS akan menangani *styling* visual untuk memastikan tampilan yang konsisten dan menarik. JavaScript, di sisi lain, akan digunakan untuk menambahkan interaktivitas pada halaman, memungkinkan pengguna untuk berinteraksi dengan elemen web secara dinamis. PHP sebagai *server back-end*

akan mengelola logika aplikasi, pengolahan data, dan interaksi dengan database, memastikan bahwa data yang disimpan dan diproses aman dan efisien. Penggabungan semua teknologi ini akan menciptakan solusi web yang kuat, memenuhi kebutuhan fungsional sambil memberikan pengalaman pengguna yang optimal.

3. *Flowchart* Sistem

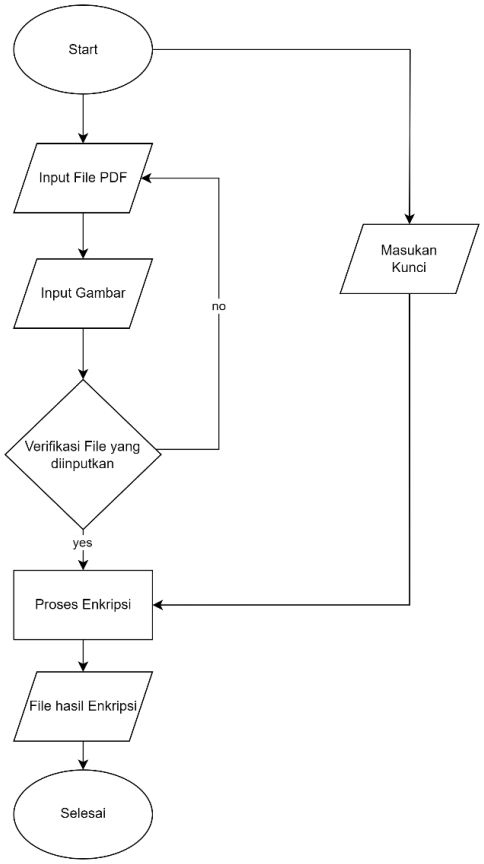
Flowchart adalah representasi visual dari alur atau langkah-langkah dalam suatu proses atau program. *Flowchart* menggunakan simbol-simbol grafis untuk menggambarkan langkah-langkah, keputusan, atau operasi dalam suatu sistem. Tujuan utama dari *flowchart* adalah memberikan gambaran yang jelas dan mudah dimengerti tentang bagaimana suatu proses atau sistem beroperasi. Pada gambar 3.3 ditampilkan *flowchart* utama sistem :



Gambar 3. 3 Flowchart Sistem

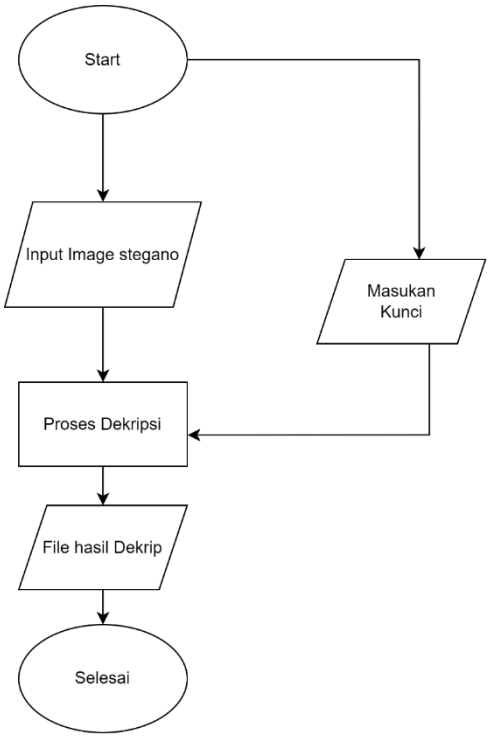
Alice ingin mengirimkan file secara aman kepada Bob, sehingga dia menggunakan kombinasi steganografi dan kriptografi. Pertama, Alice mengenkripsi file menggunakan kunci enkripsi untuk memastikan bahwa file tersebut aman dari akses tidak sah. Setelah file terenkripsi, Alice menyisipkan file tersebut ke dalam sebuah gambar menggunakan teknik steganografi, di mana gambar tersebut bertindak sebagai *'cover'* yang menyembunyikan keberadaan file. Gambar ini kemudian dikirimkan kepada Bob, yang tampak normal dan tidak menunjukkan adanya file tersembunyi. Setelah menerima gambar, Bob mengekstrak file terenkripsi dari dalamnya dan menggunakan kunci dekripsi yang sesuai untuk mendekripsi dan mengakses isi file asli. Proses ini memberikan keamanan ganda melalui enkripsi, yang melindungi isi file, dan

steganografi, yang menyembunyikan keberadaan file itu sendiri, menjamin tingkat keamanan yang sangat tinggi dalam komunikasi mereka.



