

BAB 2

DASAR TEORI

2.1 KAJIAN PUSTAKA

Penelitian [6] membahas tentang mengimplementasikan sebuah keamanan yang menerapkan keamanan ganda berupa *face recognition* dan *fingerprint* dan sudah menggunakan sensor getar jika dicuri atau dibawa oleh orang lain. Mikrokontroler dapat berfungsi untuk mengendalikan suatu sistem secara terprogram, *fingerprint* berfungsi untuk membuka pintu brankas, dan Sensor *Face Recognition* sebagai keamanan kedua, GPS berfungsi untuk melacak keberadaan brankas yang telah dipindahkan dari tempat semula di mana brankas tersebut diletakkan. SIM800L berfungsi sebagai pengirim data melalui GPS, dimana data tersebut diterima sensor getar yang berfungsi sebagai *SMS gateway*. *Buzzer* berfungsi untuk memberikan informasi atau kode berupa bunyi. Dalam penggunaan selenoid dimana berfungsi untuk membuka pintu brankas, dengan menggunakan LCD pada perancangan *system* ini, terbukti dapat menampilkan informasi yang akan ditampilkan sesuai dengan perintah.

Penelitian [7] membahas tentang penggunaan metode yang digunakan *Face Recognition* dan ESP32-Cam. Sistem *Face Recognition* harus mengambil sampel wajah terlebih dahulu untuk dijadikan data sampel. *Face Recognition* bekerja ketika ada seseorang melakukan *scan* wajah, maka citra wajah akan diproses untuk menentukan dikenali atau tidak. Sehingga ketika ingin terus saling terkoneksi, maka keduanya harus saling terhubung ke internet agar sistem brankas dapat mengirimkan notifikasi kapanpun.

Penelitian [8] membahas tentang menyempurnakan perancangan sistem pintu otomatis. Pengujian sistem ini diawali dengan menghubungkan ESP32-Cam ke hotspot perangkat Android. Setelah terhubung, sistem melakukan deteksi wajah. Jika wajah terdeteksi, kunci solenoid akan terbuka secara otomatis selama 5 detik. Namun, jika wajah tidak terdeteksi, sistem akan memberikan pemberitahuan bahwa wajah tidak terbaca. Hasil pengujian menunjukkan bahwa sistem pintu otomatis yang menggunakan sensor wajah dan kamera ESP32Cam bekerja dengan akurasi dan kecepatan yang baik. Dengan demikian, sistem ini

dapat meningkatkan keamanan dan memberikan kemudahan bagi pemilik rumah dalam mengontrol pintu secara otomatis.

Penelitian [9] menggunakan metode yang berbasis *web* yang menggunakan sensor *fingerprint* dan *passcode* sebagai autentikasinya. Penelitian ini telah melakukan pengujian dengan *black box testing* yang merupakan suatu pendekatan pengujian perangkat lunak yang fokus pada perilaku sistem dari luar tanpa memperhatikan detail internalnya. Tujuan utama dari pengujian ini adalah untuk memastikan bahwa brankas hanya dapat dibuka dengan memasukkan *passcode* yang valid dan sidik jari yang terdaftar dalam sistem. Dengan menggunakan metode ini, pengujian akan dilakukan untuk memverifikasi apakah sistem beroperasi dengan baik dan sesuai dengan harapan, tanpa memerlukan pemahaman mendalam tentang bagaimana sistem bekerja secara internal.

Penelitian [10] membahas tentang sistem keamanan aplikasi rangkaian berbasis mikrokontroler dengan menggunakan metode OTP (*One Time Password*) yang menggunakan NodeMCU, *Keypad*, baterai, *relay*, selenoid, dan aplikasi android. Kode otp akan bekerja untuk membuka brankas yang dikirimkan ke aplikasi android agar keamanan lebih terjaga, berdasarkan hasil pengujian, Tingkat keamanan lemari brankas dengan metode otp mencapai 95%, kemudian *delay* 5-10 detik pada kecepatan internet sekitar 34-56 Kbps (12). Metode OTP salah satu metode yang sangat cocok untuk keamanan brankas saat ini.

Penelitian [11] membahas tentang pengembangan dan perancangan sebuah sistem keamanan alternatif berbasis *smarthome* menggunakan *QR Code* dengan menggunakan mikrokontroler ESP32. Tujuan dari penelitian ini adalah mengembangkan sistem keamanan yang terjangkau dan efisien untuk rumah dan perangkat elektronik. *QR Code* digunakan sebagai kunci pintu yang tidak mudah dibobol, serta untuk mengaktifkan dan mengendalikan perangkat elektronik menggunakan *smart relay*. Berdasarkan hasil pengujian didapatkan bahwasanya hasil persentase *error* tegangan sampel pengujian kalibrasi sensor tegangan (V) sebesar 0.03%. sedangkan hasil persentase sampel pengujian kalibrasi sensor arus (I) didapatkan sebesar 0.31%.

Penelitian [12] membahas tentang sistem keamanan pintu brankas yang menggunakan sensor sidik jari. Sistem ini terdiri dari perangkat lunak dan

perangkat keras Arduino Uno, sensor sidik jari, *buzzer*, *solenoid* pintu, dan LCD. Sistem beroperasi dengan mendeteksi sidik jari pengguna atau pemilik brankas. Jika terdeteksi, solenoid membuka pintu. Jika tidak, pintu tetap terkunci, dan alarm dibunyikan. Brankas yang berisi barang berharga seperti sertifikat, uang, dan emas aman dengan sistem ini.

