

Implementasi Sistem Keamanan Brankas Berbasis Face Recognition Menggunakan Algoritma YOLO dengan Verifikasi Fingerprint

Amanda Tsabita Putri¹, Irma Salamah^{2*}, Martinus Mujur Rose³

^{1,2,3} Program Studi Teknik Telekomunikasi, Jurusan Teknik Elektro, Politeknik Negeri Sriwijaya, Palembang, Sumatera Selatan, Indonesia

e-mail: amanda.tsabita2303@gmail.com¹, irma_salamah@polsri.ac.id^{2*}, mujur@polsri.ac.id³

Informasi Artikel

Article History:

Received : 22 Mei 2025
Revised : 3 Juni 2025
Accepted : 13 Juni 2025
Published : 30 Agustus 2025

***Korespondensi:**

irma_salamah@polsri.ac.id

Keywords:

Face Recognition, Fingerprint, Security, YOLO

Hak Cipta ©2025 pada Penulis.
Dipublikasikan oleh Universitas
Dinamika



Artikel ini open access di bawah
lisensi [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/).



10.37802/joti.v7i2.1072

**Journal of Technology and
Informatics (JoTI)**

P-ISSN 2721-4842

E-ISSN 2686-6102

<https://e-journals.dinamika.ac.id/index.php/joti>

Abstract:

Current technological developments make security crucial in protecting important documents. Safes are commonly used for storage but remain vulnerable to burglary despite conventional locks. Based on data from the Central Bureau of Statistics (BPS) in 2023, aggravated theft was the most frequent crime with 62,872 reported cases. This highlights the need to improve safe security by adding biometric techniques such as face recognition and fingerprint verification. This study proposes a layered security system combining face recognition using the YOLO algorithm and fingerprint sensors. The system uses an ESP32-CAM to capture facial images and an ESP32 microcontroller to control a solenoid lock, fingerprint sensor and buzzer alarm. Face recognition testing on two users showed, the trained YOLO model achieved an accuracy of 83.33%, precision of 83,33% and recall of 100%. from 12 trials, with two failures due to poor lighting conditions. Fingerprint testing on 10 samples, five fingers from each of two users, showed successful recognition of all fingerprints with an average response time of 1.41 seconds. The integration of face and fingerprint biometrics significantly enhances safe security and minimizes unauthorized access risks.

PENDAHULUAN

Keamanan merupakan aspek yang sangat krusial dalam menjaga aset kantor dan dokumen penting yang ada. Oleh karena itu, diperlukan tempat penyimpanan yang aman untuk menghindari risiko kehilangan ataupun penyalahgunaan dari pihak yang tidak bertanggung jawab. Salah satu cara untuk menerapkan keamanan untuk penyimpanan tersebut dengan menerapkan keamanan dengan menggunakan brankas [1]. Hal tersebut karena brankas merupakan sebuah tempat penyimpanan yang terbuat dari besi atau baja yang dirancang untuk melindungi barang-barang berharga dari pencurian, maupun

kerusakan dan dilengkapi dengan sistem keamanan seperti kunci manual dan kombinasi pin [2]. Akan tetapi, kasus pembobolan masih sering terjadi.

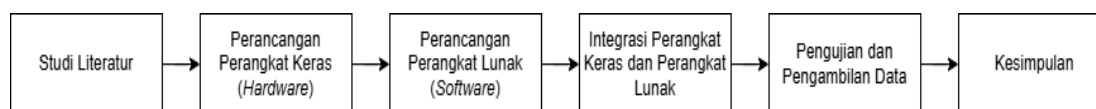
Berdasarkan data dari Badan Pusat Statistik (BPS) pada tahun 2023 kasus pencurian dengan pemberatan menjadi jenis kejahatan terbesar dengan total 62.872 kejadian [3]. Contoh kasusnya pada tahun 2023 seorang karyawan di toko ritel Palembang berhasil membobol brankas ditempatnya bekerja dan mencuri uang sebesar Rp. 60.000.000 dengan mengakses bagian kunci brankas [4]. Hal ini menandakan bahwa sistem keamanan pada brankas konvensional masih memiliki tingkat keamanan yang rendah dan perlu ditingkatkan dengan cara penambahan sistem keamanan lainnya seperti biometrik. Teknik biometrik dilakukan dengan memanfaatkan bagian tubuh seperti sidik jari, atau wajah diterapkan sebagai *face recognition* dan *fingerprint*. Penelitian oleh Immanuel dkk (2024) telah mengembangkan sistem keamanan brankas berbasis biometrik menggunakan *face recognition* dan *fingerprint*, namun belum menerapkan metode deteksi berbasis YOLO untuk pengenalan wajah [5]. Pada pengembangan teknologi *Face recognition* dapat dikembangkan dengan cara memanfaatkan kecerdasan buatan berbasis *deep learning* salah satunya dengan menggunakan algoritma *You Look Only Once* (YOLO) yang mampu mendeteksi objek termasuk wajah secara *real-time* dengan tingkat akurasi yang tinggi [6]. Algoritma ini pernah diterapkan oleh penelitian yang dilakukan oleh putri dkk. (2025) untuk merancang sistem keamanan pada pintu [7]. Selain itu, Salamah dkk. Juga menerapkan algoritma YOLO sebagai alat identifikasi wajah pada sistem presensi mahasiswa yang terhubung dengan website [8].

Beberapa penelitian sebelumnya juga telah dilakukan untuk meningkatkan sistem keamanan pada brankas melalui penerapan teknologi biometrik dan teknologi lainnya. Pada penelitian Arsyad dan Kartika (2021) mengembangkan sistem keamanan brankas menggunakan sensor sidik jari yang berfungsi untuk membuka brankas serta memberikan notifikasi melalui buzzer apabila ada akses yang tidak sah. Meskipun demikian, sistem ini masih menggunakan autentikasi tunggal sehingga masih rentan terhadap pembobolan [2]. Penelitian selanjutnya yang dilakukan oleh Alfiandi dkk. (2022) memanfaatkan metode berbasis *deep learning Convolutional Neural Network* (CNN) dalam mendeteksi wajah untuk membuka brankas, namun penelitian ini memerlukan perangkat keras yaitu Raspberry Pi dengan biaya yang tinggi [9].