Gambar 3. 4 Flowchart Enkripsi dan *Embedding*

Proses enkripsi dan *embedding* dalam aplikasi ini dimulai dengan memasukkan file PDF dan gambar yang diinginkan. Setelah verifikasi file berhasil, pengguna diminta untuk memasukkan kunci enkripsi. File PDF kemudian dienkripsi menggunakan kunci tersebut dan data yang dienkripsi disisipkan ke dalam gambar yang dipilih. Kemudian setelah itu sistem akan mengenkripsi data di dalam file menjadi ciphertext atau kode secara acak, lalu file tersebut akan disisipkan kedalam suatu media disini peneliti menggunakan gambar sebagai medianya tanpa mengubah struktur data dalam file tersebut. File yang di hasilkan akan berupa gambar yang nantinya akan diekstraksi dan didekripsi untuk mengembalikan file asli tersebut.

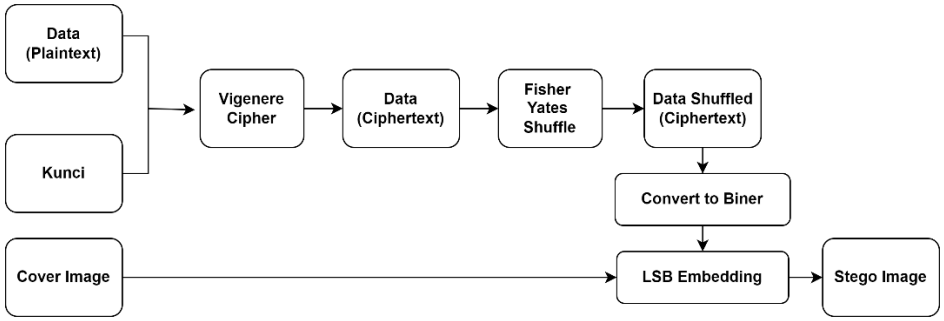


Gambar 3. 5 Flowchart Dekripsi dan Extracting

Pada gambar 3.5 menjelaskan cara kerja sistem dekripsi dan ekstraksi pada penelitian ini yang dimana nantinya membutuhkan suatu kunci atau key untuk proses ini. Kemudian masukan gambar hasil embedding untuk diekstraksi yang dimana proses ini akan mengembalikan file asli, lalu file asli tersebut akan di dekripsi agar data di dalamnya kembali menjadi sebuah plaintext atau data asli. *Output* dari sistem ini akan berupa file asli yang sudah di dekripsi dari *ciphertext* menjadi *plaintext*.

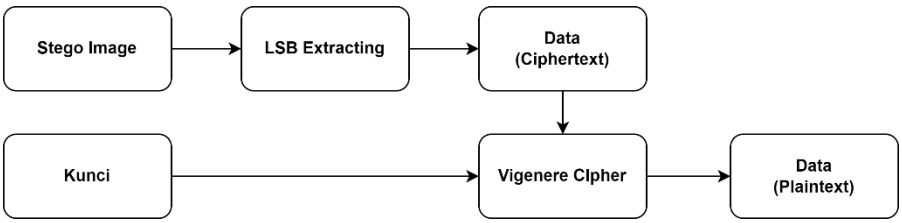
4. *Diagram Blok* Sistem

   Diagram Blok adalah representasi visual yang efektif dalam menggambarkan alur dalam suatu proses. Dalam konteks pengembangan sistem enkripsi dan *embedding* serta dekripsi dan *extracting*, *diagram blok* menjadi alat penting untuk memvisualisasikan dan merencanakan setiap tahapan proses tersebut secara detail.



Gambar 3. 6 Diagram Blok proses enkripsi dan embedding

Pada gambar 3.6 Diatas terdapat gambar *Diagram Blok* proses Enkripsi dan *Embedding* dimana nantinya terdapat Data yang berisi Plaintext dan juga Kunci dimasukan bersamaan agar bisa diproses dengan Algoritma *Vigenere Cipher* untuk dienkripsi yang nantinya akan menghasilkan Data berisi *Ciphertext*. Setelah itu Data *Ciphertext* ini akan diacak kembalikan menggunakan *Fisher Yates Shuffle* untuk meningkatkan keamanan dan menjadi Data *Ciphertext* yang sudah ter-shuffle. Data hasil shuffle ini lah yang akan di convert menjadi biner terlebih dahulu untuk masuk kedalam proses LSB *Embedding* atau proses penyisipan data kedalam sebuah *Cover Image* dan hasil akhir dari proses ini adalah Stego Image atau Gambar hasil penyisipan.detail.



Gambar 3. 7 Diagram Blok proses dekripsi dan extracting

Kemudian Pada gambar 3.7 terdapat gambar *Blok Diagram* proses Dekripsi dan *Extracting*. Proses ini nantinya akan memasukan *Stego Image* atau gambar hasil penyisipan dan masuk kedalam proses LSB *Extracting* dimana pada proses ini akan mengeluarkan Data *Ciphertext* yang ter-*shuffle*. Setelah dikeluarkan maka akan ada Kunci yang sama atau simetris yang digunakan untuk dimasukan pada proses dekripsi *Vigenere Cipher* dan hasil akhir pada proses ini yaitu kembalinya Data asli yang berisi *Plaintext.*

