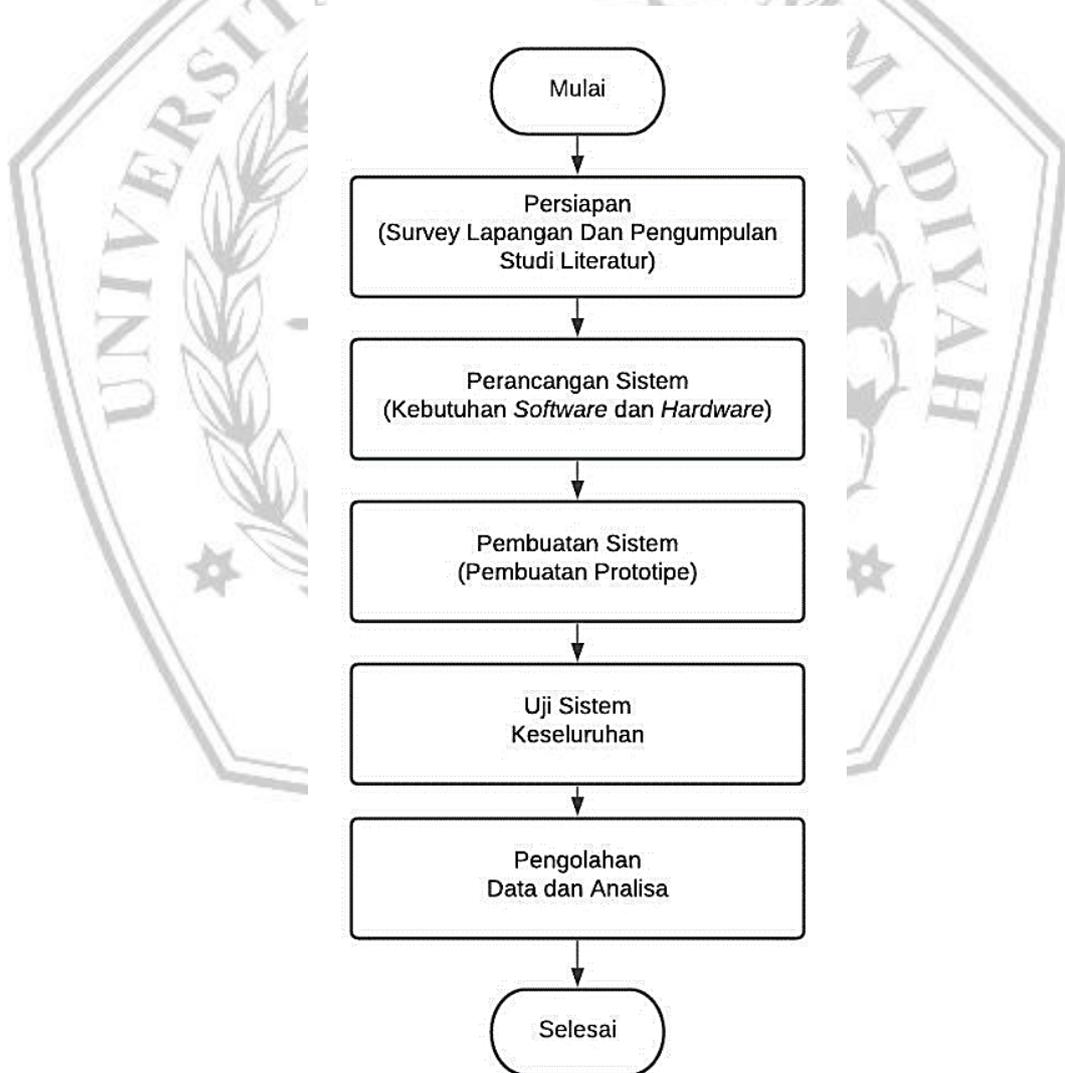


BAB III METODE PENELITIAN

3.1 Metode Penelitian

Pada bagian ini akan diuraikan terkait metode yang digunakan dalam merancang sistem lemari penyimpanan dengan sistem deteksi wajah, NFC, dan pin password sebagai validasi keamanan. Perancangan sistem ini bertujuan untuk membuat suatu sistem lemari penyimpanan yang aman dan canggih. Adapun upaya dalam mencapai tujuan dan hasil yang diinginkan maka diperlukan sebuah metode agar penelitian yang dilakukan dapat berjalan secara sistematis dan terencana. Untuk itu guna merealisasikan sistem yang dirancang maka digunakan metode atau alur penelitian yang ditunjukkan pada gambar 3.1.



Gambar 3. 1 Metode Penelitian

Dari Gambar 3.1 dapat dijelaskan bahwa pengerjaan penelitian ini diawali dengan tahapan persiapan yaitu tahapan pencarian data lapangan dengan melakukan survey secara langsung dan pengumpulan data melalui studi literatur. Survei lapangan dilakukan untuk mengidentifikasi praktik saat ini dan kebutuhan pengguna, sementara studi literatur melibatkan tinjauan karya akademis dan profesional untuk menetapkan dasar teoretis penelitian.

