BAB 2
DASAR TEORI

2.1 KAJIAN PUSTAKA

Penelitian [4] membahas tentang pengembangan system keamanan brankas menggunakan eKTP berbasis *Internet of Things* (Iot). Sistem keamanan brankas juga dilengkapi oleh notifikasi Telegram yang dimaksudkan sebagai notifikasi atau pemberitahuan ketika brankas dalam keadaan bahaya. Hasil pengujian menunjukkan bahwa notifikasi Telegram berhasil dikirimkan untuk kondisi waspada dan bahaya. Rata-rata waktu pengiriman notifikasi adalah 5,8 detik, sedangkan pengiriman foto membutuhkan waktu 6,5 detik. Sensor HCSR04 berfungsi dengan baik pada jarak 2 - 23 cm dengan rata-rata *error* sekitar 4,28%. Sistem RFID untuk e-KTP hanya dapat mendeteksi satu kartu terdaftar pada pengujian pertama dan tidak berhasil pada pengujian selanjutnya. Sensor *flame* mampu mendeteksi api dari jarak 5 cm - 50 cm. Sensor Modul *GPS Neo* 6 dapat mengidentifikasi perpindahan tempat pada brankas dengan rata-rata *error* sekitar 0,98 meter.

Penelitian [5] membahas tentang sistem keamanan pada pintu brankas menggunakan sensor sidik jari. Sistem ini terdiri dari perangkat keras dan perangkat lunak. Perangkat keras mencakup Arduino Uno, sensor sidik jari, *buzzer*, *selenoid door*, dan *LCD*. Perangkat lunaknya menggunakan program *Arduino IDE*. Sistem berfungsi dengan mendeteksi sidik jari pengguna atau pemilik brankas. Jika terdeteksi, *selenoid* membuka pintu. Jika tidak terdeteksi, pintu tetap terkunci dan alarm berbunyi. Sistem ini efektif untuk menjaga keamanan brankas yang berisi barang berharga seperti sertifikat, uang, dan emas.

Penelitian [6] membahas tentang Sistem keamanan brankas telah ditingkatkan dengan metode identifikasi personal menggunakan pola aritmatika modulo. Sistem ini memiliki lapisan keamanan tambahan dengan penggunaan tag RFID yang terdaftar dan diverifikasi pada kartu. *Password* yang dimasukkan pada kartu tidak dapat dibaca atau diverifikasi, sehingga akses ditolak jika tidak valid. Komponen termasuk *Arduino Mega 256, tag* RFID pasif, dan pembaca RFID. Hanya satu tag pasif yang dapat terverifikasi yang dapat membuka sistem keamanan

dengan penggunaan *keypad* 6 *password*, di mana hanya 3 yang perlu di*input*. *Transistor* pada rangkaian *driver solenoid* akan aktif setelah sistem keamanan terbuka. *Motor servo* dapat berputar sesuai dengan sudut program, dengan posisi terbuka pada 90° derajat.

Penelitian [7] membahas tentang sistem keamanan brankas menggunakan RFID telah dirancang, dengan notifikasi SMS saat brankas terbuka. Proses pengiriman SMS kepada pemilik memakan waktu 10-11 detik karena modul membutuhkan beberapa menit untuk mendapatkan sinyal. Respons modul RFID terhadap kartu pemilik memiliki tingkat akurasi 100%, sementara untuk kartu bukan pemilik akurasi adalah 0%. Sistem ini dapat menjadi landasan untuk pengembangan lebih lanjut dalam teori dan penelitian keamanan brankas.

Penelitian [8] membahas tentang Alat pengaman brankas efektif terdiri dari Mikrokontroller *AT89S51*, *Modul GSM Wavecom, Solenoid,* dan *handphone* sebagai media pengiriman data. Alat ini bekerja secara otomatis pada kunci brankas. Menggunakan Mikrokontroller *AT89S51* sebagai pusat pengolahan data, sistem ini tetap aktif saat terhubung ke sumber tegangan. *Handphone* digunakan untuk mengirim SMS berisi *password* akses brankas. *Modul GSM* akan menerima dan proses SMS tersebut melalui mikrokontroller.

Penelitian [9] membahas tentang Metode pengamatan menggunakan observasi langsung diterapkan pada Alat pendeteksi wajah berbasis Iot dengan Bahasa pemrograman *Python* untuk konfigurasi. Sistem ini menggunakan *Raspberry Pi Zero W* sebagai pemroses, *selenoid* kunci, *Pi camera*, dan notifikasi melalui *handphone*. Tambahan *opencv* dan *haarcascade file* xml digunakan untuk mendeteksi wajah. *Pi camera* dapat mengenali wajah jika data wajah tersimpan dalam sistem, maka *selenoid* akan terbuka. Notifikasi terkirim jika wajah tidak terdeteksi atau tidak dikenali dan *selenoid* tertutup. Secara keseluruhan, alat berfungsi sesuai fungsinya, hanya wajah yang tidak tersimpan dalam sistem yang tidak dikenali.

Penelitian [10] membahas tentang Sistem keamanan rumah mengintegrasikan mikrokontroller dengan aplikasi *smartphone* android. Menggunakan mikrokontroller *fingerprint* dan *Esp-32 Cam* dengan kamera untuk *monitoring*. Sensor *PIR* dan *solenoid lock door* digunakan untuk deteksi dan

mengunci pintu otomatis. *Esp-32 Cam* dan *Esp32 Wroom* digunakan sebagai pembaca sensor sidik jari, karena sidik jari membutuhkan serial sendiri. *Esp-32 Cam* berfungsi sebagai pusat kontrol dan media penyimpanan dataset, dengan kamera *OV2640* dan sensor sidik jari. Metode deteksi menggunakan *Haar Cascade Classifier*.

Penelitian [11] membahas tentang mengembangkan brankas otomatis dengan sistem keamanan ganda menggunakan sensor *facerecognition* dan *fingerprint*. Tujuan proyek adalah meningkatkan keamanan perhiasan dan barang berharga dengan teknologi sensor yang mencakup sensor getar untuk mengirimkan SMS melalui *gateway* jika brankas dipindahkan. Modul *SIM800L* akan mengirimkan koordinat brankas melalui SMS *gateway*, yang selanjutnya dilacak oleh *GPS*. *Buzzer* akan memberikan notifikasi atau tanda.

Penelitian [12] membahas tentang mengembangkan alat *smart CCTV* menggunakan *Raspberry Pi 4* berbasis Iot dengan sistem *face recognition* menggunakan *open source computer vision* (*opencv*). Alat ini memantau orang yang mendekati brankas dan mengirimkan gambar melalui aplikasi Telegram jika orang tersebut tidak dikenali. Hasil penelitian menunjukkan akurasi pengenalan wajah antara 40-69% dan kesesuaian fungsi sebesar 100%.

Penelitian [13] membahas tentang pengembangan sistem keamanan brankas berbasis Android dengan menggunakan *face recognition*. Tujuannya adalah meningkatkan tingkat keamanan dibandingkan dengan sistem sebelumnya. Metode pengembangan mengikuti pendekatan *waterfall*, meliputi analisis, desain, kode program, dan pengujian unit. Penggunaan algoritma *eigenfaces* digunakan untuk deteksi wajah pada tahap *training image* awal. Selain itu, algoritma *Local Binary Patterns* dan *Histogram Equalization* digunakan untuk membaca gambar pengenalan wajah dengan tingkat akurasi hingga 95.56%. Data wajah pengguna akan diproses di *Wemos D1* dan disimpan dalam database. Hasil dari *face recognition* akan digunakan sebagai data pengguna untuk membuka brankas. Kesimpulannya, sistem mampu membaca wajah pengguna secara *real-time* dan berfungsi dengan baik untuk keamanan brankas.

Penelitian [14] membahas tentang studi perbandingan algoritma *Eigenface* dan *Fisherface*, dengan fokus pada implementasinya menggunakan perpustakaan

OpenCV dan *Sci-kit*. Studi ini mengulas efektivitas kedua algoritma tersebut dalam pengenalan wajah, pentingnya pemilihan perpustakaan untuk implementasinya. Hasil penelitian menunjukkan bahwa kedua algoritma efektif dalam pengenalan wajah, namun *Fisherface* menunjukkan akurasi yang lebih tinggi dibandingkan dengan *Eigenface*. Penelitian ini memberikan wawasan berharga dalam bidang teknologi pengenalan wajah dan berfungsi sebagai referensi untuk penelitian lebih lanjut di area ini.

Penelitian [15] membahas tentang pengenalan wajah menggunakan *Fisherfaces*. Paper ini menyajikan gambaran umum tentang teknik terbaru yang digunakan untuk pengenalan wajah dan membahas berbagai aplikasi serta tuntutan keamanan tinggi dalam bidang ini. Para penulis juga membahas metode *Eigenface*, yang merupakan salah satu algoritma yang paling umum digunakan untuk pengenalan wajah, dan bagaimana metode *Fisherfaces* berbeda darinya. Metode *Fisherfaces* menggunakan Analisis *Diskriminan Linear Fisher* (FLDA atau LDA) untuk reduksi dimensionalitas, yang bekerja lebih baik daripada PCA untuk tujuan segregasi. Para penulis juga membahas tantangan dan keterbatasan teknologi pengenalan wajah serta bagaimana cara mengatasinya. Terakhir, paper ini mengeksplorasi potensi aplikasi teknologi pengenalan wajah dan implikasi etis penggunaannya. Secara keseluruhan, paper ini memberikan gambaran komprehensif tentang kondisi terkini teknologi pengenalan wajah dan dampak potensialnya pada masyarakat.