Penelitian [13] membahas tentang permasalahan yang sering terjadi di dalam gedung perkuliahan, perkantoran, tempat wisata dengan mengimplementasikan perangkat *E-Locker* yang menggunakan *QR Code* sebagai sistem pemicu kunci dan monitoring melalui *website*, yang berbasis pada teknologi *Internet of Things* (IoT). Perangkat *E-Locker* ini menggunakan *QR Code* sebagai mekanisme untuk membuka kunci *locker*. Pengguna diharuskan memindai *QR Code* yang terpasang pada *locker* menggunakan aplikasi Android. Setelah *QR Code* cocok, proses pembukaan *locker* akan diproses oleh mikrokontroler NodeMCU. Solenoid digunakan sebagai penguncian dan pembukaan pintu *locker*. Selain itu, terdapat sebuah *website* yang digunakan sebagai pusat monitoring dan kontrol *admin E-Locker*. Melalui *website* ini, admin dapat melihat status penggunaan *locker*, jumlah pengguna terdaftar, pendapatan dan penggunaan *locker* per bulan, validasi *top up* pengguna, data pengguna *E-Locker*, serta melihat riwayat pemesanan.

Tabel 2.1 Rangkuman Penelitian Terdahulu

Judul, Penulis (Tahun)	Bahan Penelitian	Hasil Penelitian
Kajian Rancang Bangun Alat Sistem Keamanan Pada Brankas Perhiasan Menggunakan <i>Face Recognition</i> Dan <i>Fingerprint</i> Berbasis Arduino Mega2560 Qadir Aziz, dkk (2023)	<ul style="list-style-type: none"> - Arduino Mega2560 - Modul Sensor <i>Fingerprint</i> - <i>Pushbutton</i> - Sensor <i>Facerecognition</i> - Sim800l - Sensor Getar - Lcd 16x2 - <i>Buzzer</i> - <i>Smartphone</i> Android 	<ul style="list-style-type: none"> - Penelitian menggunakan pengenalan wajah dan sidik jari - Sistem dilengkapi dengan sensor getar - GPS digunakan untuk melacak lokasi - Modul SIM800L digunakan untuk mengirimkan melalui GPS
Sistem Monitoring Keamanan Brankas Menggunakan <i>Face Recognition</i> Berbasis Mikrokontroler ESP32-Cam. Evindina Putra lumbanraja, Saniman dan Tugiono (2023)	<ul style="list-style-type: none"> - ESP32-Cam - Motor Servo - <i>Smartphone</i> - <i>Blynk</i> - <i>Buzzer</i> - LED 	<ul style="list-style-type: none"> - Hasil penelitian menunjukkan bahwa <i>face recognition</i> bekerja ketika seseorang melakukan <i>scan</i> wajah - Citra wajah akan diproses untuk menentukan apakah wajah valid atau tidak
Perancangan Sistem Pintu Otomatis menggunakan ESP32-Cam Ahmad Suradi, dkk (2022)	<ul style="list-style-type: none"> - Esp32-Cam - Uart Ttl - <i>Relay Module</i> - <i>Solenoid Doorlock</i> - LED (<i>Light Emitting Diode</i>) - Dc <i>Stepdown</i> 	<ul style="list-style-type: none"> - ESP32-Cam bekerja dengan akurasi yang baik - Sistem menggunakan sensor wajah untuk verifikasi masuk
Sistem Brankas Berbasis <i>Internet Of Things</i> menggunakan Arduino Mega 2560 I Gusti Nade Ngurah Desnanjaya (2022)	<ul style="list-style-type: none"> - <i>Pushbutton</i> - <i>Keypad</i> 4x4 - LCD 16x2 - <i>Fingerprint</i> - LED - <i>Arduino Mega</i> - <i>Buzzer</i> - <i>Solenoid Doorlock</i> - <i>Magnet switch doorlock</i> 	<ul style="list-style-type: none"> - Percobaan sebanyak 5x dengan wajah yang sudah terdaftar dan tidak terdaftar - Sensor dapat membaca perbedaan antara wajah terdaftar dan yang belum terdaftar
Perancangan Sistem Keamanan Aplikasi Pada Lemari Brankas Dengan Menggunakan Metode OTP Aslam Afif, dkk (2021)	<ul style="list-style-type: none"> - NodeMCU ESP8266 - <i>Keypad</i> - <i>Relay</i> - <i>Solenoid</i> 	<ul style="list-style-type: none"> - Hasil pengujian OTP pada lemari brankas adalah 95% - <i>Delay</i> 5-10 detik pada kecepatan internet
Rancang Bangun <i>Smarthome</i> Berbasis QR Code Dengan Mikrokontroler <i>Module</i> ESP32	<ul style="list-style-type: none"> - <i>Adaptor</i> 5V - ESP32 - Arduino Uno 	<ul style="list-style-type: none"> - Hasil pengujian didapatkan bahwa <i>error</i> tegangan pada kalibrasi sensor sebesar

Judul, Penulis (Tahun)	Bahan Penelitian	Hasil Penelitian
Rizky Bayu Santoso, dkk (2021)	<ul style="list-style-type: none"> - <i>Selenoid Doorlock</i> - <i>Sensor PZEM 004T</i> - Modul LM259 - LCD 16x2 - <i>Relay 6 channel</i> 	<ul style="list-style-type: none"> 0,03% - Hasil kalibrasi sensor arus sebesar 0,31%
Rancang Bangun Alat Pengaman Brankas Menggunakan Sensor Sidik Jari Berbasis Arduino Okta Rea Arsyad, Kurnia, Putri Kartika (2021)	<ul style="list-style-type: none"> - Arduino Uno - Sensor sidik jari - <i>Buzzer</i> - <i>Selenoid Doorlock</i> - LCD 	<ul style="list-style-type: none"> - Sistem berfungsi dengan mendeteksi sidik jari pengguna atau pemilik brankas - Jika sidik jari benar, <i>selenoid</i> terbuka - Jika sidik jari salah, <i>selenoid</i> tidak terbuka
Desain Dan Implementasi Perangkat <i>E-Locker</i> Menggunakan <i>QR Code</i> Dan <i>Website Monitoring</i> Berbasis <i>Internet Of Things</i> Nandy Hadiansyah P.N, Rohmat Tulloh S.T., M.T, Ridha Muldina Negara S.T., M.T (2020)	<ul style="list-style-type: none"> - ESP8266 - <i>Relay</i> - <i>Selenoid Doorlock</i> - <i>Magnetic door switch</i> - <i>QR Code</i> 	<ul style="list-style-type: none"> - <i>Website Mylocker</i> sudah berfungsi dengan baik - <i>Delay</i> : 0,84s (<i>large</i>), 0,589s (<i>Medium</i>), 0,856s (<i>small</i>) - <i>Delay website</i> 0,509 detik