Setelah survei dan data didapatkan langkah selanjutnya adalah perancangan sistem yang merupakan proses menentukan kebutuhan software dan hardware yang diperlukan. Pada tahap ini melibatkan penguraian kebutuhan fungsional dan non-fungsional sistem, dan mencakup pengembangan spesifikasi teknis dan arsitektur sistem lemari pengaman.

Setelah rancangan selesai dibuat, selanjutnya adalah tahap pembuatan sistem yang melibatkan pengembangan prototipe. Prototipe ini merupakan implementasi awal dari sistem yang dirancang untuk menguji konsep, desain, dan asumsi. Prototipe bisa berupa model kerja yang dapat menunjukkan bagaimana sistem akhir akan beroperasi dan sering kali digunakan untuk mendapatkan umpan balik awal dari pengguna.

Setelah prototype berhasil dirancang, langkah selanjutnya adalah pengujian sistem secara keseluruhan. Pada tahap ini, sistem yang telah dikembangkan diuji secara menyeluruh untuk memastikan bahwa semua komponen berfungsi sesuai dengan persyaratan yang telah ditetapkan. Pengujian ini dapat mencakup serangkaian tes fungsional, tes kinerja, dan tes keamanan untuk memvalidasi keseluruhan sistem.

Tahap terakhir dari penelitian yang dilakukan adalah tahap pengolahan data dan analisa. Data yang dikumpulkan selama pengujian sistem diolah dan dianalisis untuk mengevaluasi kinerja, efektivitas, dan efisiensi sistem. Analisis ini dapat menghasilkan wawasan penting yang akan digunakan untuk memperbaiki sistem sebelum diluncurkan secara resmi.

3.2 Studi Literatur

Studi literatur merupakan fondasi kritis yang memfasilitasi pemahaman teoritis mendalam serta aplikasi praktis dalam pengembangan tugas akhir. Studi Literatur ini berfungsi untuk mempelajari teori penunjang yang mendukung dalam pengerjaan tugas akhir, seperti pemilihan komponen yang akan digunakan, penggunaan software pendukung, serta pengintegrasian seluruh sistem. Sehingga penulis akan lebih paham mengenai bagaimana cara mengerjakan dan dari mana kah penulis harus memulai. Sumber Literatur tidak hanya berasal dari Buku, namun terdapat dalam bentuk Journal, Paper, Referensi dari web internet dan lain sebagainya. Adapun beberapa sumber literatur lain yang dibutuhkan dalam mendukung penelitian yang dilakukan harus memuat informasi sebagai berikut :

1. Penelitian yang mengkaji sistem keamanan komprehensif, termasuk tetapi tidak terbatas pada lemari pengaman berteknologi tinggi, sistem autentikasi yang menggunakan kredensial berupa password dan pengenalan wajah (face ID).
2. Studi tentang penerapan sistem pengenalan wajah dengan memanfaatkan openCV, yang mencakup ruang lingkup pendeteksian dan klasifikasi pengguna melalui fitur wajah.
3. Analisis mendetail karakteristik dan mekanisme kerja dari sensor-sensor kunci, seperti sensor kamera, NFC, dan komponen pendukung lainnya seperti selenoid dan buzzer, yang harus dijelaskan dengan tepat.
4. Eksplorasi karakteristik sirkuit elektronik yang digunakan dalam sistem penguncian pintu, termasuk sirkuit elektronik pada NFC dan keypad, serta mekanisme pemicu sistem buzzer.

Terkait hal tersebut, referensi yang kredibel dapat ditemukan melalui berbagai sumber literatur seperti buku, jurnal ilmiah, artikel, prosiding, dan laporan penelitian. Selain itu eksperimen dan pendapat dari profesional, juga memberikan kontribusi penting untuk validitas informasi. Hasil dari proses studi literatur menghasilkan serangkaian referensi yang sesuai dengan permasalahan masalah, yang kemudian akan dimasukkan dalam laporan penelitian akhir.