Berdasarkan penelitian-penelitian sebelumnya, masih terdapat celah keamanan baik dari sisi autentikasi tunggal maupun dari keterbatasan perangkat keras yang digunakan. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sistem keamanan brankas berbasis biometrik ganda dengan menggabungkan *face recognition* menggunakan algoritma YOLO dan verifikasi *fingerprint*. Sistem ini dirancang menggunakan ESP32-CAM untuk pemindaian wajah dan sensor *fingerprint* sebagai verifikasi tambahan, yang kemudian diintegrasikan ke dalam mikrokontroler ESP32 untuk mengendalikan *solenoid lock* dan memberikan notifikasi menggunakan *buzzer* jika terjadi akses yang tidak sah. Keunggulan dari sistem ini dibandingkan penelitian sebelumnya adalah penggunaan metode deteksi wajah yang lebih akurat dengan performa tinggi, penggabungan verifikasi ganda berbasis biometrik, serta penerapan perangkat keras yang efisien dan hemat biaya.

METODE

Metode tahapan penelitian ini dibuat dalam bentuk diagram untuk memberikan gambaran secara keseluruhan tentang tahapan-tahapan yang akan dilakukan pada penelitian yang akan dilakukan. Kerangka pemikiran dalam blok diagram dapat dilihat pada Gambar 1.



Gambar 1. Blok Diagram

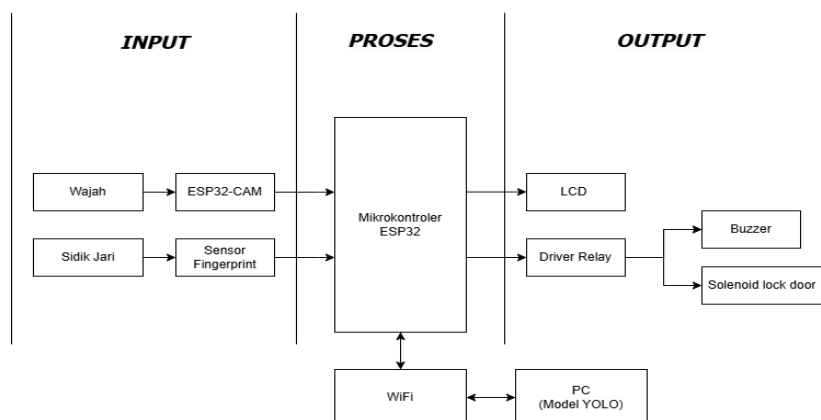
1) Studi Literatur

Studi literatur merupakan tahapan peneliti dalam mengambil beberapa data yang berasal dari berbagai sumber seperti buku, skripsi, thesis, jurnal dan internet sebagai acuan referensi dalam penelitian yang akan dilakukan.

2) Perancangan Perangkat

2.1 Perancangan Perangkat Keras (Hardware),

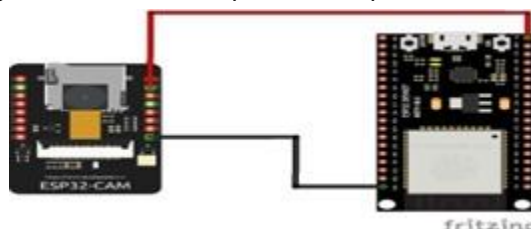
Perancangan perangkat keras melibatkan pembuatan perangkat yang akan digunakan. Komponen-komponen harus sesuai dengan karakteristik yang dibutuhkan oleh alat. Perancangan perangkat keras dimulai dengan membuat blok diagram seperti yang ada pada Gambar 2.



Gambar 2. Perancangan Perangkat Keras

- Rangkaian Koneksi ESP32-cam dengan Mikrokontroler ESP32,**

ESP32-CAM berfungsi untuk melakukan pengambilan citra dari wajah pengguna melalui sensor kamera cmos OV2640. Citra tersebut dikirim secara *real-time* melalui *streaming* berbasis IP address menggunakan *WiFi*. Alamat IP dari ESP32-CAM diakses oleh laptop yang menjalankan model YOLO untuk deteksi wajah. Proses deteksi wajah dilakukan pada laptop, sedangkan ESP32-CAM hanya bertindak sebagai kamera *streaming*. Gambar rangkaian tersebut dapat dilihat pada Gambar 3.

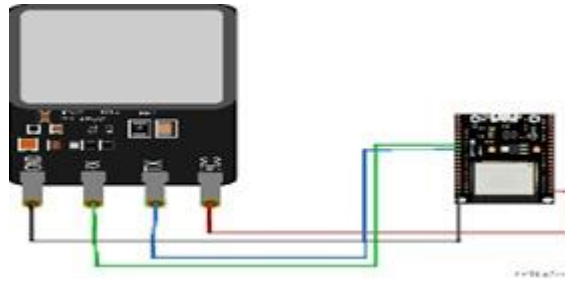


Gambar 3. Rangkaian Koneksi ESP32-CAM

- Rangkaian Koneksi Sensor *fingerprint* AS608 ke ESP32**

Pada sistem ini, sensor *fingerprint* yang digunakan adalah tipe AS608 yang berkomunikasi dengan mikrokontroler ESP32. Sensor *fingerprint* memiliki empat pin utama yaitu VCC, GND, TX, dan RX. Pin VCC sensor dihubungkan ke sumber tegangan pada ESP32 untuk memberikan daya, sedangkan pin GND dihubungkan ke ground ESP32. Pin TX pada sensor *fingerprint* berfungsi untuk mengirim data ke ESP32 dan oleh

karena itu dihubungkan ke pin RX ESP32 yaitu GPIO16, sedangkan pin RX sensor berfungsi menerima data dari ESP32 dan dihubungkan ke pin TX ESP32 yaitu pin GPIO17. Gambar rangkaian tersebut dapat dilihat pada Gambar 4.