2.2 DASAR TEORI

Bagian dasar teori menjelaskan tentang teori-teori yang digunakan dalam penelitian, termasuk metode yang digunakan serta komponen-komponen pendukung lainnya, dasar teori yang digunakan mencakup sebagai berikut :

2.2.1 Brankas

Brankas merupakan sebuah lemari atau kotak besi yang dapat menahan api, seringkali dipakai untuk menjaga barang-barang berharga dari bahaya kebakaran serta pencurian atau pembongkaran, seperti uang, dokumen penting, dan perhiasan. Asal-usul kata "brankas" datang dari bahasa Belanda, di mana "*branden*" berarti membakar dan "*kast*" berarti lemari, secara harfiah merujuk pada lemari yang tahan api. Dalam Bahasa Indonesia, "lemari besi" juga digunakan untuk menyebut lemari yang terbuat dari besi. Brankas memiliki beragam bentuk, termasuk kubus atau silinder, dan tersedia dalam berbagai ukuran serta jenis, mulai dari yang portabel hingga yang dipasang di dinding atau

berukuran besar seperti ruangan. Sistem kunci pengaman brankas dapat dibedakan menjadi dua jenis utama yaitu digital dan analog [14].



Gambar 2.1 Brankas [12]

Gambar 2.1 memperlihatkan sebuah kombinasi dari sistem keamanan brankas dengan sistem digital seringkali dilengkapi dengan kunci analog, dan ada pula yang menggunakan dua jenis kunci analog sekaligus (kunci kombinasi putar dan kunci panjang). Meskipun banyak brankas yang tersedia di toko memiliki berbagai fitur, tidak semuanya akan memenuhi kebutuhan pelanggan untuk melindungi barang berharga mereka. Pencurian brankas dapat dilakukan dengan berbagai cara, seperti penggandaan kunci atau pembobolan pintu. Saat pemilik brankas tidak ada, kejadian ini biasanya terjadi, memungkinkan orang lain untuk mencoba membuka brankas dan mengambil isinya karena dianggap mudah. Situasi ini menunjukkan bahwa keamanan brankas saat ini mungkin belum cukup untuk memberikan rasa aman kepada pengguna [4].

2.2.2 QR Code

QR Code (Quick Response Code) adalah jenis *barcode* dua dimensi yang pertama kali diperkenalkan oleh perusahaan Jepang, Denso Wave, pada tahun 1994. *QR Code* merupakan bentuk evolusi dari *barcode* tradisional yang sering kita temui pada produk-produk. *QR Code* merupakan simbol matriks dua dimensi yang terdiri dari rangkaian kotak persegi yang disusun dalam pola persegi yang lebih besar. Kotak-kotak ini disebut modul. Ukuran pola persegi tersebut akan menentukan versi dari *QR Code* [15].

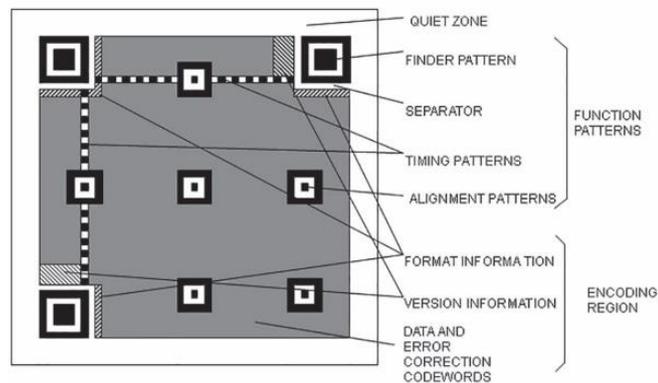


Gambar 2.2 QR Code [12]

Pada gambar 2.2 memperlihatkan sebuah *QR Code* yang memuat berbagai informasi di dalamnya seperti alamat URL, teks hingga nomor telepon, *QR Code* biasanya diletakan di berbagai produk untuk menunjukkan informasi tambahan dari produk tersebut [12]. Bagian-bagian *QR Code* terdiri dari :

A. Struktur *QR Code*

Setiap simbol *QR Code* harus dibuat dari modul persegi disusun dalam susunan persegi beraturan dan terdiri dari fungsi pola dan wilayah *encoding*. Dan seluruh simbolnya akan menjadi dikelilingi di keempat sisinya oleh perbatasan *Quiet Zone*.

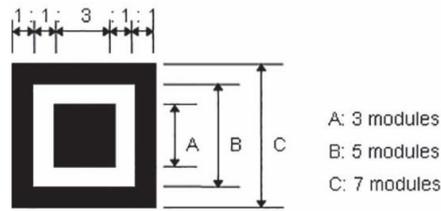


Gambar 2.3 Struktur *QR Code* [16]

Gambar 2.3 memperlihatkan bahwasanya struktur *QR Code* terdiri dari 4 *function patterns* yaitu *finder pattern*, *separator*, *timing pattern*, dan *allignment patterns*.