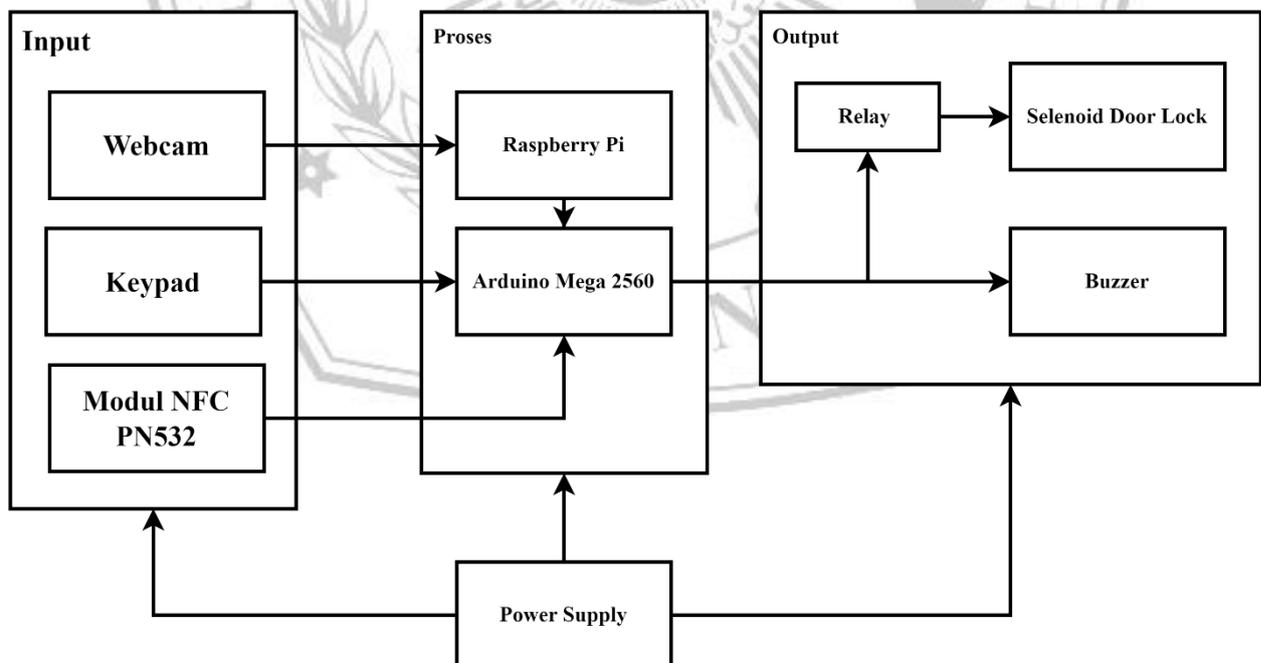
3.3 Perancangan Sistem

Perancangan sistem adalah proses yang melibatkan pengembangan konsep dan langkah-langkah metodis yang akan diikuti selama pembuatan aplikasi. Ini termasuk pemetaan arsitektur sistem, desain antarmuka pengguna, pemilihan algoritma yang tepat, dan penentuan teknologi yang akan digunakan. Proses perancangan ini bersifat abstrak dan konseptual, berfungsi sebagai cetak biru yang akan mengarahkan aktivitas pengembangan.

3.3.1 Perancangan Hardware

Perancangan perangkat keras bertujuan untuk merealisasikan sistem lemari pengaman yang sesuai dengan harapan serta mempermudah langkah pembuatan sistem. Perancangan perangkat keras akan membuat jalannya penelitian menjadi lebih efisien dan memiliki tingkat keberhasilan yang tinggi. Tahap perancangan perangkat keras pada penelitian yang dilakukan meliputi perencanaan spesifikasi sistem, diagram blok sistem, desain perangkat keras, dan perancangan elektrik yang dijabarkan sebagai berikut.

Pada rancangan perangkat keras terdapat blok diagram untuk mendukung berjalannya sistem. Dimana blok diagram terdiri dari input, proses dan output. Blok Diagram pada penelitian ini dapat dilihat pada Gambar 3.2 berikut.



Gambar 3. 2 Diagram Block Sistem

Diagram blok yang ditampilkan pada Gambar 3.2 mengilustrasikan arsitektur sistem untuk mekanisme penguncian pintu yang dioperasikan melalui berbagai metode autentikasi. Berikut adalah penjelasan yang lebih rinci dan terstruktur dari fungsi masing-masing komponen dalam sistem tersebut :