Gambar 4. Rangkaian Koneksi *Sensor fingerprint AS608* ke ESP32

- **Rangkaian Koneksi ESP32-Relay-Solenoid Lock Door**

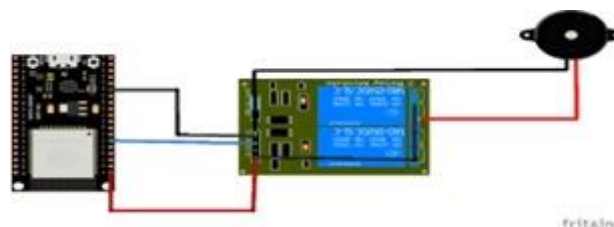
Pengunci pintu brankas dikendalikan oleh *relay* yang menerima sinyal dari mikrokontroler ESP32. Mikrokontroler ESP32 mengirimkan sinyal digital melalui pin GPIO2 untuk mengaktifkan atau mematikan *relay*. Ketika *relay aktif*, arus dari sumber daya dari *power supply* mengalir ke solenoid sehingga kunci terbuka. Sebaliknya, jika *relay* tidak *aktif*, arus terputus dan solenoid mengunci kembali pintu brankas. Gambar rangkaian tersebut dapat dilihat pada Gambar 5.



Gambar 5. Rangkaian Koneksi ESP32-Relay-Solenoid Lock Door

- **Rangkaian Koneksi ESP32-Relay-Buzzer**

Buzzer digunakan sebagai indikator suara yang memberikan notifikasi pada sistem keamanan brankas ini. *Buzzer* dikendalikan melalui modul *relay* yang dihubungkan dengan mikrokontroler ESP32 dimana pin GPIO4 mengirimkan sinyal digital dari ESP32 untuk mengaktifkan *relay*, sehingga sumber daya dari *power supply* dapat dialirkan ke *buzzer* untuk menghasilkan suara. Gambar rangkaian tersebut dapat dilihat pada Gambar 6.

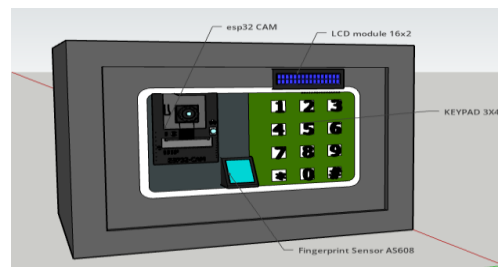


Gambar 6. Rangkaian Koneksi ESP32-Relay-Buzzer

- **Perancangan Mekanik**

Akan dilakukan pembuatan desain alat untuk *Implementasi Sistem Keamanan Brankas Berbasis Face Recognition Menggunakan Algoritma Yolo Dengan Verifikasi Fingerprint*. Desain kontruksi alat akan dibuat dengan merancang brankas dengan untuk meletakkan komponen-komponen yang akan digunakan seperti ESP32-CAM, Sensor *Fingerprint AS608*, LCD *buzzer* dan lain-lain. brankas ini berbentuk kubus dengan ukuran

sisi panjang 43cm, lebar 35cm, dan tinggi 20 cm. *Desain* brankas yang telah dibuat dapat dilihat pada Gambar 7.