Penelitian [16] membahas tentang evaluasi komprehensif terhadap metode pengenalan wajah di bawah berbagai kondisi cuaca, memberikan wawasan tentang kinerja mereka dalam skenario dunia nyata. Studi ini menyoroti penelitian yang terbatas pada pengenalan wajah *real-time* dalam kondisi berkabut dan hujan, menekankan kebutuhan untuk memahami dampak kondisi-kondisi ini pada teknik pengenalan wajah yang sudah ada. Para penulis mengidentifikasi kelemahan metode-metode sebelumnya dalam mengatasi tantangan terkait cuaca, seperti kurangnya stabilitas untuk pemrosesan gambar *real-time* dalam algoritma penghilangan hujan. Selain itu, studi ini menekankan perlunya penelitian lebih lanjut untuk mengeksplorasi implikasi kondisi cuaca yang berbeda terhadap akurasi dan waktu pemrosesan pengenalan wajah. Temuan ini menekankan signifikansi

potensial penelitian ini dalam membimbing pengembangan dan implementasi teknologi pengenalan wajah, khususnya di lingkungan luar ruangan dan tanpa batas. Lebih lanjut, penelitian ini menekankan perlunya eksperimen masa depan dengan pendekatan berbasis *deep learning* dan interpretabilitas model, mencerminkan kontribusinya dalam memajukan bidang teknologi pengenalan wajah.

Penelitian [17] membahas tentang sistem keamanan pintu menggunakan *face recognition* berbasis *Internet of Things* (Iot) dengan aplikasi *Blynk* untuk pemantauan. Menggunakan *ESP32-Cam, DfPlayer Mini*, dan *Motor Servo*. Hasil analisis dan pengujian menunjukkan sistem berfungsi optimal. Alat dapat membuka pintu melalui *face recognition*, *Touch* Sensor, dan *App Blynk*, mengurangi potensi pencurian. Pengujian *Face Detection* dan *Face recognition* berjalan dengan baik meskipun memiliki sedikit keterlambatan saat pendaftaran dan pendeteksian wajah.

Penilitian [18] membahas tentang Sistem keamanan pintu menggunakan *face recognition* dengan metode *fisherface*. Menggunakan *webcam* dan *Raspberry Pi*, sistem dapat mengirim notifikasi ke Telegram untuk mengidentifikasi orang di depan pintu. Menggunakan *OpenCV*, metode *fisherface* untuk ekstraksi ciri, dan metode klasifikasi dengan pemrograman *Python*. Tingkat akurasi sistem mencapai 80% secara keseluruhan.

Perkembangan sistem keamanan brankas semakin mendorong untuk menanggapi permasalahan terkait keamanan barang berharga. Sejumlah penelitian sebelumnya mengusulkan metode pengamanan, seperti pengenalan wajah, sidik jari, *RFID*, dan pemanfaatan *Internet of Things* (IOT). Dalam penelitian ini, penekanan diberikan pada peningkatan keamanan brankas melalui teknologi pengenalan wajah dan notifikasi *real-time*. Metode *fisherface* digunakan sebagai cara identifikasi pengguna, dengan perbandingan akurasi dan kecepatan terhadap metode lainnya menjadi fokus utama. Penggunaan aplikasi Telegram dianggap signifikan karena memberikan respons instan pada situasi mencurigakan. Pemilihan *hardware*, terutama penggunaan ESP32-CAM, menjadi aspek penting yang memengaruhi kinerja sistem. Dengan mengkaji dari beberapa jurnal terkait, evaluasi terhadap perbedaan dan pengembangan sistem ini diharapkan memberikan kontribusi positif terhadap peningkatan keamanan brankas secara keseluruhan.

Tabel 2. 1 Ringkasan kajian pustaka

Penulis	Judul Penelitian	Hasil Penelitian	Perbedaan
Muhammad Ilham Ali, Suryo Adi Wibowo, Agung Panji Sasito (2021)	Keamanan Brankas Menggunakan E-KTP dan Notifikasi *Via*Telegram Berbasis Iot (*Internet Of Things*)	Pengujian menunjukkan notifikasi Telegram sukses dikirimkan untuk kondisi waspada dan bahaya dengan waktu rata-rata 5,8 detik, foto membutuhkan 6,5 detik. Sensor HCSR04 berfungsi baik pada jarak 2-23 cm dengan *error* rata-rata 4,28%.	mengutamakan implementasi *prototype* fisik yang menggunakan sensor, RFID, dan komunikasi IOT. Yaitu penggunaan teknologi E-KTP sebagai akses untuk membuka pintu brankas.
Okta Rea Arsyad, Kurnia, P.Kartika. (2021)	Rancang Bangun Alat Pengaman Brankas Menggunakan Sensor Sidik Jari Berbasis Arduino	Sistem berfungsi dengan mendeteksi sidik jari pengguna atau pemilik brankas. Jika terdeteksi, *selenoid* membuka pintu. Jika tidak terdeteksi, pintu tetap terkunci dan alarm berbunyi. Pengujian kelayakan dilakukan dengan mengujikan alat yang telah selesai secara langsung kepada *user*. Dengan kesimpulan yang didapat bahwa alat dapat berfumgsi sebagaimana fungsinya dalam sistem pengamanan pada pintu brankas	Sistem ini terdiri dari perangkat keras dan perangkat lunak. Perangkat keras mencakup *Arduino Uno*, sensor sidik jari, *buzzer*, *selenoid door*, dan *LCD*.
Woro Agus Nurtiyanto, Perani Rosyani, Moch Koiru Ihksanudin (2022)	*Security* Sitem Pada Brankas dengan Metode Personal Identifikasi *Number* Berpola Aritmatika Modulo	Dari 3 card RFID tag pasif di dekatkan dengan RFID *reader* hanya 1 tag pasif yang tervalidasi bias membuka akses *security* sistemnya. Dari 6 *password* yang di *input* hanya 3 yang sesuai dengan format aritmatika modulonya dan dapat mebuka *security* sistemnya. Transistor pada rangkaian *driver solenoid* bekerja setelah *security* sistemnya terbuka. Motor Servo dapat berputar sesuai dengan *input*an dari program putaran sudut servo terbuka 90^{o}	Menggunakan metode Personal Identifikasi Number (PIN) yang memiliki pola aritmatika modulo.

Penulis	Judul Penelitian	Hasil Penelitian	Perbedaan
Wahyu Noor Alamsyah, Tri Listyorini,.	Rancang Bangun Sistem Keamanan Brankas Menggunakan *Radio Frequency Identification* (*RFID*) Dengan Notofikasi *Via*SMS	Proses pengiriman SMS kepada pemilik memakan waktu 10-11 detik karena modul membutuhkan beberapa menit untuk mendapatkan sinyal. Respons modul RFID terhadap kartu pemilik memiliki tingkat akurasi 100%, sementara untuk kartu bukan pemilik akurasi adalah 0%.	Menggunakan RFID dan respons notifikasi yang dilakukan melalui layanan SMS.
Nurul Chafid, Zulkifli (2021)	Sistem Keamanan Brankas Menggunakan Kunci Otomatis Dengan SMS	Hasil rangkaian secara keseluruhan dilakukan setelah semua komponen terpasang semua dan program *basic* Bascom-8051, yang sudah dimasukan ke IC Mikrokontroller AT89S51. Setelah terpasang semua komponen kemudian dipasang didalam brankas. Pada sistem ini akan bekerja setelah alat dihubungkan dengan listrik. Rangkaian tersebut harus dihubungkan dengan catu daya 12 V. kemudian sistemakan melakukan inisialisasi port serial.	Memanfaatkan kunci otomatis yang dikendalikan melalui pesan singkat (SMS)
Mohammad Noviansyah, Sopyan (2022)	Sistem Pengamanan Otomatis Dengan Pengenalan Wajah Berbasis *Internet Of Things*	Pada percobaan keseluruhan, ketika wajah tidak tersimpan dalam file sistem Raspberry pi *zero* w maka Pi camera mendeteksi tidak diketahui atau *unknown*. Pemberian tegangan masukan sebesar 5 *Volt*, alat menyala dan sistem berjalan. Untuk uji keseluruhan, wajah bisa dikenali karena wajah tersimpan dalam sistem dan wajah lain tidak diketahui karena tidak tersimpan dalam sistem.	Sistem ini menggunakan *Raspberry Pi Zero W* sebagai pemroses.