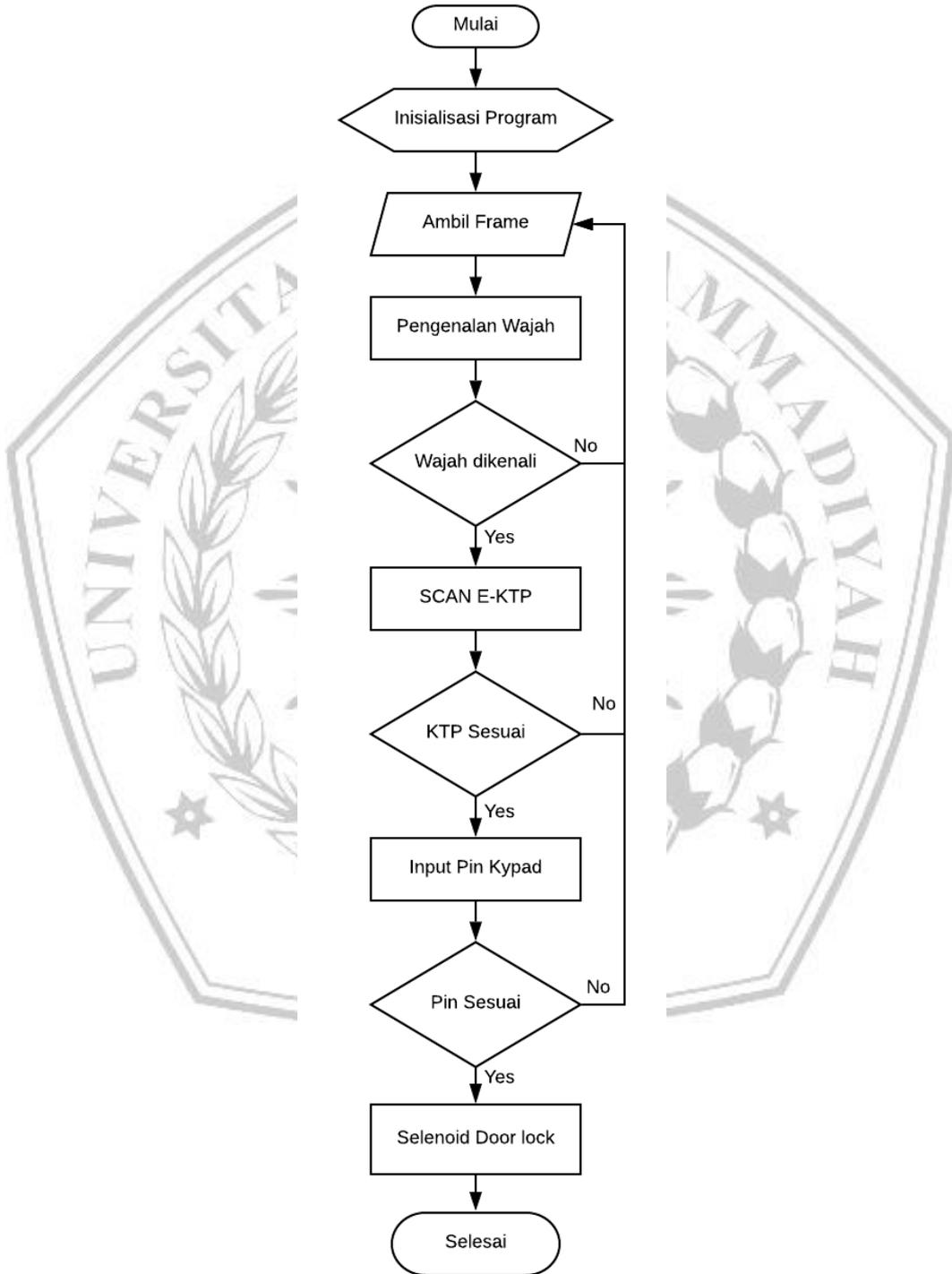
1. Webcam: Perangkat ini berperan sebagai alat pengambilan citra visual, khususnya wajah pengguna. Citra yang diambil ini akan digunakan dalam proses pengenalan wajah melalui teknik pengolahan citra.
2. Raspberry Pi: Mikrokontroler ini bertindak sebagai unit pemrosesan inti dalam sistem. Raspberry Pi mengolah data citra yang diperoleh dari webcam dengan menggunakan algoritma Haar Cascade untuk deteksi wajah. Haar Cascade adalah metode yang efisien untuk identifikasi objek wajah dalam citra real-time.
3. Arduino Mega 2560: Mikrokontroler ini digunakan sebagai pengontrol pusat untuk input dan output sistem. Arduino Mega 2560 mengelola komunikasi antara Raspberry Pi dan perangkat output seperti solenoid door lock, serta menyediakan interface untuk input tambahan seperti keypad dan modul NFC.
4. Modul NFC PN532: Modul ini menyediakan metode autentikasi kedua melalui komunikasi near-field (NFC). Dalam konteks ini, modul NFC digunakan untuk membaca data dari E-KTP sebagai kunci alternatif untuk membuka solenoid door lock.
5. Keypad: Keypad berfungsi sebagai metode autentikasi ketiga. Pengguna dapat memasukkan kode pin melalui keypad untuk mengaktifkan mekanisme pembukaan solenoid door lock.
6. Solenoid Door Lock: Ini adalah aktuator mekanis yang terhubung dengan Arduino Mega 2560. Setelah autentikasi berhasil dilakukan melalui salah satu metode input (pengenalan wajah, NFC, atau kode pin), Arduino Mega akan mengirim sinyal untuk mengaktifkan solenoid yang akan membuka kunci pintu.
7. Buzzer: Sebuah buzzer juga terhubung dengan sistem dan dikendalikan oleh Arduino Mega 2560. Buzzer ini dapat mengeluarkan sinyal suara sebagai indikator dari berbagai event dalam sistem, seperti pemberitahuan keberhasilan atau kegagalan autentikasi.