5. Pengembangan Sistem

   Metode *Agile* dipilih untuk pengembangan aplikasi Pengamanan Data Medis berbasis web karena keunggulannya dalam menangani perubahan kebutuhan secara fleksibel, memungkinkan tim untuk mudah kembali ke tahap pengembangan sebelumnya jika ada perubahan yang diperlukan, seperti yang dijelaskan oleh D. A. P. Putri (2019). Metode ini melibatkan serangkaian iterasi singkat yang disebut *sprint*, di mana setiap *sprint* difokuskan pada penambahan atau peningkatan fitur tertentu yang selanjutnya dapat segera diuji dan dievaluasi. Proses pengembangan menggunakan Agile melalui enam tahap utama, yaitu perencanaan, desain, pengembangan, pengujian, penerapan, dan evaluasi, memastikan bahwa aplikasi terus berkembang sesuai dengan kebutuhan pengguna dan kondisi pasar yang berubah-ubah.

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

Uji Coba Sistem akan menggunakan metode *Black Box Testing*, yang bertujuan untuk mengevaluasi fungsi aplikasi tanpa memeriksa struktur internal atau kode sumber aplikasi tersebut (Fahrezi dkk., 2022). Pendekatan *Black Box Testing* ini menekankan pada pemeriksaan input dan output aplikasi untuk memverifikasi bahwa setiap fitur beroperasi sesuai dengan persyaratan yang ditetapkan. Dengan metode ini, pengujian dilakukan dari perspektif pengguna akhir, yang memungkinkan identifikasi kesalahan atau kekurangan yang mungkin tidak terdeteksi dari sisi pengembang, serta memastikan kualitas dan keandalan aplikasi sesuai tujuan yang diinginkan. Tahapan pengujian perangkat lunak dengan metode *Black Box Testing* dapat dilihat pada tabel 3.1. Proses ini melibatkan berbagai skenario uji untuk mengidentifikasi potensi bug atau kesalahan fungsi dalam aplikasi.

Tabel 3. 1
Uji Coba Sistem

Fitur yang Diuji	Jenis Fitur	Kebutuhan	Hasil yang Diharapkan
Enkripsi	1. Tampilan Input File.	Pengguna dapat mengunggah file PDF	1. File PDF yang diunggah akan

	2. Tampilan Input Kunci. 3. Tampilan Input Gambar.	dan gambar cover dengan memverifikasi bahwa kedua file tersebut dalam format yang tepat dan memenuhi kriteria ukuran serta resolusi yang diperlukan. Harus ada input teks untuk memasukkan kunci enkripsi yang aman.	dienkripsi menggunakan kunci yang dimasukan. 2. File PDF yang telah dienkripsi akan diembed ke dalam gambar cover yang dipilih menggunakan teknik steganografi LSB, tanpa mengganggu kualitas visual gambar. 3. Gambar cover dengan file PDF yang tersembunyi siap untuk disimpan atau dikirim, memastikan bahwa data terenkripsi terlindungi selama transmisi atau penyimpanan.
Dekripsi	1. Tampilan Input Gambar hasil Stego. 2. Tampilan Input Kunci.	Pengguna dapat mengunggah gambar cover yang mengandung file PDF terenkripsi. Sistem memvalidasi bahwa file yang diunggah adalah gambar dalam format yang didukung dan memeriksa integritas gambar untuk memastikan tidak ada kerusakan data. Harus ada input teks untuk pengguna memasukkan kunci dekripsi yang harus sama dengan kunci yang digunakan pada saat enkripsi. Sistem harus memastikan bahwa kunci yang dimasukkan benar dan valid untuk	1. Gambar cover akan diproses untuk mengekstrak data PDF yang tersembunyi menggunakan teknik steganografi LSB. Data PDF yang diekstrak kemudian akan didekripsi .menggunakan kunci yang diberikan. 2. File PDF yang didekripsi siap untuk diakses atau disimpan oleh pengguna, memastikan pemulihan data yang aman dan akurat.

	proses dekripsi yang sukses.

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

Evaluasi dilakukan dengan menganalisis data dari serangkaian percobaan yang telah terkumpul. Proses ini bertujuan untuk menarik kesimpulan mengenai kesesuaian produk yang dikembangkan dengan tujuan penelitian yang telah ditetapkan. Dalam konteks ini, evaluasi bertindak untuk memastikan bahwa solusi keamanan yang telah dibuat benar-benar efektif dalam melindungi data medis. Hasil pengujian akan dievaluasi berdasarkan nilai korelasi Pearson, MSE, dan PSNR untuk menentukan keberhasilan algoritma dalam menjaga integritas dan kerahasiaan data medis.

3.7 Mengkomunikasikan Hasil Uji (*Comunicating the testing result*)

Hasil dari analisis data kemudian disimpulkan untuk selanjutnya dilaporkan sebagai laporan tertulis skripsi dan dikomunikasikan dalam bimbingan skripsi dihapadapan dosen pembimbing. Proses komunikasi hasil analisis data ini memuat berbagai informasi mengenai proses dari desain dan pengembangan sistem, kontribusi system yang dikembangkan dalam penelitian terhadap ranah medis, keterkaitan antara penelitian yang dilakukan dengan penelitian-penelitian sebelumnya.