Penulis	Judul Penelitian	Hasil Penelitian	Perbedaan
Ahmad Haris Bachtiar, Pressa Perdana Surya, Rini Puji Astutik (2022)	Rancang Bangun Dual Keamanan Sistem Pintu Rumah Menggunakan Pengenalan Wajah Dan Sidik Jari Berbasis IOT (*Internet Of Things*)	Pada jarak 10 cm, kamera tidak dapat menangkap citra wajah, namun pada jarak 30 cm, 50 cm, 75 cm, dan 100 cm, citra wajah tertangkap dengan baik. ESP-32 CAM hanya dapat menyimpan data 3 pengguna karena kapasitas 4 MB. Sinyal router/hotspot mempengaruhi keterlambatan pengiriman data ke Telegram, dengan delay 3-6 detik. Sensor sidik jari berfungsi baik dengan rata-rata delay 3,86 detik, dan penempatan jari yang tepat diperlukan untuk kinerja efektif.	Pengembangan sistem keamanan pintu rumah dengan menggunakan pengenalan wajah dan sidik jari.
Johan Eudes Saleilei, Halifia Hendri, Nanda Tommy Wirawan (2023)	Rancang Bangun Alat Sistem Keamanan Pada Brankas Perhiasan Dengan Menggunakan *Face recognition* Dan *Fingerprint* Berbasis *Arduino Mega2560* Terkendali *Smartphone* Android	Mikrokontroler mengendalikan sistem: fingerprint membuka pintu brankas, sensor Face recognition menambah keamanan, GPS melacak lokasi brankas, SIM800L mengirim data GPS ke SMS gateway melalui sensor getar, buzzer memberikan informasi suara, solenoid membuka pintu, dan LCD menampilkan informasi perintah.	Menggunakan Mikrokontroller *Arduinomega* 2560 dan dilengkapi fitur *GPS*.
Fikriansyah Martunus (2020)	Implementasi *Face recognition* Dengan *Opencv* Pada *Smart Cctv* Untuk Keamanan Brankas Berbasis Iot	Hasil *face recognition* berupa pelabelan pada nama dengan akurasi 40-69% dan tidak dikenali sebagai *unknown*. Masih terdapat kesalahan dalam mengenali identitas gambar masukkan, baik itu kesalahan dalam mengenali identitas gambar masukan sebanyak 1:40 yaitu 0.025% untuk dataset.	penerapan teknologi pengenalan wajah dengan menggunakan *OpenCV* pada sistem *Smart CCTV* untuk meningkatkan keamanan brankas berbasis *Internet of Things (*Iot*)*

Penulis	Judul Penelitian	Hasil Penelitian	Perbedaan
Gilang Aditya Rama, Fauziah, Nurhayati (2020)	Perancangan Sistem Keamanan Brangkas Menggunakan Pengenalan Wajah Berbasis Android	Pengujian sistem keamanan brangkas menggunakan pengenalan wajah dengan metode LPBH pada parameter Grid X dan Grid Y = 8x8, Neighbors = 8, Radius = 1, dan jarak 20-25 cm menghasilkan akurasi 95,56% dan waktu komputasi 2,35 detik. Jarak optimal pengambilan gambar adalah 20-25 cm; gambar terlalu dekat menjadi blur, sementara gambar terlalu jauh tidak terdeteksi.	Menggunakan metode LBPH dengan tingkat akurasi 95,56% dan eigenfaces untuk mendukung berbagai sudut pandang citra, sehingga pengguna tidak perlu selalu tegak lurus menghadap kamera.
Ismail Aliyu, Muhammad Ali Bomoi and Maryam Maishanu (2022)	*A Comparative Study of Eigenface and Fisherface Algorithms Based on OpenCV and Sci-kit Libraries Implementations*	Hasil penelitian ini menunjukkan bahwa Fisherface lebih akurat daripada Eigenface dalam pengenalan wajah. Penelitian ini juga menekankan pentingnya memilih pustaka yang tepat untuk implementasi algoritma. Studi ini berkontribusi pada pengembangan teknologi pengenalan wajah dan dapat menjadi referensi untuk penelitian selanjutnya.	Penelitian ini membahas perbandingan antara algoritma Eigenface dan Fisherface dalam konteks pengenalan wajah.
Rupali Sunil Salunke, Prof. K. N. Pawar (2019)	*Face Recognition using Fisherfaces*	Teknik pengenalan wajah menggunakan Fisherfaces dan metode terbaru dalam keamanan tinggi. Fisherfaces, menggunakan Analisis Diskriminan Linear Fisher (FLDA atau LDA) untuk reduksi dimensionalitas yang lebih baik dibandingkan metode Eigenface yang menggunakan PCA. Selain membandingkan kedua metode, jurnal ini juga menyoroti tantangan dan keterbatasan teknologi pengenalan wajah serta solusi potensial.	Penelitian ini berfokus mengenai Metode *fisherface*.

Penulis	Judul Penelitian	Hasil Penelitian	Perbedaan
Md Manjurul Ahsan, Yueqing Li, Jing Zhang, Md Tanvir Ahad dan Kishor Datta Gupta (2021)	*Evaluating the Performance of Eigenface, Fisherface, and Local Binary Pattern Histogram-Based Facial Recognition Methods under Various Weather Conditions*	Hasil jurnal menunjukkan bahwa Eigenface, Fisherface, dan LBPH mampu mencapai akurasi 100% dalam kondisi cuaca hujan, cerah, dan terbatas lainnya. Namun, LBPH unggul dalam kondisi berkabut dan berawan, sementara Eigenface memiliki akurasi lebih rendah di kedua kondisi tersebut. Studi ini menekankan perlunya penelitian lebih lanjut tentang pengaruh kondisi cuaca terhadap pengenalan wajah dan waktu pemrosesan.	Md Manjurul Ahsan, Yueqing Li, Jing Zhang, Md Tanvir Ahad dan Kishor Datta Gupta (2021)
A.Ipanhar, Toni Wijaya, Pamor Gunoto (2022)	Perancangan Sistem *Monitoring* Pintu Otomatis Berbasis Iot Menggunakan *ESP32-CAM*	Hasil analisis dan pengujian yang dilakukan, sistem keamanan pintu rumah berbasis ESP32-CAM dengan IoT menunjukkan kinerja optimal. Sistem ini menggunakan face recognition, Touch Sensor, dan aplikasi Blynk untuk membuka pintu. Pengujian menunjukkan bahwa sistem face detection dan face recognition berjalan dengan baik meskipun ada sedikit delay saat pendaftaran dan pendeteksian wajah.	A.Ipanhar, Toni Wijaya, Pamor Gunoto (2022)
Friska Yolanda Sitorus, Umar Ali Ahmad, Dick Maryopi (2022)	Desain Dan Implementasi Sistem Keamanan Pintu Menggunakan *Face recognition* Dengan Metode *Fisherface*	Sistem ini menggunakan webcam dan Raspberry Pi untuk mendeteksi orang di depan pintu. Menggunakan OpenCV dan metode fisherface untuk ekstraksi ciri, serta klasifikasi menggunakan Python. Sistem dapat mengirim notifikasi ke Telegram tentang siapa yang berada di depan pintu dengan tingkat akurasi sekitar 80%.	Friska Yolanda Sitorus, Umar Ali Ahmad, Dick Maryopi (2022)

2.2 DASAR TEORI

Dasar teori dalam penelitian ini mencakup berbagai konsep dan prinsip yang mendasari studi yang telah dilakukan. Tujuannya adalah untuk memperkuat pemahaman teori mengenai topik penelitian serta memberikan landasan yang kuat bagi penelitian ini. Dalam bagian ini, akan diuraikan berbagai teori yang mendukung dan berhubungan langsung dengan penelitian yang telah dilaksanakan, sehingga memberikan konteks dan kerangka berpikir yang baik.

2.2.1 Brankas

Brankas adalah lemari atau kotak besi tahan api yang digunakan untuk melindungi barang-barang berharga dari bahaya kebakaran dan pencurian/pembongkaran, seperti uang, surat-surat berharga, perhiasan, dan sebagainya. Asal kata "brankas" berasal dari Bahasa Belanda, di mana "*branden*" berarti membakar dan "*kast*" berarti lemari, sehingga secara harfiah berarti lemari tahan kebakaran. Dalam bahasa Indonesia, brankas juga dikenal sebagai lemari besi, yaitu lemari yang terbuat dari besi. Bentuk brankas dapat berupa kubus/balok atau silinder, dan ada berbagai jenisnya, mulai dari yang kecil dan portabel hingga brankas yang dipasang di dinding atau berbentuk ruangan besar. Sistem kunci pada brankas umumnya dapat berupa digital atau analog, dan kadang-kadang kedua sistem ini digabungkan [4].

Gambar 2. 1 Brankas

Pada gambar 2.1 brankas, terdapat beberapa tipe brankas yang dapat dipilih sesuai dengan kebutuhan pengguna. Namun, kebanyakan orang cenderung memilih brankas tipe baja karena ketahanannya yang tinggi. Brankas ini memiliki sifat tahan terhadap berbagai risiko seperti kebakaran, patah, dan sulit untuk dibuka secara

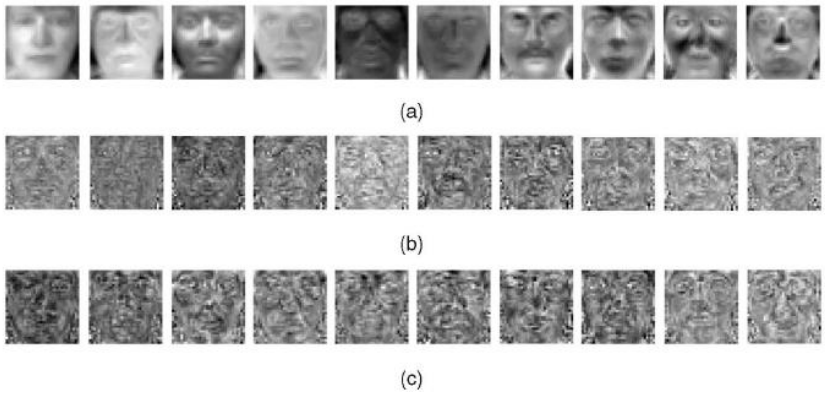
paksa. Selain itu, keamanan pintu brankas juga bervariasi. Pada masa lampau, brankas menggunakan sistem kombinasi angka yang diputar untuk membuka, sementara ada juga yang menggunakan kunci fisik atau kartu. Namun, kunci fisik dan kartu dapat lebih rentan terhadap kerusakan atau kehilangan dibandingkan dengan sistem kombinasi angka.