Pada dasarnya, setiap komponen ini terhubung ke mikrokontroler dan berkomunikasi melalui pin I/O untuk melaksanakan fungsi tertentu dalam sistem. Mikrokontroler akan diprogram untuk membaca input dari sensor atau perangkat input (seperti keypad atau NFC), dan kemudian memproses data tersebut untuk mengambil tindakan, seperti mengaktifkan solenoid atau buzzer sebagai respons. Untuk lebih detail, berikut penjelasan untuk pin I/O yang digunakan dalam perancangan sistem.

1. Webcam terhubung dengan sistem melalui port USB yang terhubung dengan Raspberry Pi, Raspberry Pi bertugas untuk menjalankan algoritma pengolahan citra menggunakan OpenCV untuk deteksi wajah atau pemrosesan gambar lainnya.
2. Raspberry Pi dan Arduino Mega2560 terhubung melalui pin UART yang ada pada masing-masing perangkat. Pada sistem yang dirancang pin UART yang digunakan berada pada pin 16 (TX) dan pin 17 (RX) pada Arduino.
3. Keypada terhubung ke pin digital pada Arduino Mega 2560 pada pin D2-D9. Setiap tombol pada keypad akan mengirim sinyal digital ke pin yang terkait ketika ditekan. Fungsi I/O ini digunakan untuk menerima input dari pengguna sebagai metode autentikasi.
4. Solenoid Door Lock terhubung dengan relay yang mana salah satu pin trigernya ke salah satu pin output digital yaitu pin D10 yang mampu memberikan atau memutus arus yang cukup untuk mengaktifkan solenoid. Fungsi I/O ini digunakan untuk mengontrol penguncian atau pembukaan mekanis pintu.
5. Modul NFC PN532 terhubung ke pin komunikasi, kemungkinan menggunakan protokol komunikasi Serial atau I2C/SPI. Modul ini menggunakan I/O untuk berkomunikasi dengan mikrokontroler dan memproses identifikasi dari tag NFC, seperti E-KTP.
6. Buzzer terhubung ke pin output digital D11 yang dapat menghasilkan PWM (Pulse Width Modulation) untuk mengontrol buzzer. Fungsi I/O ini digunakan untuk memberikan umpan balik audio berdasarkan berbagai kondisi sistem, misalnya konfirmasi pembukaan kunci.

3.3.3 Perancangan Flowchart Sistem

Pada rancangan perangkat lunak terdapat flowchart dimana flowchart adalah alur pada program yang telah dibuat. Flowchart dapat dilihat pada Gambar 3.4 berikut ini.



Gambar 3.4 Flowchart Sistem

Gambar 3.4 menggambarkan proses operasional dari sistem pengamanan lemari dengan implementasi metode pengenalan wajah, otentikasi berbasis e-KTP, dan input PIN melalui keypad. Sistem ini dirancang untuk mengintegrasikan teknologi biometrik dan keamanan elektronik untuk meningkatkan keamanan.

Proses dimulai dengan inialisasi program yang mempersiapkan sistem untuk operasi berikutnya. Kamera, sebagai perangkat input utama, mengambil gambar pengguna secara real-time. Gambar ini selanjutnya diproses menggunakan perangkat lunak OpenCV yang terintegrasi dengan algoritma Haar Cascade untuk mengidentifikasi apakah fitur wajah dalam gambar sesuai dengan parameter yang telah ditentukan sebelumnya. Jika tidak terdapat kesesuaian, sistem tidak akan melanjutkan ke langkah berikutnya, sehingga menjamin bahwa hanya individu yang wajahnya terdaftar yang dapat memicu proses otentikasi selanjutnya.

Dalam fase berikutnya, pembacaan e-KTP dilakukan melalui teknologi NFC. Sistem telah dirancang untuk memberikan hingga tiga kesempatan bagi pengguna untuk memindai e-KTP yang telah terdaftar dalam database sistem. Kegagalan dalam pembacaan e-KTP dalam ketiga percobaan tersebut akan menyebabkan sistem kembali ke fase awal pengambilan gambar.

Setelah validasi e-KTP berhasil, langkah terakhir dari prosedur keamanan ini adalah input 4 digit PIN melalui keypad. Sistem ini memberikan pengguna tiga kesempatan untuk memasukkan PIN yang benar. Jika pengguna gagal dalam ketiga kesempatan tersebut, maka alarm buzzer akan terpicu sebagai indikator kegagalan otentikasi, dan sistem akan otomatis mengulang siklusnya kembali ke tahap pengambilan gambar wajah.

Keseluruhan prosedur ini menggambarkan sebuah sistem keamanan yang robust, menggabungkan teknologi pengenalan wajah dengan verifikasi identitas dua faktor untuk memastikan bahwa hanya individu yang berwenang yang dapat mengakses lemari penyimpanan. Ini merupakan contoh evolusi dalam sistem keamanan yang mengadopsi pendekatan multi-modal untuk autentikasi pengguna, meningkatkan keandalan dan mengurangi risiko akses tidak sah.