1. *Finder Pattern* (Pola Pencari)

Finder Pattern merupakan sebuah pola pendeteksi posisi khusus sebagai pola pendeteksi yang terletak pada bagian tiga sudut (kiri atas, kanan atas, dan kiri bawah).



Gambar 2.4 Struktur *Finder Pattern* [16]

Gambar 2.4 menunjukkan stuktur *finder pattern* yang digunakan dalam *QR Code*. Pada pola *finder pattern* ini terdiri dari 3 lapisan modul. Setiap pola *finder pattern* dapat dilihat sebagai tiga pola yang direpresentasikan dalam kotak konsentris dan dirancang dengan kotak gelap luar yaitu 7x7 modul, bagian terang didefinisikan 5x5 modul dan gelap di tengah sebanyak 3x3 modul.

2. *Separator* (Pemisah)

Separator merupakan area yang ditempatkan di antara *finder pattern* dan *encoding region*. *Separator* biasanya terdiri dari modul-modul terang yang berfungsi untuk membantu pemindai *QR Code* dalam mendeteksi dan membaca kode tersebut agar lebih akurat.

3. *Timing Patterns* (Pola Waktu)

Timing Pattern memiliki pengaturan waktu horizontal dan vertikal. Masing-masing terdiri dari baris atau kolom lebar satu modul yang terdiri dari modul gelap dan terang bergantian, dimulai dan diakhiri dengan modul gelap. Pola pengaturan waktu horizontal ditempatkan di baris keenam *QR Code* di antara garis pemisah. Sedangkan pola pengaturan waktu vertikal terletak di kolom keenam *QR Code* juga di antara garis pemisah. Fungsi dari pola-pola ini adalah untuk menentukan kepadatan simbol, koordinat modul, dan area informasi versi dalam *QR Code*.

4. *Alignment Patterns* (Pola Pengaturan)

Alignment Patterns hanya ada pada simbol *QR Code* versi 2 atau lebih besar yang dibuat dari modul gelap 5x5, modul terang 3x3, dan satu modul gelap di tengah. *QR Code* yang versi 2 dan yang lebih besar harus mempunyai pola keselarasan dan jumlahnya pola penyalarsan tergantung pada versi simbol.

5. *Encoding Region*

Wilayah pengkodean berisi format informasi, informasi versi, data dan kesalahan kode koreksi.

6. *Quiet Zone*

Quiet Zone merupakan wilayah yang harus bebas dari tanda lainnya, yang mengelilingi simbol di keempat sisinya.

B. Karakteristik *QR Code*

Karakteristik dari *QR Code* dua dimensi adalah dapat menampung jumlah data yang besar. Secara teori sebanyak 7089 karakter numerik maksimum dapat tersimpan di dalamnya. Berikut adalah karakteristik *QR Code* :

1. *Format* :

- 1) *QR Code* memiliki kemampuan lengkap dan kapasitas data maksimal.
- 2) *QR Code Micro* memiliki kemampuan pengurangan *overhead* dengan beberapa pembatasan kemampuan dan pengurangan data kapasitas (dibandingkan dengan simbol *QR Code*).

2. Kumpulan Karakter yang Dapat Dikodekan

- 1) Model ECI (*Extended Channel Interpretation*)
- 2) Data Numerik (0-9)
- 3) Alfanumerik (0-9, Karakter a-z, dan 9 simbol spasi, \$,%*,+,-,.,/,,:)
- 4) *Byte* data (8 bit setiap karakter)
- 5) Huruf Kanji (Setiap 2 *byte* karakter kanji di tampung dalam 13 bit biner)

3. Representasi Data

Modul gelap secara nominal merepresentasikan angka biner satu, sedangkan yang terang secara nominal merepresentasikan angka biner nol.

4. Ukuran Simbol

- 1) Mikro *QR Code* : 11 x 11 modul – 17 x 17 modul (versi M1-M4).
- 2) *QR Code* : 21 x 21 modul hingga 177 x 177 modul (versi 1-40).

5. Karakter Data Per Simbol

- 1) Numerik : 35 karakter
- 2) Alpanumerik : 21 karakter
- 3) *Byte* : 15 karakter
- 4) Kanji : 9 karakter

2.2.3 *Encoding dan Decoding*

Encoding merupakan proses mengubah informasi dari satu format ke bentuk format yang lain. Untuk mengubah data input menjadi *output* berupa *QR Code*, maka terdapat beberapa langkah proses *encoding* yang harus dilakukan.

A. *Prosedur Encoding pada QR Code*

Prosedur *encoding* pada *QR Code* melibatkan beberapa langkah untuk mengonversi data menjadi pola visual yang dapat dibaca oleh *scanner*. Berikut adalah tahapan-tahapan dasar dalam proses *encoding* pada *QR Code*.

1. *Data Analysis*

QR Code mengkodekan sebuah string teks. Standar *QR Code* memiliki empat mode untuk mengkodekan teks yaitu numerik, alfanumerik, *byte*, dan kanji. Setiap mode mengkodekan teks sebagai rangkaian bit (1 dan 0), tetapi setiap mode menggunakan metode yang berbeda untuk mengubah teks menjadi bit, dan setiap metode pengkodean dioptimalkan untuk mengkodekan data dengan rangkaian bit yang sesingkat mungkin.

2. *Data Encoding*

Hasil dari proses ini adalah rangkaian bit yang dipecah menjadi data *codewords*, masing-masing sepanjang 8 bit. Mode yang digunakan untuk pengkodean diidentifikasi oleh *Mode Indicator*, yaitu rangkaian 4 bit. Data yang telah dikodekan harus diawali dengan mode indicator yang sesuai yang digunakan dalam pengkodean.

3. *Error Correction Coding*

QR Code menggunakan koreksi kesalahan. Ini berarti bahwa rangkaian bit data yang mewakili teks digunakan untuk menghasilkan *codewords* koreksi kesalahan menggunakan proses yang disebut koreksi kesalahan *Reed-Solomon*.