Beberapa cara yang digunakan untuk mengamankan brankas adalah sebagai berikut:

1. *PIN*, singkatan dari *Personal Identification Number*, yang merupakan sandi numerik yang telah diprogram oleh pemilik. Jika *PIN* yang dimasukkan tidak sesuai, sistem akan menolak untuk membuka pintu. Kelemahan dari metode ini adalah ketika pemilik atau pengguna lupa *PIN* [6].
2. *RFID*, singkatan dari *Radio-Frequency Identification*, adalah teknologi *nirkabel* yang dianggap sebagai inovasi penting dalam dunia komersial. Ini memanfaatkan frekuensi radio untuk melakukan identifikasi otomatis terhadap obyek atau manusia. Fakta bahwa manusia memiliki kemampuan untuk mengidentifikasi obyek di berbagai kondisi lingkungan menjadi latar belakang bagi pengembangan teknologi ini. Namun, kelemahan dari sistem keamanan ini terletak pada risiko kehilangan atau kerusakan kartu. Jika kartu hilang atau mengalami kerusakan seperti patah, maka pintu tidak dapat dibuka [4].
3. Sidik jari, Sensor Sidik Jari atau *Fingerprint* adalah perangkat elektronik yang berfungsi untuk mengidentifikasi sidik jari pengguna dengan menggunakan sensor pemindaian. Akses ke perangkat ini hanya dapat dilakukan oleh pengguna yang terdaftar. Namun, kekurangan dari sistem ini adalah jika sidik jari mengalami luka atau tertutup debu, maka sensor tidak dapat membaca dengan baik, sehingga sistem akan menolak untuk membuka pintu brankas [5].
4. SMS, Melalui SMS, cara kerja sistem ini adalah bahwa perangkat selalu aktif saat terhubung dengan sumber daya listrik. Sistem ini menggunakan telepon seluler untuk mengirimkan SMS yang berisikan kata sandi untuk membuka brankas. SMS tersebut akan diterima oleh modul *GSM* dan diolah oleh mikrokontroller. Kelemahan dari metode ini muncul ketika tidak ada pulsa atau sinyal, sehingga pesan tidak dapat dikirim dan akibatnya pintu brankas tidak dapat terbuka. Sistem ini mengandalkan ketersediaan sinyal telepon seluler untuk mengirim SMS berisi kata sandi, sehingga kehandalannya dapat terganggu jika tidak ada pulsa atau sinyal yang memadai [7].

2.2.2 Metode Pengenalan Wajah

Metode pengenalan wajah menggunakan berbagai teknik untuk mengidentifikasi dan membedakan antara wajah individu. Teknologi ini telah berkembang pesat, memungkinkan sistem komputer untuk mengenali dan memverifikasi identitas seseorang berdasarkan fitur wajah mereka. Terdapat berbagai pendekatan yang dapat digunakan dalam pengenalan wajah, masing-masing dengan kelebihan dan kekurangannya.



Gambar 2. 2 Fitur pengenalan wajah (a.*eigenface*), (b.LBHP), (c.*fisherface*)

Gambar 2.2 berikut ini adalah tiga metode utama yang sering digunakan dalam pengenalan wajah *eigenface*, LBHP (*Local Binary Pattern Histogram*), dan *fisherface*.

1. *Eigenface*, berasal dari dua kata dari bahasa Jerman: "*eigenwert*", yang berarti "karakteristik", dan "*wert*", yang berarti "nilai." Salah satu algoritma pemrosesan gambar yang menggunakan prinsip *Principal Component Analysis* (*PCA*) adalah *Eigenface*. Algoritma ini bertujuan untuk mengurangi dimensionalitas gambar dan menemukan nilai vektor tertinggi yang kemudian digunakan untuk mendistribusikan gambar wajah. Nilai *eigenvector* diurutkan dari *eigenvalue* tertinggi ke *eigenvalue* paling terendah. Nilai-nilai ini kemudian difilter dari sejumlah besar nilai *eigenvector* untuk menghasilkan bentuk primordial komponen [19].
2. *Local Binary Pattern Histograms* (*LBPH*), Metode ekstraksi fitur *LBPH* adalah kombinasi dari metode *Local Binary Pattern* (*LBP*) dan metode *Histograms of Oriented Gradients* (*HOG*). Tahap pertama proses *LBPH* adalah melakukan

operasi tekstur dengan menggunakan operator *LBP*, yang menghasilkan citra baru yang memiliki tekstur yang berbeda untuk setiap orang. Tahap selanjutnya adalah menemukan *histogram* dari citra hasil *LBP* dengan menggunakan alat yang sesuai [20].

3. *Fisherface*, metode *fisherface* adalah hasil dari kombinasi teknik pengelompokan pola menggunakan *PCA* (*Principal Component Analysis*) dan *LDA* (*Linear Discriminant Analysis*). Pendekatan ini memanfaatkan kedua metode tersebut untuk memaksimalkan perbandingan distribusi pola antar kelas dibandingkan dengan distribusi pola di dalam kelas itu sendiri. *Fisherface* lebih unggul dibandingkan *PCA* dan *LDA* secara terpisah, karena semakin besar rasio distribusi, maka vektor fitur yang dihasilkan akan semakin tidak sensitif terhadap perubahan pencahayaan. Oleh karena itu, dapat disimpulkan bahwa metode *fisherface* menghasilkan klasifikasi yang lebih baik [18].

2.2.3 *Fisherface*

Wajah merupakan salah satu indikator fisiologis yang sering digunakan untuk membedakan identitas orang satu dengan lainnya. Manusia memiliki kemampuan untuk membedakan wajah antar orang dan mengingat wajah dengan cepat. Oleh karena itu, pengenalan wajah merupakan salah satu teknologi biometrik yang banyak diteliti dan dikembangkan oleh para ahli. Salah satu tantangan dalam pengembangan pengenalan wajah adalah kompleksitas kondisi wajah, termasuk kualitas gambar, warna, pencahayaan, posisi gambar, dan perubahan geometri. Oleh karena itu, dalam tulisan ini, metode *fisherface* akan diuji untuk melakukan pengenalan wajah. Beberapa penelitian lain yang mengkaji informasi dari wajah manusia termasuk pengklasifikasian berdasarkan ras, gender, dan bentuk wajah. Pendekatan umum untuk pengenalan wajah berfokus pada bentuk wajah dan penempatan atribut seperti mata, alis, hidung, bibir, dan dagu, serta hubungan antar atribut tersebut atau analisis wajah secara keseluruhan yang menghasilkan representasi wajah sebagai kombinasi dari beberapa wajah kanonik. Dalam penelitian ini, akan dibahas klasifikasi bentuk wajah.

Metode *fisherface* merupakan hasil karya dari Peter N. Belhumeur, João P. Hespana, dan David J. Kreigman pada tahun 1997. Metode ini dirancang untuk

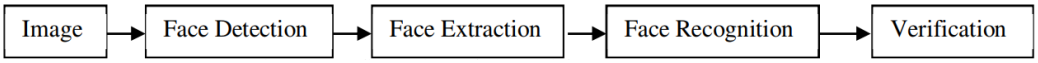
mengatasi kelemahan metode *Eigenface*, terutama dalam menghadapi variasi pencahayaan dan ekspresi wajah. Metode ini melakukan transformasi vektor dari ruang citra berdimensi-n ke ruang citra berdimensi-m, dengan m yang lebih kecil dari n pangkat 2. Dasar dari metode *fisherface* ini adalah *Fisher's Linear Discriminant* (*FLD*), yang ditemukan oleh Robert Fisher pada tahun 1936. *FLD* awalnya digunakan untuk klasifikasi taksonomi dan sejak itu menjadi salah satu teknik yang sering digunakan dalam pengenalan pola. Metode *FLD* termasuk dalam kategori metode kelas khusus, karena fokusnya adalah membentuk jarak (*scatter*) antara kelas-kelas dan dalam kelas sehingga dapat menghasilkan klasifikasi yang lebih akurat.

Face recognition atau pengenalan wajah adalah salah satu teknik identifikasi teknologi biometrik dengan menggunakan wajah individu yang bersangkutan sebagai parameter utamanya. Secara garis besar proses pengenalan wajah terdiri dari tiga proses utama yaitu:

1. Deteksi wajah (*Face Detection*).
2. Ektraksi ciri/wajah (*face/feature extraction).*
3. Pengenalan wajah (*face recognition*).