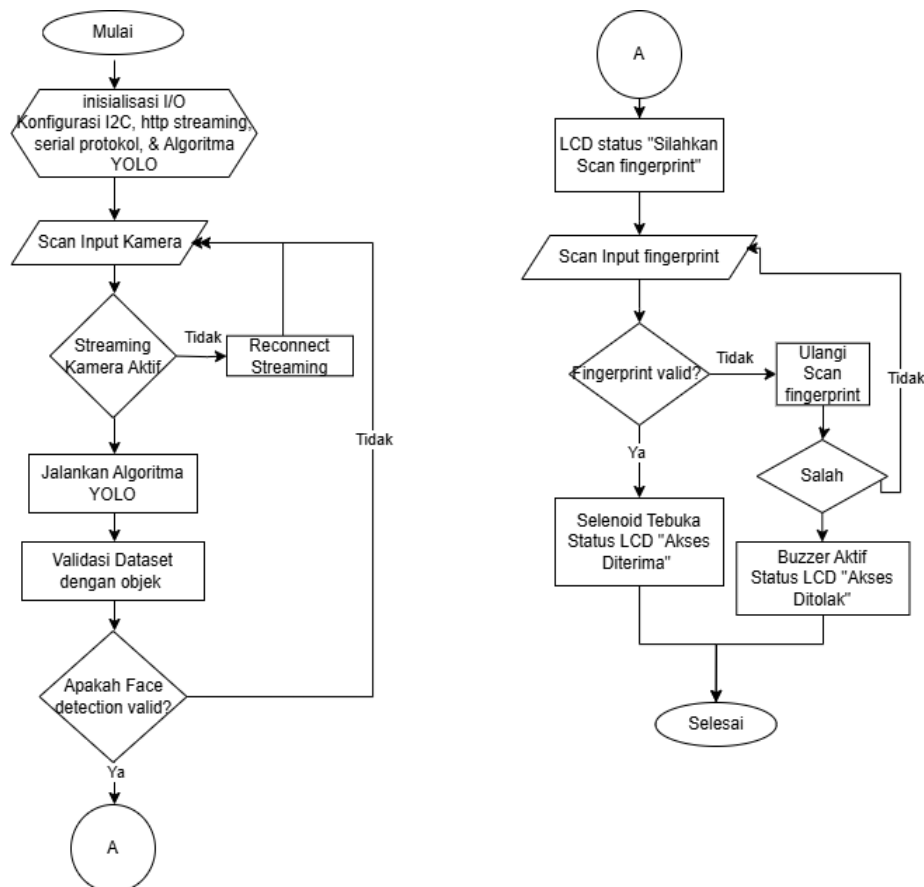


Gambar 7. *Desain* Brankas

2.2 Perancangan Perangkat Lunak (*Software*)

2.2.1 Perancangan Model Deteksi Wajah dengan *Algoritma* YOLO untuk Proses Pengenalan wajah (*Face Recognition*)

2.2.2 *Flowchart* Kerja Sistem



Gambar 8. *Flowchart*

Pada Gambar 8 merupakan *flowchart* sistem. Sistem ini dimulai dengan inisialisasi sensor dan *output*, termasuk konfigurasi I2C untuk komunikasi LCD, *http streaming* digunakan untuk video streaming dari ESP32-CAM, *serial protocol* sebagai komunikasi data ke mikrokontroler ESP32, dan algoritma YOLO untuk pedeteksian wajah. Setelah itu, kamera ESP32-CAM akan memindai wajah pengguna dan mencocokkannya dengan data yang telah diproses dengan model YOLO tadi. Jika wajah tidak terdeteksi maka akan kembali ke *scan input* wajah, apabila wajah terdeteksi, LCD akan menampilkan informasi untuk pemindaian sidik jari, Jika sidik jari sesuai, sistem akan membuka

brankas dan menampilkan status "akses diterima" pada tampilan LCD. Namun, jika sidik jari tidak terdeteksi maka *buzzer* akan *aktif*, dan *user* harus mengulangi pemindaian.

2.2.3 Pengujian Sistem

Pengujian sistem dilakukan secara menyeluruh untuk memahami bagaimana alat beroperasi dalam keseluruhan tahap pengujian, yaitu:

- 1) Pengujian terhadap kinerja model yang telah di *training* untuk *face recognition* dengan menggunakan model *You Only Look Once* (YOLO) dilakukan untuk mengevaluasi performa model. Evaluasi ini menggunakan parameter pengukuran seperti akurasi, *recall*, dan *precision*. Adapun untuk proses evaluasi ini menggunakan rumus sebagai berikut:

$$\text{Akurasi} = \frac{\text{Pengujian berhasil}}{\text{Total Pengujian}} \times 100\% \quad (1)$$

$$\text{Recall} = \frac{TP}{TP+FP} \times 100\% \quad (2)$$

$$\text{Precision} = \frac{TP}{TP+FN} \times 100\% \quad (3)$$

- 2) Pengujian secara keseluruhan memastikan semua komponen sistem keamanan brankas berfungsi dengan baik. ESP32-CAM menangkap citra wajah dan mengidentifikasinya menggunakan model YOLO yang sudah di *training*. Jika wajah terdeteksi, sistem melanjutkan verifikasi sidik jari dengan sensor *fingerprint*, apabila kedua akses berhasil *solenoid lock* akan membuka brankas.

HASIL DAN PEMBAHASAN

1) Hasil Perancangan Perangkat Keras (*Hardware*)

Pada blok *input* Gambar 9, terdiri dari *fingerprint* sensor dan ESP32-CAM yang berfungsi sebagai masukan bagi sistem untuk pemrosesan lebih lanjut oleh blok proses. Pemrosesan ini dilakukan melalui algoritma yolo untuk mengidentifikasi wajah pengguna yang telah didaftarkan sebagai pengguna yang telah terdaftar, lalu data tersebut dikirimkan ke mikrokontroler ESP32. Adapun pada sisi output, terdapat *interface* LCD 16x2 sebagai penampil informasi, *buzzer* sebagai indikator suara hasil deteksi, dan *output* solenoid sebagai fungsi utama sistem pengamanan brankas yang akan aktif ketika pengguna sah mengakses sistem keamanan ini. Seluruh rangkaian ini terhubung dengan *power supply* yang menyediakan arus listrik ke setiap komponen dalam sistem.



Gambar 9. Perangkat Keras (*Hardware*) dan Rangkaian Sistem

2) Hasil Perancangan Perangkat Lunak (*Software*)

2.1 Perancangan Model *You Only Look Once* (YOLO)

Perangkat lunak yang digunakan untuk mendeteksi wajah adalah model *You Only Look Once* (YOLO) yang bekerja dengan mendeteksi objek secara langsung di seluruh gambar dalam satu langkah, sehingga menghasilkan prediksi yang cepat dan akurat.

Untuk meningkatkan akurasi deteksi wajah pada model YOLO, dataset khusus yang berisi gambar wajah digunakan dalam pelatihan model.

2.2 Proses pengumpulan dataset

Proses ini dilakukan dengan mengambil citra wajah dari dua individu yang berbeda, kemudian pengguna dibuat label atau kelas yang berbeda. Dataset dikumpulkan menggunakan kamera *smartphone* dengan format (.jpg). Total terdapat 200 citra wajah yang berhasil dikumpulkan. Dengan masing-masing kelas terdiri dari 100 sampel foto. Pengambilan gambar dilakukan dalam berbagai kondisi pencahayaan, sudut pengambilan gambar, dan ekspresi wajah untuk meningkatkan keberagaman data.