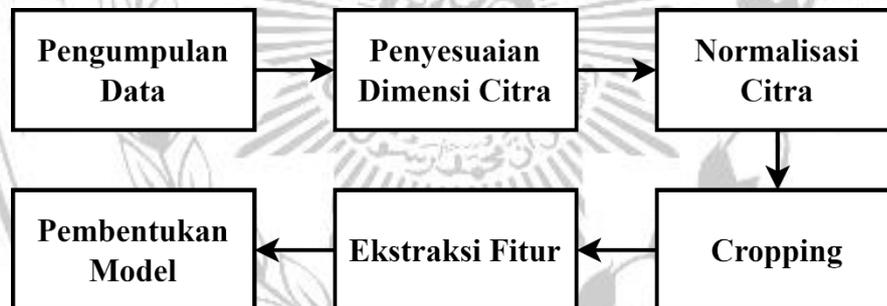
3.3.4 Perancangan Algoritma Deteksi Wajah

Pada perancangan algoritma deteksi wajah tersusun atas beberapa langkah perancangan mulai dari persiapan data dan Pre-prosesing data dan pembentukan model algoritma yang dijabarkan sebagai berikut.

1. Tahap persiapan data

Tahap persiapan data merupakan langkah awal yang dilakukan guna mendapatkan dan memproses data hingga dapat diimplementasikan kedalam model algoritma yang dirancang. Tahap awal dalam persiapan data adalah pengumpulan dataset dengan cara mengupulkan data gambar pengguna sistem dalam hal ini foto wajah pengguna sebanyak mungkin sehingga mendapatkan jumlah data yang cukup untuk proses generateing algoritma.

Pada tahap persiapan data akan dilakukan beberapa langkah seperti mengekstraksi data sekaligus melakukan pemrosesan data dari dataset untuk menghapus atau memproses gambar sehingga memiliki dimensi atau pixel yang sesuai yang dapat mempengaruhi perancangan algoritma. Gambar 3.5 menunjukkan alur persiapan data hingga pada tahap pembentukan model.



Gambar 3.5 Tahap persiapan data

Dari diagram diatas maka dapat dijabarkan tiap langkah persiapan data sebagai berikut.

- Pengumpulan data : Mengumpulkan sejumlah besar citra wajah dari pengguna sistem untuk membangun dataset yang komprehensif.
- Penyesuaian dimensi citra : Mengubah ukuran semua citra ke dimensi yang konsisten yang sesuai dengan input algoritma yang akan digunakan.
- Normalisasi citra : Menyesuaikan distribusi intensitas pixel dalam citra melalui teknik seperti equalisasi histogram.

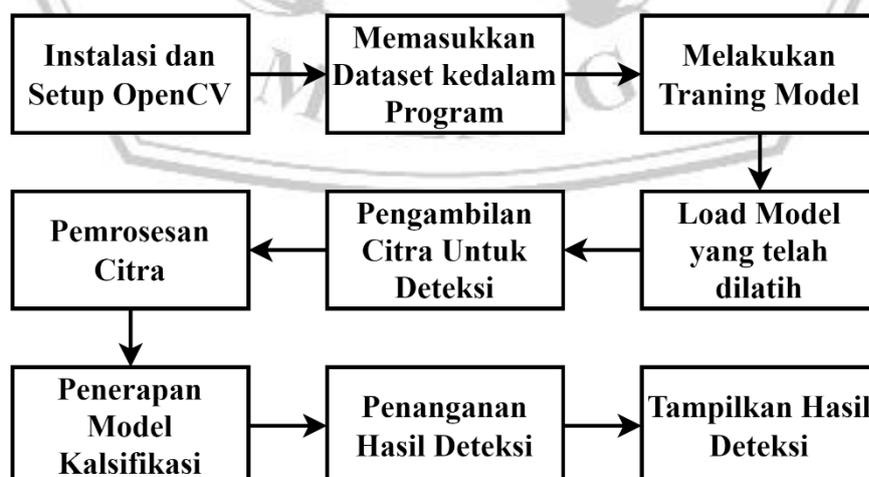
- d. Cropping : Memotong citra untuk fokus pada area wajah dan menghilangkan bagian latar belakang yang tidak perlu.
- e. Ekstraksi fitur : Mengidentifikasi dan mengekstrak fitur yang relevan dari citra untuk digunakan dalam algoritma deteksi wajah.
- f. Pembentukan model : Menggunakan classifier (seperti Haar Cascades atau LBP Cascades) yang telah dilatih sebelumnya untuk mendeteksi wajah dalam citra.

Setiap langkah pada tahap pemrosesan data harus dilakukan dengan hati-hati untuk memastikan bahwa data yang digunakan dalam pelatihan algoritma adalah representatif, relevan, dan berkualitas tinggi untuk mendukung pengembangan solusi deteksi wajah yang akurat dan efektif.

2. Tahap Perancangan model algoritma

Setelah data selesai dilakukan pemrosesan, mulai dari pengumpulan data, penyesuaian data, hingga ekstraksi fitur, langkah selanjutnya adalah membangun model algoritma deteksi wajah. Pada penelitian ini menggunakan framework openCV dengan algoritma (seperti Haar Cascades atau LBP Cascades) yang ada didalam OpenCV secara default.