4. *Structure Final Message*

Data dan *codewords* koreksi kesalahan yang dihasilkan pada langkah sebelumnya sekarang harus disusun dalam urutan yang benar. Untuk *QR Code* yang besar, data dan *codewords* koreksi kesalahan dihasilkan dalam blok-blok, dan blok-blok ini harus disusun secara interleaved sesuai dengan spesifikasi *QR Code*.

5. *Module Placement in Matrix*

Setelah menghasilkan data *codewords* dan *codewords* koreksi kesalahan serta menyusunnya dalam urutan yang benar, selanjutnya adalah menempatkan bit-bit tersebut dalam matriks *QR Code*. *Codewords* disusun dalam matriks dengan cara tertentu.

6. *Data Masking*

Pola-pola tertentu dalam matriks *QR Code* dapat menyulitkan pemindai *QR Code* untuk membaca kode dengan benar. Untuk mengatasi hal ini, spesifikasi *QR Code* mendefinisikan delapan pola *masking*, yang masing-masing mengubah *QR Code* sesuai dengan pola tertentu.

7. *Format And Version information*

Langkah terakhir adalah menambahkan informasi format dan (jika diperlukan) versi ke *QR Code* dengan menambahkan piksel di area tertentu pada kode yang sebelumnya dibiarkan kosong. Format piksel mengidentifikasi tingkat koreksi kesalahan dan pola *masking* yang digunakan dalam *QR Code* ini. Piksel versi mengkodekan ukuran matriks *QR Code* dan hanya digunakan pada *QR Code* yang lebih besar.

B. Prosedur *Decoding* pada *QR Code*

Prosedur *decoding* pada *QR Code* melibatkan beberapa langkah teknis mengubah pola-pola visual pada kode menjadi data yang dapat dibaca dan dipahami oleh manusia atau sistem komputer. Berikut adalah tahapan-tahapan dasar dalam proses *decoding* pada *QR Code*.

1. *Recognizing Modules*

Temukan dan dapatkan gambar simbol. Kenali modul gelap dan terang sebagai *array* bit "0" dan "1". Identifikasi polaritas reflektansi dari pewarnaan modul pola pencari.

2. *Extract Format Information*

Lepaskan pola *mask* dan lakukan koreksi kesalahan pada modul informasi format jika diperlukan. Jika berhasil, simbol berada dalam orientasi normal, jika tidak, coba dekoding informasi format. Identifikasi tingkat koreksi kesalahan, baik secara langsung pada simbol *QR Code*, atau dari nomor simbol *QR Code*, dan referensi pola *mask* data.

3. *Determine version Information*

Baca informasi versi (jika ada), kemudian tentukan versi simbol (dari nomor simbol, untuk simbol *micro QR Code*).

4. *Release Masking*

Lepaskan *mask* data dengan melakukan operasi XOR antara pola bit wilayah pengkodean dengan data pola *mask* yang referensinya telah diekstrak dari informasi format.

5. *Restore Data and Error Correction Codewords*

Baca karakter simbol sesuai aturan penempatan untuk model tersebut dan pulihkan data serta codeword koreksi kesalahan dari pesan.

6. *Error Detection and Correction*

Dengan memanfaatkan *codeword* koreksi kesalahan, identifikasi kesalahan dan jika ada kesalahan terdeteksi maka perbaiki.

7. *Decode Data Codewords*

Membagi *codeword* datanya menjadi beberapa segmen sesuai dengan indikator mode dan indikator jumlah karakter. Dan terakhir, pecahkan kode karakter data sesuai dengan mode yang digunakan dan menampilkan teks yang didekodekan sebagai hasilnya [16].

2.2.4 Face Recognition

Salah satu metode biometrik yang dikenal sebagai pengenalan wajah memungkinkan komputer untuk mengenal wajah manusia. Sistem pengenalan wajah menghadapi sejumlah masalah, termasuk ekspresi wajah, iluminasi atau pencahayaan, dan jarak, yang membuatnya sangat sulit untuk membedakan beberapa wajah manusia dalam gambar. Pengenalan wajah yang merupakan salah satu metode berbasis wajah dalam konsep *face recognition*, membagi identifikasi menjadi dua kategori, yaitu dikenali atau tidak dikenali, setelah sampel disimpan dalam sistem. Meskipun pengenalan wajah memberikan kemudahan, namun terdapat beberapa masalah yang mungkin terjadi dalam proses pengenalan wajah. Ada beberapa masalah dengan deteksi wajah karena faktor-faktor berikut :

1. Terhalang oleh objek atau wajah lain. Citra wajah dapat terhalang sebagian oleh objek atau wajah lain.

2. Kondisi pengambilan gambar: Banyak faktor, termasuk arah sumber cahaya, intensitas cahaya ruangan, dan fitur sensor dan lensa kamera, mempengaruhi gambar yang diambil.
3. Posisi wajah. Ekspresi wajah seseorang, seperti tersenyum, tertawa, sedih, berbicara, dan sebagainya, sangat mempengaruhi penampilan wajahnya.
4. Komponen wajah yang ada atau tidak ada. Komponen wajah seperti kumis, jenggot, dan kacamata dapat ada di dalam gambar.
5. Ekspresi wajah. Ekspresi wajah seseorang sangat dipengaruhi oleh bagaimana wajahnya diposisikan, seperti tegak, miring, menoleh, atau dilihat dari samping [17].