2.3 Pre-processing Citra

Proses ini dilakukan menggunakan *platform roboflow* untuk mempermudah pemrosesan anotasi dan pengelolaan dataset. Setiap gambar dianotasi atau di label dengan kotak pembatas (*bounding box*). Anotasi ini diperlukan agar model dapat belajar untuk mengenali wajah secara akurat dan efektif [10]. Gambar yang sudah dianotasi kemudian diproses dan dipersiapkan untuk pelatihan model, termasuk *resizing* ke format 640x640 piksel dan proses augmentasi seperti *rescale*, *zoom*, *flip* agar meningkatkan kualitas untuk membantu mencegah *overfitting* dan meningkatkan jumlah data pelatihan dengan membuat variasi dari data yang sudah ada seperti yang terlihat pada Gambar 10 yang merupakan hasil *pre-processing* dataset yang telah dilakukan.



Gambar 10. Hasil Pre-Processing

Selanjutnya, proses pemisahan atau *splitting* dataset untuk membagi 70% menjadi data *train*, 20% data *valid*, 10% data *testing*. Dataset pelatihan diambil 70% dari total keseluruhan dataset untuk digunakan dalam pelatihan agar model dapat mengenali objek secara optimal dan mempelajari pola-pola dari data yang ada, Selanjutnya 20% data valid digunakan untuk memantau performa model selama pemrosesan pelatihan dan berfungsi untuk mencegah terjadinya *overfitting*. Kemudian 10% data *testing* digunakan untuk mengevaluasi performa model secara objektif setelah proses pelatihan selesai.

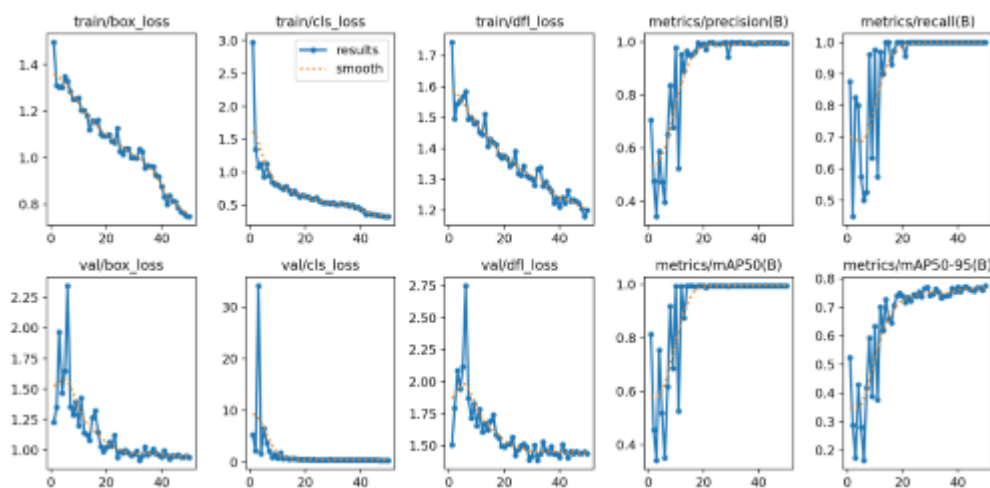
2.4 Pelatihan Model

Proses pengambilan dataset dilakukan menggunakan bantuan *platform Roboflow* yang terintegrasi langsung melalui kode *Python*. Langkah awal dimulai dengan pembuatan direktori bernama *datasets*, yang bertujuan sebagai lokasi penyimpanan

dataset yang diunduh. Setelah itu, akun *Roboflow* dihubungkan dengan menggunakan API key dari platform *roboflow*, kemudian sistem diarahkan untuk mengakses *workspace* dan memilih proyek dataset yang akan digunakan. Pelatihan model ini memanfaatkan fasilitas GPU yang telah tersedia dari *Google Colaboratory* [11]. Setelah dataset selesai dibuat dan diproses, Sebelum melakukan *training* perlu dilakukannya *custom training* yaitu mengatur beberapa parameter seperti *epochs* dan *image size* menyesuaikan kebutuhan yang diperlukan untuk model. Pada penelitian ini dilakukan proses pelatihan dengan menggunakan model *yolo8s.pt* yang dirancang dengan 50 epoch dan image size diatur menjadi 640x640 piksel untuk melatih dataset. Pemilihan parameter ini mengacu pada penelitian yang dilakukan oleh Adrezo dkk. (2024) yang menggunakan parameter serupa pada model YOLOv8 untuk mendeteksi wajah berdasarkan jenis kelamin. Penelitian tersebut menunjukkan bahwa penggunaan parameter ini mampu mendukung proses pelatihan model dan memperoleh performa model yang baik [12].

Parameter *epochs* menentukan berapa kali seluruh data latih di proses secara keseluruhan dalam melatih model untuk mempelajari pola-pola yang terdapat dalam data latih untuk meminimalisir kesalahan dalam proses pengenalan wajah. Proses pelatihan dilakukan sebanyak 50 *epoch* dengan waktu total pelatihan selama 0,136 jam. File hasil pelatihan yang telah dilakukan kemudian disimpan dengan nama *file best.pt*. File ini dihasilkan secara otomatis setelah proses pelatihan model selesai dilaksanakan, Kemudian file ini dapat diintegrasikan ke dalam sistem atau perangkat keras untuk keamanan brankas.

2.5 Hasil Training



Gambar 11. Hasil *Evaluasi Model*

Berdasarkan Gambar 11, grafik hasil pelatihan dan *evaluasi* model selama 50 *epoch*, terlihat bahwa proses pembelajaran berjalan dengan stabil. Nilai *loss* pada data pelatihan, yang mencakup *train box loss*, *train classification loss*, dan *train dfl_loss*, menunjukkan penurunan yang konsisten, hal ini menandakan bahwa model semakin akurat dalam mengenali dan mengklasifikasikan objek wajah. Penurunan nilai juga terlihat pada data validasi yaitu *validation box loss*, *validation classification loss*, dan *validation dfl_loss*, yang menandakan bahwa model tidak mengalami *overfitting* dan mampu melakukan generalisasi terhadap wajah.