Secara umum, teknik dan metode dalam pengenalan wajah dapat dikelompokan ke dalam tiga pendekatan berdasarkan data yang dibutuhkannya yaitu:

1. Pendekatan holistik. Pada pendekatan holistik, seluruh bagian atau ciri-ciri global wajah digunakan sebagai data masukan untuk pengenalan wajah. Contoh: *eigenface, fisherface, nearest feature line* (*NFL*), dan *support vector machine* (*SVM*).
2. Pendekatan *feature-based*. Pada pendekatan *feature-based*, wajah terbagi berdasarkan ciri-ciri lokal wajah seperti hidung, mulut, mata, dan lainnya yang kemudian digunakan sebagai data masukan. Contoh: *Hidden Markov Model* dan *Dynamic Link Architecture.*
3. Pendekatan *hybrid*. Pendekatan *hybrid* menggunakan seluruh bagian wajah dan ciri-ciri lokal wajah sebagai data masukan. Contoh: *modular eigenfacedan hybrid local feature.* Pendekatan hybrid menggunakan seluruh bagian wajah dan ciri-ciri lokal wajah sebagai data masukan [2].



Gambar 2. 3 Konfigurasi struktur pengenalan wajah umum

Gambar 2.3 tujuan utama dari langkah deteksi wajah adalah untuk menentukan (1) apakah wajah manusia muncul dalam gambar yang diberikan, dan (2) di mana wajah-wajah tersebut berada. Hasil yang diharapkan dari langkah ini adalah gambar berisi setiap wajah dalam gambar *input*. Untuk membuat sistem pengenalan wajah lebih kuat dan mudah dirancang, penyelarasan wajah dilakukan untuk membenarkan skala dan orientasi wajah ini. Selain berfungsi sebagai pra-pemrosesan untuk pengenalan wajah, deteksi wajah dapat digunakan untuk deteksi area yang diminati, penargetan ulang video, dan klasifikasi gambar, dll.

Secara umum, metode *fisherface* akan memiliki lebih dari 2 kelas. Dalam kasus tersebut, dapat diformulasi masalah yang dinyatakan di atas sebagai masalah meminimalkan perbedaan dalam kelas dan memaksimalkan jarak antar kelas. Perbedaan dalam kelas dapat diestimasi menggunakan matriks sebar dalam kelas, yang diberikan oleh

$$Sw=\sum Cj=1\sum nji=1(xij-\mu j)(xij-\mu j)T \quad (1)$$

dimana xij adalah sampel ke-i dari kelas j, μj adalah mean dari kelas j, dan nj adalah jumlah sampel di kelas j. Demikian pula antar kelas perbedaan dihitung menggunakan matriks pencar antar kelas.

$$Sb=\sum Cj=1(\mu j-\mu)(\mu j-\mu)T \quad (2)$$

di mana μ mewakili rata-rata semua kelas. Sekarang kita ingin mencari vektor basis V dimana Sw diminimalkan dan Sb dimaksimalkan, dimana V adalah matriks yang kolomnya vi adalah vektor basis yang mendefinisikan subruang. Ini diberikan oleh,

$$|VTSbV||VTSwV| \quad (3)$$

Solusi untuk masalah ini diperoleh melalui metode yang dikenal sebagai dekomposisi nilai eigen umum atau generalized eigenvalue decomposition. Metode

ini digunakan untuk menemukan vektor-vektor basis yang memaksimalkan perbedaan antara kelas-kelas (Sb) sekaligus meminimalkan perbedaan dalam kelas (Sw). Secara matematis, ini dicapai dengan menyelesaikan persamaan eigen umum sebagai berikut,

$$SbV=SwV\Lambda \tag{4}$$

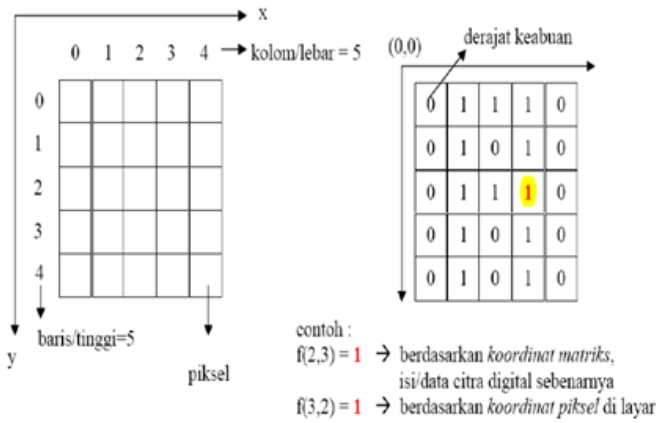
dimana V adalah (seperti di atas) matriks vektor eigen dan Λ adalah matriks diagonal dari nilai eigen yang bersesuaian. Vektor eigen dari V terkait dengan nilai eigen bukan nol adalah Fisherfaces. Terdapat maksimum C−1 Fisherfaces. Hal ini dapat dengan mudah dilihat dari definisi Sb. Perhatikan bahwa dalam definisi kami, Sb adalah kombinasi vektor fitur C. Setiap vektor C mendefinisikan subruang dari C−1 atau dimensi lebih sedikit. Persamaan berlaku jika vektor-vektor ini bebas linier satu sama lain. Gambar 1 menunjukkan empat yang pertama Fisherfaces diperoleh saat menggunakan algoritma yang ditentukan pada kumpulan gambar wajah frontal dari 100 subjek berbeda. Gambar dipilih untuk memiliki ekspresi netral [15].

2.2.4 Citra

Citra merupakan representasi atau gambaran dari suatu objek yang bisa berupa gambar optik seperti foto, sinyal video analog seperti yang terdapat pada layar televisi, atau data digital yang dapat disimpan di media penyimpanan. Proses pengubahannya menjadi data numerik dengan nilai-nilai diskrit disebut digitalisasi, dan hasil akhir dari proses ini disebut citra digital. Terdapat dua jenis citra, yaitu citra kontinu dan citra diskrit. Citra kontinu dihasilkan dari sistem optik yang menerima sinyal analog, seperti mata manusia dan kamera analog. Sedangkan citra diskrit dihasilkan melalui proses digitalisasi dari citra kontinu. Beberapa perangkat optik dilengkapi dengan kemampuan digitalisasi, seperti kamera digital dan *scanner*. Citra diskrit juga dikenal sebagai citra digital. Komputer digital *modern* hanya mampu memproses citra digital. Dalam penelitian ini, citra yang akan diolah adalah citra digital.

Citra digital direpresentasikan sebagai fungsi dua dimensi f(x,y) dengan ukuran M baris dan N kolom, di mana x dan y adalah koordinat dalam bidang dua

dimensi, dan f(x,y) menunjukkan tingkat intensitas cahaya atau tingkat keabuan pada titik tersebut. Citra digital dapat dianggap sebagai matriks dengan indeks baris dan kolom yang menunjukkan titik pada citra, dan setiap elemen matriks (disebut juga sebagai piksel) mewakili nilai tingkat keabuan pada titik tersebut. Citra digital dengan ukuran N x M (dengan tinggi N dan lebar M) direpresentasikan sebagai matriks N x M. Contoh bentuk matriks citra digital dapat dilihat pada gambar 2.4.



Gambar 2. 4 Representasi Citra Digital 2 Dimensi [2]

Citra digital umumnya memiliki bentuk persegi panjang dengan dimensi yang diukur dalam tinggi dan lebar. Untuk mengindikasikan tingkat kecerahan pada setiap pixel, digunakan bilangan bulat 8 bit (atau 1 *byte*) untuk masing-masing pixel, dengan nilai yang berkisar dari 0 hingga 255. Di mana 0 mewakili warna hitam, 255 mewakili warna putih, dan nilai di antara 0 hingga 255 menunjukkan berbagai tingkat keabuan [2].

2.2.5 ESP32-CAM

ESP32-CAM adalah mikrokontroller yang dilengkapi dengan *Wifi* dan *Bluetooth built-in*, serta memiliki tambahan 4MB RAM eksternal. Mikrokontroller ini dilengkapi dengan modul kamera berukuran kecil yang sangat kompetitif dan dapat beroperasi secara independen. ESP32-CAM dapat digunakan dalam berbagai aplikasi *Internet of Things* (Iot), termasuk perangkat pintar untuk rumah, kontrol nirkabel industri, pemantauan nirkabel, identifikasi *QR* nirkabel, sistem penentuan posisi nirkabel, dan berbagai aplikasi Iot lainnya. ESP32-CAM dirancang dalam

paket *DIP* dan dapat langsung dimasukkan ke dalam papan sirkuit untuk mempercepat proses produksi produk dengan koneksi yang sangat andal [17].

Papan pengembangan ini memiliki kemampuan *Wifi* dan *Bluetooth* bawaan dengan mikrokontroller ESP32-CAM serta dilengkapi dengan kamera. Modul ini bersifat *open source*, artinya fiturnya dapat digunakan oleh siapa saja. Salah satu kegunaannya adalah untuk mengambil gambar, melakukan pengenalan wajah, dan mendeteksi wajah. Modul periferal ini dapat diakses dan dimanfaatkan dengan menggunakan pemrograman Arduino IDE, yang menyediakan berbagai pustaka dan fitur yang telah disiapkan sebelumnya. Pada gambar 2.5 terlihat tampilan fisik dari ESP32-CAM.