Verifikasi dan identifikasi adalah dua kategori utama pengenalan wajah. Pengenal wajah berbasis verifikasi digunakan untuk tujuan keamanan seperti kontrol akses, penjagaan perbatasan, dan penegakan hukum. Contohnya, teknologi pengenalan wajah di bank atau pintu masuk gedung hanya memungkinkan orang yang terdaftar di sana untuk mengakses. Sebaliknya, pengenalan wajah berbasis identifikasi digunakan untuk mengenali orang yang tidak dikenal, seperti yang terlihat pada kamera CCTV yang digunakan untuk mencari pelaku kejahatan. Meningkatkan akurasi dan keandalan mengenali wajah meskipun ada perbedaan dalam pose, pencahayaan, dan ekspresi wajah merupakan tantangan utama dalam pengembangan teknologi ini.

Teknik pengenalan wajah merupakan suatu proses yang terdiri dari beberapa tahap. Tahap pertama, Sebelum proses penghapusan, gambar atau video wajah diproses untuk menghilangkan gangguan atau *noise* pada gambar agar hasilnya lebih akurat. Menghasilkan data yang bersih dan terstruktur adalah kunci untuk tahap ini. Pada tahap kedua, fitur wajah diekstraksi dari gambar yang sudah diproses sebelumnya. Pada teknik pengenalan wajah beberapa pendekatan, seperti *Principal Component Analysis (PCA)*, dapat digunakan untuk mengekstrak fitur-fitur penting dari wajah [18]. PCA adalah teknik untuk mengurangi dimensi gambar yang berdimensi tinggi dengan hasil gambar yang berdimensi rendah. Proses ekstraksi mencari vektor ciri dari gambar wajah yang dikenali. Proses ini pada dasarnya mencari bobot dari setiap *eigenface* yang digunakan untuk merepresentasikan citra wajah [7].

2.2.5 ESP32-Cam

Esp32-Cam merupakan sebuah pengembangan yang menggabungkan antara *WiFi* dan *Bluetooth* dengan mikrokontroler Esp32 dan kamera. Komponen ini menyediakan fitur yang dapat diakses oleh siapa saja, yang juga dikenal sebagai *open source*. Salah satu dari fitur-fitur tersebut adalah kemampuan untuk mengambil gambar, melakukan pengenalan wajah (*face recognition*) dan pendeteksi wajah (*face detection*). Modul perangkat tambahan ini dapat dimanfaatkan melalui editor Arduino IDE untuk mengakses berbagai *library* atau fitur yang telah disediakan.



Gambar 2.5 ESP32-CAM [8]

Pada gambar 2.5 adalah modul multifungsi yang dapat digunakan dalam berbagai proyek dan merupakan solusi terpadu karena memiliki mikrokontroler yang memungkinkannya beroperasi secara mandiri. ESP32-Cam memiliki konektivitas *WiFi* dan *bluetooth*, serta kamera video terintegrasi yang memungkinkan untuk mengambil gambar atau merekam video. Selain itu, modul ini memiliki slot microSD, yang dapat digunakan untuk menyimpan hasil tangkapan gambar atau video. Semua fitur ini membuat ESP32-Cam pilihan yang menarik untuk digunakan dalam berbagai proyek, terutama yang berkaitan dengan pemrosesan gambar, video, atau aplikasi [19].

Tabel 2.2 *Datasheet* ESP32-CAM

Nama Alat	Spesifikasi
ESP32-CAM	- <i>SPI Flash</i> : default 32Mbit
	- <i>RAM</i> : built-in 520 KB+external 4MPSRAM
	- <i>Dimension</i> : 27*40.5*4.5 (± 0.2) mm/1.06*1.59*0.18''
	- <i>Bluetooth</i> : Bluetooth 4.2 BR/EDR and BLE standards

Nama Alat	Spesifikasi
	- <i>Wi-Fi</i> : 802.11b/g/n/e/i
	- <i>Support Interface</i> : UART, SPI, I2C, PWM
	- <i>Support TF card</i> : maximum support 4G
	- <i>IO port</i> : 9
	- <i>Serial Port Baud-rate</i> : Default 115200 bps
	- <i>Image Output Format</i> : JPEG(OV2640 support only), BMP, GRAYSCALE
	- <i>Spectrum Range</i> : 2412 ~2484MHz
	- <i>Antenna</i> : onboard PCB antenna, gain 2dBi
	- <i>Transmit Power</i> : 802.11b: 17±2 dBm (@11Mbps); 802.11g: 14±2 dBm (@54Mbps); 802.11n: 13±2 dBm (@MCS7)
	- <i>Receiving Sensitivity</i> : CCK, 1 Mbps : -90dBm; CCK, 11 Mbps: -85dBm; 6 Mbps (1/2 BPSK): -88dBm; 54 Mbps (3/4 64-QAM): -70dBm; MCS7 (65 Mbps, 72.2 Mbps): -67dBm
	- <i>Security</i> : WPA/WPA2/WPA2-Enterprise/WPS
	- <i>Power supply range</i> : 5V
	- <i>Operating temperature</i> : -20 °C ~ 85 °C
	- <i>Storage environment</i> : -40 °C ~ 90 °C, < 90%RH
	- <i>Weight</i> : 10g

2.2.6 Solenoid Doorlock

Solenoid *doorlock* merupakan jenis *solenoid* yang khusus difungsikan sebagai pengunci pintu secara elektronik. Solenoid *doorlock* ini memiliki dua mode operasi yaitu *Normally Closed* (NC) dan *Normally Open* (NO). Pada mode NC, *solenoid* akan mengunci pintu dalam keadaan *default* atau saat tidak ada aliran listrik. Pada mode NO, sebaliknya, *solenoid* akan membuka kunci pintu saat tidak ada aliran listrik. Kedua mode operasi ini memungkinkan *solenoid* untuk dikonfigurasi sesuai kebutuhan [12].