Untuk merancang sebuah program yang menggunakan classifier seperti Haar Cascades atau LBP Cascades untuk deteksi wajah dalam citra menggunakan OpenCV, berikut adalah tahapan perancangan program deteksi wajah yang ditampilkan pada gambar 3.6.



Gambar 3.6 Alur pembuatan model algoritma

Proses perancangan model algoritma dimulai dengan menginisialisasi dan menginstal openCV pada raspi, Proses ini melibatkan pengaturan lingkungan pengembangan dengan menginstal perpustakaan OpenCV yang menyediakan alat dan fungsi untuk pemrosesan citra dan visi komputer.

Setelah openCV berhasil disiapkan, langkah selanjutnya adalah memasukkan dataset kedalam program. Dataset yang berisi citra wajah dikumpulkan dan dimasukkan ke dalam program. Data ini umumnya meliputi banyak citra wajah positif (yang menampilkan wajah) dan negatif (yang tidak menampilkan wajah), yang akan digunakan untuk melatih model Haar Cascade.

Setelah dataset dimasukan, langkah selanjutnya adalah mentarining model. Dalam tahap ini, model Haar Cascade dilatih menggunakan dataset yang telah dimasukkan. OpenCV menyediakan alat untuk pelatihan model Haar Cascade, yang akan menghasilkan file classifier (seringkali dalam format XML) setelah proses pelatihan selesai.

Setelah model selesai dibangun, selanjutnya adalah melakukan load model kedalam program. Model Haar Cascade yang telah dilatih (file classifier XML) dimuat ke dalam program. Ini memungkinkan program untuk menggunakan model tersebut dalam mendeteksi wajah pada citra yang diambil.

Selanjutnya program akan mengambil citra untuk deteksi secara realtim. Dalam proses ini citra diambil secara real-time (misalnya, dari kamera atau webcam) atau diimpor dari sebuah file untuk deteksi wajah. Proses ini menyediakan data input untuk model Haar Cascade yang telah dilatih.

Langkah berikutnya yaitu memproses citra, pada langkah ini citra yang akan digunakan untuk deteksi wajah diproses, yang biasanya termasuk konversi citra ke skala abu-abu dan normalisasi. Pra-pemrosesan ini penting untuk meningkatkan akurasi deteksi wajah.

Setelah data masukan selesai didapatkan, berikutnya Model yang telah dilatih diterapkan pada citra yang telah diproses. OpenCV menggunakan fungsi `detectMultiScale` untuk mengidentifikasi wajah pada citra. Setiap wajah yang terdeteksi akan diberi kotak pembatas (bounding box). Hasil dari deteksi kemudian dilakukan penanganan seperti untuk membuka door lock atau sejenisnya, kemudian data hasil deteksi ditampilkan melalui antar muka pada python OpenCV.

3.4 Desain Sistem

3.4.1 Spesifikasi Sistem

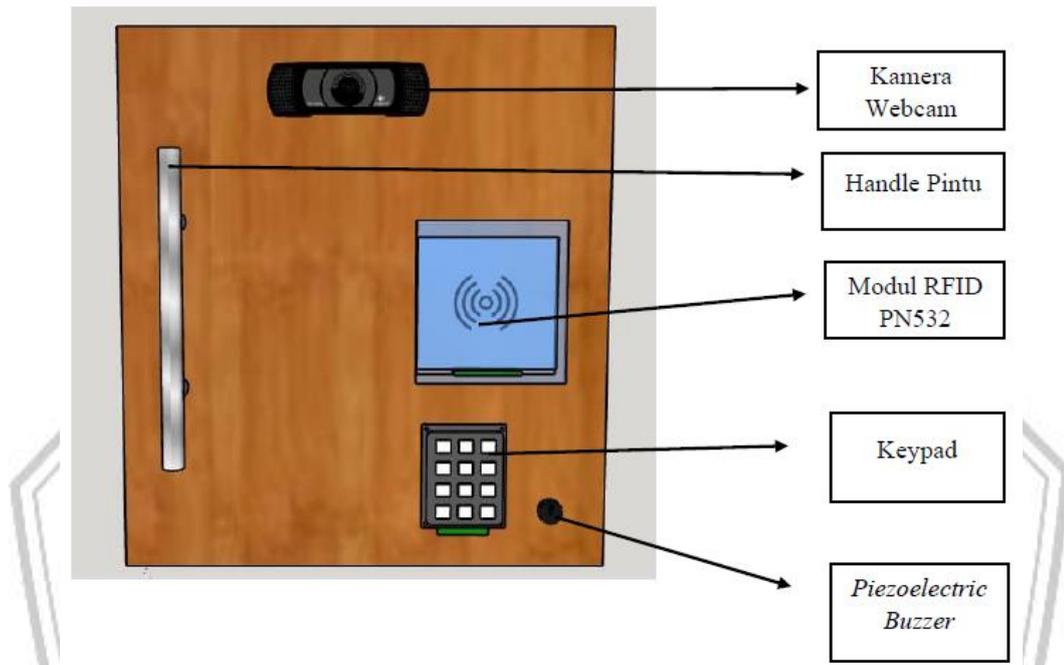
Spesifikasi sistem keamanan lemari penyimpanan yang terintegrasi dengan teknologi pengenalan wajah, otentikasi e-KTP berbasis NFC, dan keypad untuk input PIN didesain dengan memperhatikan keandalan dan integritas keamanan. Berikut ini adalah prinsip kerja dan spesifikasi sistem yang dirancang dimana pada prinsipnya sistem yang dirancang bekerja dengan cara sebagai berikut. Sistem diinisialisasi dengan memuat semua komponen operasional, termasuk memulai kamera, memuat algoritma deteksi wajah, dan menyiapkan sensor NFC dan keypad. Kamera mengambil gambar wajah pengguna secara real-time. Algoritma Haar Cascade dalam OpenCV memproses gambar untuk mendeteksi wajah yang sesuai dengan set parameter yang telah ditentukan dalam database sistem.