Pada *epoch* ke-50, yang merupakan *epoch* terakhir, performa model mencapai hasil yang optimal dengan nilai *box loss* sebesar 0.7469, *classification loss* sebesar 0.3274, dan *dfl_loss* sebesar 1.199. Hal ini menunjukkan bahwa kesalahan prediksi model berada pada tingkat yang rendah. Dari sisi evaluasi metrik, model diuji berhasil memperoleh nilai *precision* sebesar 0.994 dan *recall* sebesar 1.0, yang berarti model hampir berhasil mengenali semua wajah yang ada dalam data uji. Selain itu, mAP50 mencapai 0.995, dan mAP pada berbagai ambang mAP50-95 sebesar 0.774, menunjukkan bahwa model sangat andal dalam mengenali wajah dengan akurasi tinggi pada berbagai skenario. Hasil ini menunjukkan bahwa model pengenalan wajah yang dilatih dengan model *You Only Look Once* (YOLO) sangat *efektif* dan akurat untuk digunakan dalam *implementasi* sistem keamanan pada brankas.

2.6 Intergrasi Model Ke Perangkat Keras

File hasil latih disimpan dengan nama *best.pt* sebagai model yang digunakan untuk proses deteksi wajah yang akan diintegrasikan dengan sistem perangkat keras yaitu sistem brankas yang telah dirancang dan dilengkapi dengan sensor *fingerprint* sebagai sistem *verifikasi* tambahan untuk membuka brankas. Komunikasi antara model dan perangkat keras ini dilakukan menggunakan melalui protokol komunikasi asinkron, yaitu UART (*Universal Asynchronous Receiver and Transmitter*). Melalui konfigurasi tersebut, kode *python* akan menjalankan model dengan nama *best.pt* dan mengirimkan hasil deteksi wajah melalui sensor kamera ESP32-CAM, kemudian data tersebut diterima oleh mikrokontroler ESP32.

Proses koneksi ini melibatkan komunikasi data dengan protokol serial asinkron menggunakan parameter: *Baudrate* = 115200 bps, *Bytesize* = 8 bit, *Parity* = none, *Stopbit* = 1 dengan mengirimkan karakter "1" sebagai hasil deteksi wajah ke mikrokontroler ESP32. Proses ini menggunakan bahasa pemrograman *python* untuk menghubungkan dan menjalankan komunikasi antara perangkat lunak yang menjalankan model untuk deteksi wajah dengan perangkat keras berupa mikrokontroler ESP32 untuk menjalankan proses selanjutnya. Pengaksesan kamera ESP32-CAM menggunakan HTTP (*Hypertext Transfer Protocol*) dengan alamat IP yang telah ditentukan sesuai dengan perangkat yang dipakai. Proses ini digunakan untuk mengambil citra wajah secara langsung dari ESP32-CAM yang kemudian akan diproses lebih lanjut menggunakan algoritma YOLO melalui URL *endpoint* <http://172.20.10.4/capture>. Setelah data *validasi* deteksi wajah berhasil diterima, mikrokontroler ESP32 akan melanjutkan proses selanjutnya yaitu, *verifikasi fingerprint*. *Verifikasi fingerprint* ini dibaca oleh ESP32 kemudian dibandingkan dengan data sidik jari yang telah terdaftar.

3) Hasil Pengujian Face Recognition

Proses ini diawali dengan menghadapkan wajah pada sensor kamera ESP32-cam, selanjutnya ESP32-cam akan melakukan pemindaian melalui video *capture* dan mengirimkan data melalui *streaming web*. video *streaming* kemudian akan diambil menjadi *image capture* yang selanjutnya akan diolah sebagai data input sistem melalui algoritma YOLO. Ketika sistem mengidentifikasi kesesuaian dengan dataset yang telah dilatih memiliki *confidence* sebesar 70% maka sistem pengidentifikasian wajah akan mengirimkan hasil deteksi untuk pemrosesan selanjutnya, yaitu ke tahap verifikasi *fingerprint*. Hasil pengujian ini dilakukan dalam kondisi wajah yang bervariasi seperti

wajah menghadap depan, kanan, kiri, atas, bawah dan kondisi pencahayaan yang gelap. Pada tabel 1 merupakan hasil pengujian *face recognition*.

Tabel 1. Hasil Pengujian *Face Recognition*

Gambar	Parameter	Status
	Wajah menghadap kedepan	Berhasil Dikenali
	Pencahayaan Gelap	Tidak Terdeteksi
	Wajah menghadap kedepan	Berhasil dikenali
	Pencahayaan Gelap	Tidak Terdeteksi

Hasil pengujian pada percobaan pengenalan wajah (Tabel 1) (*face recognition*) dari pemilik brankas yang diuji pada 2 orang dengan kriteria pengujian yang berbeda. Proses pengenalan wajah ini dapat bekerja dengan baik kecuali pada saat pendeteksian dengan kondisi pencahayaan yang gelap. Hasil evaluasi dapat dihitung dengan menggunakan perhitungan terhadap ketepatan pengenalan wajah sebagai berikut.

$$Akurasi = \frac{\text{Pengujian berhasil}}{\text{Total Pengujian}} \times 100\%$$

$$Akurasi = \frac{10}{12} \times 100\%$$

$$Akurasi = 0,833 \times 100\%$$

$$Akurasi = 83,3\%$$

$$Recall = \frac{TP}{TP+FP} \times 100\%$$

$$Recall = \frac{10}{10+2} \times 100\%$$

$$Recall = 0,833 \times 100\%$$

$$Recall = 83,3\%$$

$$Precision = \frac{TP}{TP+FN}$$

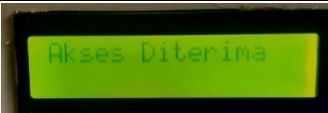
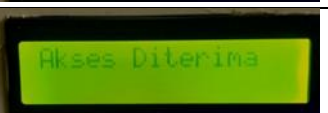
$$Precision = \frac{10}{10+0} \times 100\%$$

$$Precision = 100\%$$

4) Hasil Pengujian *Fingerprint*

Pengujian *fingerprint* (Tabel 2) dilakukan untuk memastikan bahwa sensor sidik jari yang digunakan mampu mem-*verifikasi* identitas pengguna secara akurat sebagai bagian dari sistem keamanan pada brankas. Pengujian ini mengukur tingkat keberhasilan sensor dalam mendeteksi sidik jari pengguna dan kecepatan waktu respons sensor yang ditunjukkan pada tabel dibawah ini.