Gambar 2.6 Solenoid Doorlock [12]

Untuk menggerakkan *solenoid door lock* yang terlihat pada gambar 2.6, dibutuhkan sebuah komponen bernama *relay*. *Relay* berfungsi sebagai saklar elektronik yang memfasilitasi pengoperasian *solenoid* dalam mekanisme

penguncian pintu. *Relay* merupakan komponen elektronika yang dioperasikan menggunakan arus listrik untuk menggerakkan saklar. Secara prinsip kerja, *relay* terdiri dari tuas saklar dan lilitan kawat (*solenoid*) yang berdekatan. Ketika *solenoid* mendapat aliran arus listrik, akan terbentuk gaya magnet yang menarik tuas saklar sehingga kontak saklar akan menutup. Dengan memanfaatkan *relay*, arus listrik dari sistem kontrol dapat digunakan untuk mengaktifkan *solenoid door lock* agar dapat membuka atau mengunci pintu secara elektronik [20].

Tabel 2.3 Datasheet *Solenoid Doorlock*

Nama Alat	Spesifikasi
<i>Solenoid Doorlock</i>	- <i>Operating Temperature / Humidity : -20°C to +45°C / 5% to 95% RH</i>
	- <i>Store Temperature / Humidity : -20°C to +65°C / 5% to 60% RH</i>
	- <i>Operating Voltage : 12V DC ±10% Insulation Resistance : 500V DC, ≥50MΩ</i>
	- <i>Dielectric Strength : 700V AC 50/60Hz</i>
	- <i>Insulation Level : Class B (130°C)</i>
	- <i>Wattage : 9W (12V DC, R=16Ω ±10%)</i>
	- <i>Stroke-Force : 6mm thrust: ≥50gf (12V DC)</i>
	- <i>Work Cycle : Pass 0.05 seconds, break 0.05 seconds, max. power-on time, 10 seconds (ED 50%)</i>
	- <i>Temperature Rise : ≤80°C (12V DC, 0.05 seconds off for 0.05 seconds, no load)</i>
	- <i>Response Time : ≥50mS (12V DC, S=10.5mm, no load)</i>
	- <i>Leading strength : 1Kgf-30 seconds</i>
	- <i>Life : ≥500,000 times (12V DC, pass for 0.05 seconds, break 0.05 seconds for one time, load (institution))</i>

2.2.7 Relay 1 Channel

Relay merupakan sebuah perangkat elektronik yang mengelola arus listrik tinggi pada perangkat dengan bantuan sinyal listrik berdaya rendah. Meskipun mirip dengan saklar, modul *relay* beroperasi secara elektronis. Komponen pada gambar 2.7 terdiri dari kumparan dan *switch*, dimana kumparan menerima tegangan rendah (biasanya sekitar 5V atau 12V).



Gambar 2.7 Relay 1 Channel [8]

Ketika kumparan diaktifkan, *switch* akan terhubung sehingga arus dapat mengalir. Fungsi utama modul *relay* adalah mengontrol perangkat berdaya tinggi menggunakan sinyal kontrol berdaya rendah, serta mengisolasi sirkuit listrik dengan daya tinggi dan rendah. *Switch* untuk menjalankan berbagai peralatan elektronik, dan siap menjalankan fungsi logika jika lampu *relay module* sedang menyala [8]. Pada tabel 2.4 menjelaskan tentang *datasheet relay 1 channel*.

Tabel 2.4 Datasheet Relay 1 Channel

Nama Alat	Spesifikasi
<i>Relay Module</i>	- 1 channel relay module
	- One normally closed contact and one normally open contact
	- High impedance controller pin
	- Default High-level trigger
	- Pull-down circuit for the avoidance of malfunction
	- Power supply indicator lamp
	- Can be controlled various appliances & other Equipment with Large current
	- Standard TTL Level logic controlled
	- The module is compliant with international safety standards
	- With 4 fixed screw holes, hole diameter- 3.1mm, convenient installation and fixation
	- Channel – 1
	- Trigger Voltage (VDC) – 5
	- Switching Voltage (VAC) – 250@10A
- Switching Voltage (VDC) – 30@10A	

2.2.8 LCD 16X2

LCD (*liquid crystal display*) merupakan salah satu jenis media tampilan yang menggunakan kristal cair sebagai tampilan utamanya. LCD digunakan di berbagai bidang, termasuk perangkat elektronik seperti televisi, kalkulator, dan layar komputer.



Gambar 2.8 LCD 16x2 [12]

Pada gambar 2.8 aplikasi LCD yang digunakan adalah LCD dot matrik 2 x 16 karakter. LCD sebenarnya bertindak sebagai tampilan dan kemudian digunakan untuk menunjukkan status kerja [12].

Tabel 2.5 Datasheet LCD 16x2

Nama Alat	Spesifikasi
Kabel Jumper	- <i>Type: Character</i>
	- <i>Display format: 16 x 2 characters</i>
	- <i>Built-in controller: ST 7066 (or equivalent)</i>
	- <i>Duty cycle: 1/16</i>
	- <i>5 x 8 dots includes cursor</i>
	- <i>+ 5 V power supply</i>
	- <i>LED can be driven by pin 1, pin 2, or A and K</i>
	- <i>N.V. optional for + 3 V power supply</i>
- <i>Optional: Smaller character size (2.95 mm x 4.35 mm)</i>	

2.2.9 Push Button

Push button dikenal sebagai saklar tombol tekan yang merupakan perangkat/saklar sederhana yang dapat menghubungkan atau memutuskan aliran arus listrik dengan sistem kerja tekan *unlock* (tidak mengunci).



Gambar 2.9 Push Button Momentary [21]

Pada gambar 2.9 ketika tombol ditekan, saklar berfungsi sebagai alat penghubung/pemutus aliran arus listrik, tetapi saat tombol tidak ditekan atau dilepas, saklar akan kembali ke kondisi normal [21]. Pada tabel 2.6 memperlihatkan *datasheet push button*.