Gambar 2. 5 ESP32-CAM

ESP32-CAM adalah modul serbaguna yang dilengkapi dengan mikrokontroller terintegrasi, memungkinkannya untuk beroperasi secara mandiri tanpa perlu tambahan komponen eksternal yang kompleks. Modul ini tidak hanya mendukung konektivitas Wifi dan Bluetooth untuk komunikasi nirkabel, tetapi juga dilengkapi dengan kamera video terintegrasi. Fitur tambahan berupa slot microSD memungkinkan penyimpanan lokal data secara langsung pada modul tersebut. Dengan kemampuan ini, ESP32-CAM menawarkan fleksibilitas yang tinggi untuk aplikasi penelitian dan pengembangan teknologi. Modul ini ideal digunakan dalam berbagai proyek yang membutuhkan integrasi sensor visual dan komunikasi nirkabel, serta memfasilitasi pengembangan solusi IoT yang komprehensif. Keseluruhan, keunggulan ESP32-CAM membuatnya sangat cocok untuk eksperimen dan inovasi di berbagai bidang teknologi[21].

Tabel 2. 2 *Datasheet* ESP32-CAM

Nama Alat	Spesifikasi
ESP 32-CAM	- *SPI Flash: default 32Mbit* - *RAM: built-in 520 KB+external 4MPSRAM* - *Dimension: 27*40.5*4.5（±0.2）mm/1.06*1.59*0.18”* - *Bluetooth: Bluetooth 4.2 BR/EDR and BLE standards* - *Wi-Fi: 802.11b/g/n/e/i* - *Support Interface: UART, SPI, I2C, PWM* - *Support TF card: maximum support 4G* - *IO port: 9* - *Serial Port Baud-rate: Default 115200 bps* - *Image Output Format: JPEG(OV2640 support only), BMP, GRAYSCALE* - *Spectrum Range: 2412 ~2484MHz* - *Antenna: onboard PCB antenna, gain 2dBi* - *Transmit Power: 802.11b: 17±2 dBm (@11Mbps); 802.11g: 14±2 dBm (@54Mbps); 802.11n: 13±2 dBm (@MCS7)* - *Receiving Sensitivity: 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* - *Power consumption: Turn off the flash: 180mA@5V Turn on the flash and adjust the brightness to the maximum: 310mA@5V Deep-sleep: the lowest power consumption can reach 6mA@5V Moderm-sleep: up to 20mA@5V Light-sleep: up to 6.7mA@5V* - *Security: WPA/WPA2/WPA2-Enterprise/WPS* - *Power supply range: 5V* - *Operating temperature: -20 °C ~ 85 °C* - *Sorage environment: -40 °C ~ 90 °C, < 90%RH* - *Weight: 10g*

Tabel 2.2 merupakan *datasheet* dari modul ESP32-CAM, yang menjelaskan berbagai spesifikasi teknis dari modul ini. Ditabel sudah menjelaskan apa saja fitur yang dimiliki ESP32-Cam secara keseluruhan. Tabel bertujuan untuk mempermudah untuk mengetahui spesifik yang dimiliki oleh ESP32-CAM.

2.2.6 Relay Module

Relay module adalah komponen elektronik yang mengendalikan perangkat dengan daya tinggi melalui sinyal listrik rendah. Mirip dengan saklar, namun berfungsi secara elektronik. Terdiri dari kumparan dan kontak. *Relay module* berguna untuk mengendalikan perangkat dengan daya tinggi menggunakan sinyal kontrol rendah, serta memisahkan sirkuit listrik tinggi dan rendah.

Gambar 2. 6 *Relay Module*

Gambar 2.6 *Switch* ini digunakan untuk mengaktifkan berbagai peralatan elektronik, dan juga siap untuk menjalankan fungsi logika ketika lampu *Relay Module* sedang menyala. [1].

Tabel 2. 3 *Datasheet relay module*

Nama Alat	Spesifikasi
RELAY MODULE	- *Contact current 10A and 250V AC or 30V DC.* - *Each channel has indication LED.* - *Coil Voltage 12V per channel.* - *Kit operating Voltage 5-12 V* - *Input signal 3-5 V for each channel.* - *Three pins for normally open and closed for each channel.*

Tabel 2.3 merupakan *datasheet* yang detail mengenai spesifikasi teknis dari modul *relay* yang terbaru. Salah satu fitur istimewa dari modul relay ini adalah adanya LED indikator yang terletak pada setiap kanal. Fungsi LED ini sangat penting karena memberikan visualisasi yang jelas mengenai status operasi *relay*, memungkinkan pengguna untuk dengan mudah memantau dan memastikan bahwa *relay* sedang beroperasi dengan baik. Modul ini dirancang dengan tegangan kumparan sebesar 12 *Volt* dan memiliki rentang operasi yang luas, yaitu dari 5 hingga 12 *Volt*, sehingga memberikan fleksibilitas yang tinggi dalam aplikasi praktisnya. Selain itu, modul relay ini juga dilengkapi dengan pin untuk konfigurasi *Normally Open* (NO) dan *Normally Closed* (NC), yang secara signifikan meningkatkan kemudahan dalam mengintegrasikan modul ini dengan berbagai jenis sirkuit elektronik.

2.2.7 Selenoid Door Lock

Solenoid door lock atau kunci pintu *solenoid* adalah perangkat penguncian yang menggunakan prinsip elektromagnetik untuk mengendalikan mekanisme penguncian dan pembukaan pintu.

Gambar 2. 7 *Selenoid Door Lock*

Fungsinya adalah sebagai kunci elektronik yang akan digunakan dalam sistem ini. Untuk menggerakkan *solenoid*, diperlukan penggunaan *relay*. *Relay* berfungsi sebagai saklar elektronik. Prinsip kerjanya melibatkan tuas saklar yang memiliki lilitan kawat di sekitar batang besi (*solenoid*) di sebelahnya. Ketika *solenoid* mendapatkan aliran arus listrik, tuas akan tertarik karena adanya gaya magnet dari *solenoid*, sehingga kontak saklar akan menutup [8].

Tabel 2. 4 *Datasheet selenoid door lock*

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

Tabel 2.4 adalah *datasheet* untuk perangkat kunci pintu *solenoid* (*Selenoid door lock*). *Datasheet* ini mencantumkan spesifikasi teknis dari perangkat tersebut, termasuk rentang suhu operasi dan penyimpanan, kelembaban, tegangan operasional, resistansi isolasi, kekuatan dielektrik, tingkat isolasi, konsumsi daya, gaya dorong, siklus kerja, kenaikan suhu, waktu respon, kekuatan memimpin, dan masa pakai perangkat. Spesifikasi ini memberikan informasi rinci tentang kondisi dan kinerja yang diharapkan dari kunci pintu *da* tersebut dalam berbagai situasi.

2.2.8 Kabel Jumper

Kabel jumper adalah jenis kabel yang digunakan untuk membuat koneksi listrik sementara atau sementara-permanen antara titik-titik di dalam suatu rangkaian elektronik. Kabel jumper sering digunakan dalam *prototyping* dan debugging rangkaian elektronik di *breadboard* atau papan rangkaian lainnya. alat yang esensial dalam elektronik untuk membuat koneksi sementara yang cepat dan mudah. Mereka sangat berguna dalam *prototyping*, pembelajaran, *debugging*, dan pengembangan proyek DIY.

Gambar 2. 8 Kabel Jumper

Gambar 2.8 kabel jumper biasanya terdiri dari seutas kawat berlapis isolasi dengan konektor di kedua ujungnya. Konektor ini bisa berupa pin (*male*), soket (*female*), atau kombinasi keduanya (*male to female*). Jenis-jenis kabel jumper meliputi *Male to Male* (M-M) yang memiliki konektor jantan di kedua ujungnya, sering digunakan untuk menghubungkan titik-titik pada *breadboard*, *Male to Female* (M-F) yang memiliki konektor jantan di satu ujung dan konektor betina di

ujung lainnya, berguna untuk menghubungkan pin pada modul atau sensor ke *breadboard*, serta *Female to Female* (F-F) yang memiliki konektor betina di kedua ujungnya, cocok untuk menghubungkan dua pin jantan. Kabel jumper tersedia dalam berbagai panjang dan warna, yang membantu dalam pengorganisasian dan identifikasi koneksi dalam rangkaian. Kabel jumper tersedia dalam berbagai panjang dan warna, yang membantu dalam pengorganisasian dan identifikasi koneksi dalam rangkaian [17].