Tabel 2. Hasil Pengujian Fingerprint

Uji Coba	Fingerprint	Status	Waktu Respons (detik)	Tampilan LCD
User manda	Jari Jempol Kanan	Terdeteksi	1,38	
	Jari Telunjuk Kanan	Terdeteksi	1,08	
	Jari Tengah Kanan	Terdeteksi	1,60	
	Jari Manis Kanan	Terdeteksi	1,11	
	Jari Kelingking Kanan	Terdeteksi	1,51	
User salsa	Jari Jempol Kanan	Terdeteksi	0,94	
	Jari Telunjuk Kanan	Terdeteksi	1,82	
	Jari Tengah Kanan	Terdeteksi	1,97	
	Jari Manis Kanan	Terdeteksi	1,23	
	Jari Kelingking Kanan	Terdeteksi	1,46	
Waktu Rata-Rata			1,41 Detik	

Pengujian dilakukan terhadap dua orang pengguna, dengan menggunakan lima jari yang telah terdaftar menggunakan tangan kanan yaitu, jari jempol hingga kelingking. Hasilnya menunjukkan bahwa seluruh jari dari kedua pengguna berhasil terdeteksi oleh sistem, yang menandakan bahwa akurasi sistem mencapai 100% dalam mengenali sidik

jari. Waktu respons dari sistem dalam mendeteksi sidik jari bervariasi, dengan waktu tercepat sebesar 0,94 detik dan waktu paling lama 1,97 detik, dengan hasil waktu rata-rata sebesar 1,41 detik.

5) Hasil Pengujian Keseluruhan Sistem

Pengujian keseluruhan sistem (Tabel 3), membahas hasil dari pengujian keseluruhan sistem yang telah dirancang dan diimplementasikan. Pengujian dilakukan pada seluruh kemungkinan upaya akses pada brankas, dengan kombinasi deteksi wajah dan pemindaian *fingerprint* sebanyak empat kali percobaan kemungkinan pengaksesan. Berdasarkan rancangan sistem yang telah dibuat, sistem hanya akan merespon pembukaan brankas hanya jika wajah berhasil dideteksi sebagai pengguna dan deteksi *fingerprint* benar. Selain kemungkinan tersebut, sistem akan menolak akses pembukaan brankas. Proses pengujian ini dimulai dengan pengambilan citra wajah kemudian diproses menggunakan model YOLO dan melanjutkan proses verifikasi fingerprint untuk membuka akses brankas. Berdasarkan hasil pengujian tersebut, didapatkan rata-rata waktu respon sistem secara keseluruhan adalah 3,03 detik. Seluruh rangkaian proses ini bertujuan untuk memastikan bahwa integrasi antara perangkat keras dan perangkat lunak bekerja dengan baik. Tabel 3 merupakan tabel hasil pengujian keseluruhan sistem yang dirancang.

Tabel 3. Pengujian Keseluruhan Sistem

NO	Status Wajah	Status Fingerprint	Buzzer	Validasi	Solenoid	Waktu Respons (detik)
1.	Wajah Terdeteksi	Benar	Off	Akses Diterima	Tertutup	2,73
2.	Wajah Terdeteksi	Salah	On	Akses Ditolak	Tertutup	2,20
3.	Wajah Tidak Terdeteksi	-	Off	Akses Ditolak	Tertutup	3,09
4.	Wajah Terdeteksi Tapi Bukan Pengguna	Salah	On	Akses Ditolak	Tertutup	4,12
Waktu Rata-Rata						3,03

Peneliti menyadari bahwa masih terdapat sejumlah keterbatasan dalam penelitian ini. Oleh karena itu, disarankan untuk menggunakan dataset dengan jumlah kelas lebih banyak untuk menguji model dalam mengenali dan membedakan lebih banyak individu. Sistem harus diintegrasikan dengan *single board computer* spesifikasi yang lebih tinggi seperti *Raspberry Pi* atau Mini PC lainnya agar waktu respon sistem yang digunakan lebih cepat lagi.

KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian dan analisis yang dilakukan, sistem deteksi wajah menggunakan model YOLO pada sistem keamanan brankas menunjukkan kinerja yang

sangat baik. Model yang telah dilatih berhasil memperoleh nilai *precision* sebesar 0.994 dan *recall* sebesar 1.0. Selain itu, mAP50 mencapai 0.995, dan mAP50-95 sebesar 0.774, yang berarti model hampir berhasil mengenali semua wajah yang ada dalam data uji. Model yang telah dilatih kemudian disimpan dan diintegrasikan dengan perangkat keras melalui protokol komunikasi UART (*Universal Asynchronous Receiver and Transmitter*) yang dihubungkan menggunakan *program python* dan dikirimkan ke mikrokontroler ESP32, integrasi ini dilakukan untuk melanjutkan proses *verifikasi fingerprint* untuk membuka solenoid. Hasil pengujian *face recognition* menunjukkan bahwa dari 12 kali pengujian terhadap dua pengguna, sistem berhasil mendeteksi wajah sebanyak 10 kali, dan gagal 2 kali karena kondisi pencahayaan gelap. Dan tingkat akurasi yang diperoleh sebesar 83,33%, *recall* sebesar 83,33% dan *Precision* sebesar 100%. Hasil pengujian sensor *fingerprint* terhadap 10 sampel sidik jari yaitu, masing-masing lima jari dari dua pengguna, menunjukkan bahwa sistem berhasil mengenali seluruh sidik jari yang diuji dengan rata-rata waktu respons sebesar 1,41 detik. *Notifikasi buzzer* akan berbunyi apabila sensor *fingerprint* gagal mendeteksi sidik jari pengguna brankas dengan benar.