Tabel 2.6 Datasheet Push Button Momentary

Nama Alat	Spesifikasi
Push Button	- <i>Bushing : 12mm</i>
	- <i>Contact Rating : 2a @36vdc</i>
	- <i>Electrical Life : 200.000 Cycles At Full Load</i>
	- <i>Contact Resistance: 50m-Ohms Max. Initial @2-4vdc</i>
	- <i>Insulation Resistance: 1,000m-Ohms Min. @ 500vdc</i>
	- <i>Dielectric Strength: 2,000v Rms 50~60hz.</i>
	- <i>Ip Class: Ip65 Protection.</i>
	- <i>Torque: 5~14nm Max. Applied To Nut.</i>

2.2.10 *Internet Of Things*

Konsep *internet of things* (IoT) berarti bahwa semua benda dapat berinteraksi dan berbicara satu sama lain. Setelah semua benda memiliki kemampuan untuk berinteraksi dengan manusia, kita dapat mengontrolnya. IoT telah menjadi bagian dari industri teknologi dan menawarkan kenyamanan dan kemudahan kepada penggunaannya dalam bidang kesehatan, *smart home*, dan transportasi. Dengan tiga lapisan utama arsitektur *internet of things* yaitu *application layer*, *connectivity layer*, dan *device layer* [22].



Gambar 2.10 *Internet Of Things* (IoT) [22]

Sebagai teknologi seperti pada gambar 2.10, IoT dapat membantu dan mempermudah kehidupan manusia dengan berbagai cara, seperti berbagi data dan mengontrol secara *remote*. IoT juga dapat diterapkan pada hal-hal yang ada di sekitar, seperti perangkat elektronik, pengolahan makanan, dan berbagai mesin, atau melalui sensor yang tertanam di jaringan. IoT bekerja dengan menggunakan logika pemrograman tertentu. Setiap instruksi dalam logika tersebut memungkinkan interaksi antar perangkat yang terhubung secara otomatis, tanpa perlu campur tangan manusia. Meskipun tampak ideal, IoT tetap menghadapi tantangan besar dalam proses konfigurasinya, terutama dalam jaringan komunikasi karena jaringan IoT sangat kompleks dan membutuhkan sistem keamanan yang sangat ketat. Selain itu, biaya pengembangan IoT yang tinggi juga sering menjadi hambatan, yang pada akhirnya bisa menyebabkan kegagalan dalam produksi dan pengembangan [23].

2.2.11 Quality of Service (QoS)

Parameter *Quality of Service* menunjukkan kualitas paket data jaringan. Tujuan *Quality of Service* adalah untuk membantu pengguna meningkatkan produktivitas dengan memastikan bahwa pengguna mendapatkan kinerja yang andal dari aplikasi berbasis jaringan. Mengirimkan data melalui jaringan berbasis IP dan internet menghadirkan tantangan dalam mempertahankan *Quality of Service*. Biasanya parameter yang didapatkan dari hasil *capture software wireshark* dapat dibandingkan dengan standar ITU-T G.1010. Berikut parameter yang digunakan pada pengujian :

1. Throughput

Throughput yang selalu dikaitkan dengan *bandwidth* merupakan kemampuan jaringan untuk mengirimkan data yang sebenarnya. *Bandwidth* lebih tetap dan dinamis, tetapi tergantung pada lalu lintas yang sedang berlangsung. Nilai *throughput* dapat dihitung secara matematis dengan menggunakan rumus persamaan 2.1. Kategori *packet loss* berdasarkan standar ditunjukkan pada tabel 2.7 [24].

$$\text{Throughput} = \frac{\text{jumlah bytes}}{\text{time span (s)}} \quad (2.1)$$

Tabel 2.7 Kategori Throughput

Kategori Latensi	Throughput	Indeks
Sangat Baik	>2.1 Mbps	4
Baik	1200 kbps – 2,1 Mbps	3
Cukup	700-1200 kbps	2
Kurang Baik	338-700 kbps	1
Buruk	0-338 kbps	0

2. Packet Loss

Packet loss didefinisikan sebagai kegagalan transmisi paket data saat mencapai tujuannya. Kegagalan pada paket tersebut mencapai tujuan, dapat disebabkan oleh beberapa kemungkinan, yaitu mencakup penurunan pada signal dalam media jaringan, melebihi batas saturasi jaringan, paket yang *corrupt* yang menolak untuk transit, dan kesalahan *hardware* jaringan [24]. Kategori *packet loss* berdasarkan standar ITU-T ditunjukkan pada tabel 2.8 [25].

$$Packet\ Loss = \frac{Paket\ Dikirim - Paket\ Diterima}{paket\ dikirim} \times 100 \quad (2.2)$$

Tabel 2.8 Kategori Packet Loss

Kategori Latensi	Packet Loss	Indeks
Sangat Baik	0-2%	4
Baik	3-14%	3
Cukup	15-24%	2
Buruk	>25%	1

3. Delay

Delay adalah waktu yang diperlukan bagi data untuk dikirim dari satu komputer ke komputer lain. *Delay* dalam transmisi paket di jaringan komputer disebabkan oleh antrian yang panjang atau pengambilan rute alternatif untuk menghindari kemacetan pada *routing* [25]. Faktor-faktor yang mempengaruhi *delay* antara lain jarak, media fisik, kongesti, dan waktu pemrosesan yang lama. Kategori *delay* berdasarkan standar ITU-T ditunjukkan pada tabel 2.9 [26].

$$Rata - rata\ Delay = \frac{Total\ Delay}{Jumlah\ Paket\ Diterima} \quad (2.3)$$

Tabel 2.9 Kategori Delay

Kategori Latensi	Besar Delay
Very Good	<150 ms
Good	150 – 300 ms
Enough	300 – 450 ms