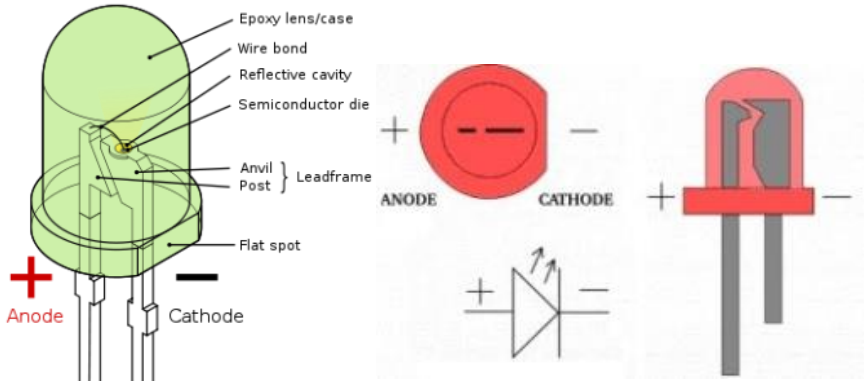
Tabel 2. 5 *Datasheet* kabel jumper

Nama Alat	Spesifikasi
KABEL JUMPER	- *Multi-color ribbons of 40 wires with male-male, female female, or male-female connectors available in 10 cm lengths.* - *Ideal for use with solderless BreadBoards or to connect to square post headers or 0.1" pitch sockets.* - *Rainbow colored ribbon cable provides the 10 standard electrical colors to color-code your connections.* - *28AWG PVC insulated ribbon cable can be unzipped in gropus to organize signals or as individual wires.* - *Contacts use tinned beryllium-copper in black plastic housings.*

Tabel 2.5 adalah *datasheet* yang menjelaskan spesifikasi kabel jumper. Kabel pita berwarna pelangi menyediakan 10 warna standar elektrik untuk kode warna koneksi Anda. Kabel pita dengan insulasi PVC 28AWG dapat dipisahkan dalam grup untuk mengatur sinyal atau digunakan sebagai kabel individual. Kontak menggunakan *beryllium-copper* yang dilapisi timah dalam housing plastik hitam.

2.2.9 LED

LED (*Light Emitting Diode*) adalah komponen semikonduktor yang menghasilkan cahaya saat arus listrik mengalir melaluinya. Proses pemancaran cahaya ini terjadi akibat rekombinasi elektron dan hole dalam material semikonduktor, di mana energi dilepaskan dalam bentuk foton. Cahaya yang dihasilkan oleh LED sangat efisien dan bervariasi tergantung pada material yang digunakan. LED telah diterapkan dalam berbagai aplikasi, termasuk pencahayaan umum seperti lampu rumah dan jalan, indikator status pada berbagai peralatan, serta komunikasi optik yang memanfaatkan cahaya untuk mentransmisikan informasi.



Gambar 2. 9 LED Hijau dan Merah

Gambar 2.9 warna yang dihasilkan oleh LED ditentukan oleh bahan semikonduktor yang digunakan dalam konstruksinya. LED merah, yang umumnya menggunakan bahan semikonduktor seperti *aluminium gallium arsenide* (AlGaAs) atau *gallium arsenide phosphide* (GaAsP), seringkali diterapkan dalam berbagai aplikasi seperti indikator, tanda, dan layar elektronik. Sementara itu, LED hijau menggunakan bahan semikonduktor yang melibatkan campuran *aluminium gallium arsenide* (AlGaAs) atau *gallium phosphide* (GaP), dan sering digunakan dalam indikator, layar, dan aplikasi lainnya. Dalam *smart safe*, dua LED berwarna, hijau dan merah, memberikan informasi visual tentang status keamanan. LED merah menyala saat brankas tertutup atau terkunci, menandakan keamanan. Sebaliknya, LED hijau menyala saat brankas terbuka, menunjukkan ketersediaan akses. Dengan dua warna ini, menjadikannya sistem yang intuitif dan cepat dimengerti[1].

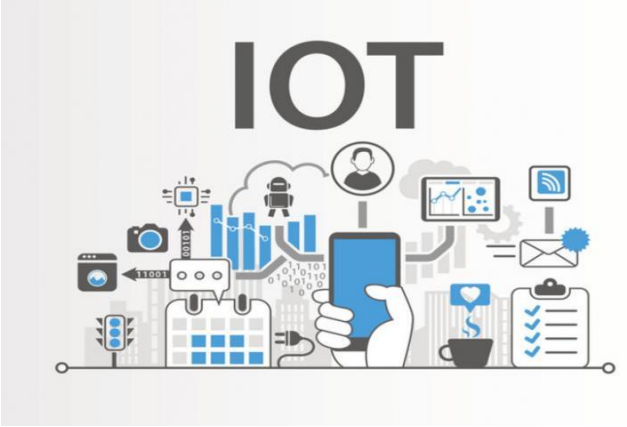
Tabel 2. 6 *Datasheet* LED

Nama Alat	Spesifikasi
LED	- *Standard Red 30mA 1.7V 2.1V 5V 5mcd @ 10mA 60° 660nm* - *Standard Bright red 30mA 2.0V 2.5V 5V 80mcd @ 10mA 60° 625nm* - *Standard Yellow 30mA 2.1V 2.5V 5V 32mcd @ 10mA 60° 590nm* - *Standard Green 25mA 2.2V 2.5V 5V 32mcd @ 10mA 60° 565nm* - *High intensity Blue 30mA 4.5V 5.5V 5V 60mcd @ 20mA 50° 430nm* - *Super bright Red 30mA 1.85V 2.5V 5V 500mcd @ 20mA 60° 660nm* - *Low current Red 30mA 1.7V 2.0V 5V 5mcd @ 2mA 60° 625nm*

Tabel 2.6 menunjukkan spesifikasi berbagai jenis LED berdasarkan warna dan intensitasnya. Tabel mengelompokkan LED ke dalam beberapa kategori seperti "*Standard Red*," "*Standard Bright Red*," "*Standard Yellow*," "*Standard Green*," "*High Intensity Blue*," "*Super Bright Red*," dan "*Low Current Red*." Setiap kategori LED memiliki nilai arus (30mA atau 25mA), tegangan (1.7V hingga 5V), intensitas cahaya (5mcd hingga 500mcd), dan panjang gelombang yang berbeda (660nm, 625nm, 590nm, 565nm, 430nm). Sudut pandang LED juga dicatat dalam tabel ini (50° atau 60°). Sebagai contoh, "*Standard Red*" memiliki spesifikasi arus 30mA, tegangan 1.7V hingga 5V, intensitas cahaya 5mcd pada 10mA, dan panjang gelombang 660nm dengan sudut pandang 60°.

2.2.10 *Internet of Things*

Internet of Things (Iot) adalah konsep pengembangan komunikasi jaringan di mana berbagai benda terhubung satu sama lain melalui internet, memungkinkan pertukaran data dan informasi. Hal ini memungkinkan transformasi data menjadi pemberitahuan dan notifikasi yang dapat diakses secara *online*. Seperti gambar 2.10.



Gambar 2. 10 *Internet of Things*

Untuk meningkatkan tingkat keamanan secara otomatis melalui Iot, berbagai sensor digunakan untuk mendeteksi sinyal dari objek tertentu yang berfungsi sebagai panduan untuk sistem pengamanan. Salah satu sensor yang diterapkan adalah *Pi Camera*, yang mampu mendeteksi wajah seseorang. Sistem keamanan otomatis ini mengintegrasikan teknologi *Pi Camera* untuk mendeteksi

wajah, dengan bantuan ESP32-CAM untuk melakukan proses pengolahan data. Hasil dari proses ini kemudian digunakan untuk mengendalikan *solenoid* agar dapat terbuka atau tertutup sesuai kebutuhan. Jika terjadi situasi di mana *solenoid* tidak terbuka, sistem akan segera menghasilkan notifikasi yang akan disampaikan melalui perangkat telepon genggam [9].

2.2.11 Telegram

Selama 20 tahun terakhir, teknologi komunikasi telah mengalami perkembangan yang signifikan. Dari awalnya hanya terbatas pada SMS dan panggilan telepon di telepon genggam, sekarang telah muncul aplikasi pesan instan yang mengakomodir berbagai kebutuhan komunikasi, bahkan termasuk *video call* dan berbagai fitur lainnya. Saat ini, memiliki banyak opsi aplikasi pesan instan seperti *Whatsapp, Line*, *Snapchat*, *Facebook Messenger*, dan Telegram. Di antara aplikasi pesan instan tersebut, Telegram menonjol sebagai satu-satunya yang menyediakan antarmuka pemrograman aplikasi (API) bagi pengguna untuk membuat bot yang dapat dimanfaatkan dalam sistem informasi. Bot adalah aplikasi pihak ketiga yang dapat dijalankan di dalam *platform* Telegram. Pengguna dapat mengirim pesan, perintah, dan permintaan *inline* kepada bot ini. Dengan menggunakan *HTTPS* ke API Telegram, dapat mengontrol dan berinteraksi dengan *bot*. Bot atau robot sering kali digunakan untuk mengotomatisasi tugas-tugas yang perlu diulang secara teratur. Mereka juga dapat berfungsi sebagai alat pengawasan atau *monitoring* yang dapat dioperasikan oleh *administrator*. Gambar 2.11 Logo aplikasi [3].

Gambar 2. 11 Logo Aplikasi Telegram

Langkah-langkah dalam pembuatan bot Telegram sebagai berikut:

1. Buka aplikasi Telegram dan cari *BotFather*. *BotFather* berfungsi sebagai alat untuk membuat bot baru, meskipun pada awalnya belum dapat dijalankan.
2. Untuk memulai pembuatan bot, ketikkan perintah "/*start*" saat berinteraksi dengan *BotFather*.
3. *BotFather* akan memberikan informasi mengenai langkah-langkah selanjutnya dalam pembuatan bot.
4. Selanjutnya, ketikkan perintah "/*newbot*" untuk membuat bot baru. Sebagai contoh, kita dapat menggunakan nama "Info Kesehatan" dan *username* "info_bot". Pada tahap ini, *BotFather* akan memberikan token yang diperlukan untuk mengakses *HTTP* API bot.
5. Bot yang baru dibuat dapat diakses melalui *URL* yang diberikan oleh *BotFather* setelah pembuatan.
6. Langkah berikutnya adalah memulai percakapan dengan bot yang telah berhasil dibuat dengan menekan tombol "*start*". Ini merupakan langkah awal untuk berinteraksi dengan bot tersebut.