Modul NFC menunggu pengguna untuk memindai e-KTP. Sistem membandingkan data dari chip pada e-KTP dengan database yang ada untuk validasi. Pengguna memasukkan 4 digit PIN melalui keypad. Sistem memverifikasi PIN yang dimasukkan dengan informasi yang telah disimpan sebelumnya. Apabila deteksi wajah, pembacaan e-KTP, dan input PIN valid, sistem akan mengaktifkan solenoid untuk membuka kunci lemari penyimpanan.

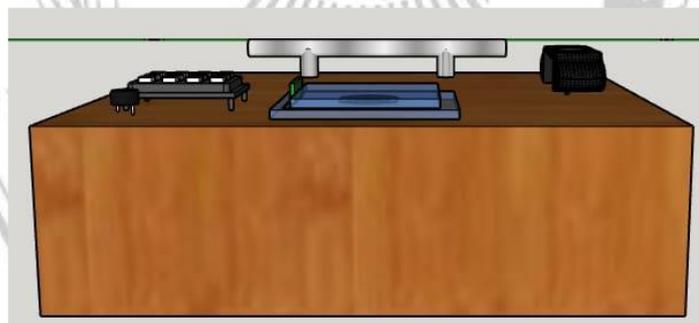
Sistem keamanan lemari penyimpanan yang terintegrasi dirancang dengan menggunakan komponen-komponen canggih untuk memastikan keandalan dan integritas. Sebuah kamera digital beresolusi tinggi terhubung ke Raspberry Pi, yang bertindak sebagai otak pemrosesan citra dengan menggunakan OpenCV dan algoritma Haar Cascade untuk fungsi pengenalan wajah. Arduino Mega 2560 digunakan sebagai pusat kontrol yang mengkoordinasikan input dari berbagai modul seperti pembaca NFC untuk otentikasi e-KTP dan keypad untuk input PIN pengguna. Setelah semua tahapan verifikasi berhasil dilalui, Arduino akan mengaktifkan mekanisme kunci solenoid untuk memberikan akses ke lemari penyimpanan. Sistem ini juga dilengkapi dengan buzzer sebagai sistem alarm untuk indikasi keamanan.

3.4.2 Desain Perangkat Keras

Desain sistem ini adalah desain per angkat yang dapat membantu dalam perancangan hardware. Desain ini berbentuk kursi pada umumnya tetapi telah dipasang sensor pada dudukan dan diatas perangkat. Desain dapat dilihat pada Gambar dibawah ini.



Gambar 3.7 Desain tampak depan



Gambar 3.8 Desain tampak samping

Desain lemari penyimpanan ini terbuat dari bahan acrylic dengan memiliki panjang 50 cm, lebar 50 cm, dan tinggi 50 cm. Dalam desain lemari penyimpanan ini terlihat beberapa komponen antara lain Handle Pintu, Webcam Logitech C270, Modul RFID PN532, Keypad 3x4, dan Piezoelectric Buzzer dengan masing-masing penempatan sesuai gambar diatas.

3.5 Pengujian Sistem

Evaluasi dan pengujian dilakukan untuk mendapatkan data dan kesimpulan terhadap sistem yang diterapkan pada Tugas Akhir ini dan setelah semua komponen pada sistem yang dirancang sudah terhubung sesuai dengan diagram blok serta perangkat lunak sistem sudah selesai dibuat, maka dilakukan pengujian dan analisis kinerja alat. Tahapan metode pengujian yang akan dilakukan adalah sebagai berikut.

- 1) Pengujian Arduino Mega 2560
- 2) Pengujian Webcam
- 3) Pengujian Keypad
- 4) Pengujian Modul NFC
- 5) Pengujian Sistem Deteksi Wajah
- 6) Pengujian Keseluruhan Sistem