Hasil penelitian yang telah dilakukan menunjukkan bahwa sistem keamanan brankas berbasis *face recognition* menggunakan algoritma YOLO yang dikembangkan dalam penelitian ini memiliki tingkat akurasi yang lebih tinggi dibandingkan dengan penelitian sebelumnya. Pada penelitian yang dilakukan mencapai tingkat akurasi pengenalan wajah sebesar 83.33%. Sedangkan, pada penelitian sebelumnya penggunaan metode Viola-Jones pada keamanan brankas menghasilkan tingkat keberhasilan akurasi wajah hanya sebesar 60% [13]. Perbedaan signifikan ini menunjukkan bahwa implementasi YOLO dalam sistem pengenalan wajah pada brankas memberikan performa yang lebih baik dalam konteks pengenalan wajah secara *real-time* dengan kondisi pencahayaan yang bervariasi. Namun penelitian selanjutnya juga disarankan dapat menambahkan fitur notifikasi seperti *telegram* atau *email* yang bertujuan untuk memberikan peringatan secara *real-time* dari jarak jauh.

DAFTAR PUSTAKA

- [1] M. Ilham Ali, S. Adi Wibowo, and A. Panji Sasmito, "Keamanan Brankas Menggunakan E-Ktp Dan Notifikasi Via Telegram Berbasis Iot (Internet of Things)," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 5, no. 2, pp. 589–596, 2021, doi: 10.36040/jati.v5i2.3793.
- [2] O. R. Arsyad and K. P. Kartika, "Rancang Bangun Alat Pengaman Brankas Menggunakan Sensor Sidik Jari Berbasis Arduino," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 5, no. 1, pp. 1–6, 2021, doi: 10.36040/jati.v5i1.3285.
- [3] BPS (Badan Pusat Statistik), "Statistik Kriminal 2024," vol. Volume 15, 2024.
- [4] P. Syahbana, "Terlilit Pinjol, Karyawati Alfamart di Sumsel Bobol Brankas-Gasak Rp 60 Juta", [Online]. Available: <https://www.detik.com/sumut/hukum-dan-kriminal/d-6559008/terlilit-pinjol-karyawati-alfamart-di-sumsel-bobol-brankas-gasak-rp-60-juta>
- [5] J. M. Immanuel, I. Ibrahim, R. Rahmadewi, and Y. Saragih, "IoT-based Facelook and Fingerprint Safe Security System," *Jurnal Penelitian Pendidikan IPA*, vol. 10, no. 2, pp. 500–505, 2024, doi: 10.29303/jppipa.v10i2.6832.
- [6] D. Ayu, D. Syaiful, and A. Ramelan, "Rancang Bangun Alat Sistem Absensi Mahasiswa menggunakan Face Recognition dengan Metode YOLO berbasis Raspberry Pi," vol. 6, no. 2, 2024. doi: 10.26905/jasiek.v7i2.14144

- [7] H. Putri *et al.*, "Security System for Door Locks Using YOLO-Based Face Recognition," *International Journal on Informatics Visualization*, vol. 9, no. 1, pp. 224–230, 2025, doi: 10.62527/joiv.9.1.2410.
- [8] I. Salamah, M. R. A. Said, and S. Soim, "Perancangan Alat Identifikasi Wajah Dengan Algoritma You Only Look Once (YOLO) Untuk Presensi Mahasiswa," *Jurnal Media Informatika Budidarma*, vol. 6, no. 3, p. 1492, 2022, doi: 10.30865/mib.v6i3.4399.
- [9] M. Fauzan Alfiandi, F. Utaminingrum, and E. Rosana Widasari, "Perancangan Sistem Pengamanan Ganda pada Brankas menggunakan Convolutional Neural Network berbasis Raspberry Pi," ... *Teknologi Informasi dan ...*, vol. 6, no. 9, pp. 2548–964, 2022, [Online]. Available: <http://j-ptiik.ub.ac.id>
- [10] N. Chalista *et al.*, "Identifikasi Pengenalan Wajah Berdasarkan Jenis Kelamin Menggunakan Metode Convolutional Neural Network (CNN) *Journal of Technology and Informatics (JoTI)*," vol. 6, no. 1, 2024, doi: 10.37802/joti.v6i1.694.
- [11] M. R. Daffa Ulhaq, M. A. Zaidan, and D. Firdaus, "Pengenalan Ekspresi Wajah Secara Real-Time Menggunakan Metode SSD Mobilenet Berbasis Android," *Journal of Technology and Informatics (JoTI)*, vol. 5, no. 1, pp. 48–52, 2023, doi: 10.37802/joti.v5i1.387.
- [12] M. Adrezo, M. E. Ardiansyah, and P. S. Informatika, "Deteksi Jenis Kelamin Berdasarkan Wajah Menggunakan Metode YOLOv8 Gender Detection Based on Face Using The YOLOv8 Method 1,2," vol. 7, no. 2019, pp. 1757–1762, 2024. doi: 10.31539/intecom.v7i5.12482
- [13] N. Prasetyo, F. Gozali, E. Djuana, and R. Rambung, "Sistem Brankas Menggunakan Pengenalan Wajah Berbasis Raspberry Pi," *Jetri: Jurnal Ilmiah Teknik Elektro*, vol. 19, no. 1, pp. 60–76, 2021, doi: 10.25105/jetri.v19i1.10005.