2.2.12 Arduino IDE

Arduino IDE (*Integrated Development Environment*) merupakan sebuah *platform* pengembangan yang didesain secara khusus untuk pemrograman dan penelitian menggunakan *platform* Arduino. Arduino sendiri adalah sebuah *platform* perangkat keras yang mencakup papan sirkuit mikrokontroler serta lingkungan pengembangan perangkat lunak yang memfasilitasi pembuatan dan pengujian berbagai proyek elektronik. *Platform* ini telah menjadi pilihan populer di kalangan penggemar elektronika, pelajar, dan profesional karena kemudahannya dalam penggunaan serta fleksibilitasnya dalam berbagai aplikasi. Arduino IDE menyediakan antarmuka yang intuitif bagi pengguna untuk menulis, mengedit, dan mengunggah kode program ke papan Arduino. Dengan bahasa pemrograman yang mirip dengan C/C++, pengguna dapat dengan mudah mengembangkan berbagai proyek mulai dari yang sederhana hingga yang kompleks, seperti sistem otomatisasi rumah, robotika, sensor, dan banyak lagi. Selain itu, Arduino IDE mendukung berbagai macam papan Arduino, termasuk Uno, Mega, Nano, dan lainnya, sehingga

memungkinkan penggunaan dalam berbagai jenis proyek. *Platform* Arduino juga didukung oleh komunitas besar yang aktif, menyediakan banyak sumber daya, tutorial, dan perpustakaan (*libraries*) yang dapat mempercepat proses pengembangan proyek. Pengguna dapat dengan mudah menemukan contoh kode, skema sirkuit, dan diskusi yang membantu dalam menyelesaikan permasalahan teknis yang mungkin dihadapi. Dengan ekosistem yang komprehensif ini, Arduino IDE dan *platform* Arduino memberikan peluang besar bagi inovasi dan eksperimen dalam dunia elektronika dan pemrograman. Seperti gambar 2.12 [5].

Gambar 2. 12 Fitur Arduino IDE

Langkah-langkah dalam mengunggah skrip dalam Arduino IDE sebagai berikut:

1. Pastikan ESP32-CAM terhubung ke papan pengembangan dan terhubung ke komputer melalui kabel USB.
2. *Instal Board* ESP32-CAM di Arduino IDE dengan menambahkan *URL https://dl.espressif.com/dl/package_esp32_index.json* di "*Preferences*" > "*Additional Boards Manager URLs*". Selanjutnya, instal pustaka ESP32 dari *Espressif Systems* melalui "*Tools*" > "*Board*" > "*Boards Manager*".

3. Pilih *Board* ESP32-CAM dengan menu "*Tools*" > "Board" > "*ESP32 Wrover Module*".
4. Konfigurasi port dan kecepatan unggah di "*Tools*" > "*Port*" dan "*Tools*" > "*Upload Speed*".
5. Unggah skrip ke ESP32-CAM dengan membuka skrip Arduino, memeriksa dan menyuaikan konfigurasi pin serta pengaturan lainnya, lalu klik ikon "*Upload*" atau tekan Ctrl + U.
6. Amati hasilnya melalui Serial Monitor untuk melihat debug dan pesan keluaran.
7. Pastikan proses unggah selesai tanpa kesalahan.
8. Periksa perangkat ESP32-CAM untuk memastikan bahwa skrip berjalan sesuai yang diharapkan setelah proses unggah selesai.

2.2.13 *Confusion Matrix*

Kecerdasan buatan (*artificial intelligence*) adalah cabang ilmu yang mempelajari bagaimana komputer dapat melakukan tugas-tugas yang biasanya memerlukan kecerdasan manusia. Salah satu aspek penting dari kecerdasan buatan adalah machine learning, yang memungkinkan komputer untuk belajar dari data dan meningkatkan kinerjanya seiring waktu. *Machine learning* melibatkan penggunaan berbagai jenis dataset. Dalam konteks ini, kita akan membahas tentang *supervised learning*, di mana model prediksi diketahui berdasarkan data pelatihan yang telah diberikan. Seperti tabel 2.13.

		Predicted	
		Negative **(N)** -	Positive **(P)** +
Actual	Negative -	True Negative **(TN)**	**False Positive (FP) Type I Error**
	Positive +	**False Negative (FN) Type II Error**	True Positive **(TP)**

Gambar 2. 13 Tabel *Confusion Matrix*

Machine Learning merupakan salah satu cabang dari disiplin ilmu kecerdasan buatan (*artificial intelligence*) yang membahas bagaimana sistem

dibangun berdasarkan pada data. Jadi *machine learning* merupakan proses komputer untuk belajar dari data (*learn from* data). Jika tidak ada data, komputer tidak akan bisa belajar. Salah satu teknik aplikasi pada *machine learning* adalah *supervised learning*. Klasifikasi merupakan *supervised learning*, yang merupakan model prediksi dimana hasil prediksinya bersifat diskrit. Bagaimana mengukur performa dari model klasifikasi yang digunakan? Jawaban sederhananya adalah membandingkan nilai aktual dengan nilai prediksi. *Confusion Matrix* adalah pengukuran performa untuk masalah klasifikasi *machine learning* dimana keluaran dapat berupa dua kelas atau lebih. *Confusion Matrix* adalah tabel dengan 4 kombinasi berbeda dari nilai prediksi dan nilai aktual. Ada empat istilah yang merupakan representasi hasil proses klasifikasi pada *confusion matrix* yaitu *True Positif, True Negatif, False Positif,* dan *False Neg*atif [14].

Akurasi, presisi, *recall,* dan skor F-1 dapat dihitung menggunakan rumus-rumus berikut:

Rumus untuk menghitung akurasi (5)

$$A = \frac{TP+TN}{TP+TN+FP+FN} \text{ x } 100\% \quad (5)$$

Akurasi menggambarkan seberapa akurat model dapat mengklasifikasikan dengan benar. Maka, *accuracy* merupakan rasio prediksi benar (positif dan negatif) dengan keseluruhan data. Dengan kata lain, *accuracy* merupakan tingkat kedekatan nilai prediksi dengan nilai aktual (sebenarnya). Nilai *accuracy* dapat diperoleh dengan persamaan [1].

Rumus untuk menghitung presisi (6)

$$P = \frac{TP}{TP+FP} \quad (6)$$

Presisi menggambarkan tingkat keakuratan antara data yang diminta dengan hasil prediksi yang diberikan oleh model. Maka, *precision* merupakan rasio prediksi benar positif dibandingkan dengan keseluruhan hasil yang diprediksi positf. Dari semua kelas positif yang telah di prediksi dengan benar, berapa banyak data yang benar-benar positif. Nilai *precision* dapat diperoleh dengan persamaan [2].

Rumus untuk menghitung *Recall* (7)

$$R = \frac{TP}{TP+FN} \quad (7)$$

Recall menggambarkan keberhasilan model dalam menemukan kembali sebuah informasi. Maka, *recall* merupakan rasio prediksi benar positif dibandingkan dengan keseluruhan data yang benar positif. Nilai *recall* dapat diperoleh dengan persamaan [3].

Rumus untuk menghitung F1 *Score* (8)

$$\text{F1} = 2 \text{ x } \frac{P \ X \ R}{R+P} \quad (8)$$

F-1 *Score* menggambarkan perbandingan rata-rata *precision* dan *recall* yang dibobotkan. *Accuracy* tepat digunakan sebagai acuan performansi algoritma jika dataset memiliki jumlah data *False* Negatif dan *False* Positif yang sangat mendekati (*symmetric*). Namun jika jumlahnya tidak mendekati, maka sebaiknya menggunakan F1 *Score* sebagai acuan [16].

Keterangan:

- True Positive (TP): Jumlah data yang diklasifikasikan dengan benar sebagai positif.
- True Negative (TN): Jumlah data yang diklasifikasikan dengan salah sebagai negatif.
- False Positive (FP): Jumlah data yang benar diklasifikasikan sebagai negatif.
- False Negative (FN): Jumlah data yang salah diklasifikasikan sebagai positif.

Keterangan ini berfungsi untuk menjelaskan empat kategori utama yang sangat penting dalam evaluasi performa model klasifikasi, yang sering digunakan dalam konteks machine learning dan statistik. Keempat kategori ini membantu kita mengukur akurasi dan efektivitas dari model prediksi yang sedang diuji. Dengan memahami dan menganalisis keempat kategori ini kita dapat menghitung berbagai metrik evaluasi performa model yang lebih kompleks. Beberapa metrik tersebut meliputi akurasi, presisi, recall, dan F1-score. Dengan menghitung dan menganalisis metrik-metrik ini, kita mendapatkan gambaran yang lebih komprehensif tentang kekuatan dan kelemahan model klasifikasi yang digunakan. Memahami kategori-kategori ini juga membantu dalam mengidentifikasi dan mengurangi kesalahan yang mungkin terjadi selama proses klasifikasi, sehingga model prediksi dapat diandalkan dan memberikan hasil yang akurat dalam aplikasi nyata.