

Purwarupa Sistem Keamanan Kunci Pintu Menggunakan *Face Recognition* Berbasis Raspberry Pi

Syahrul Rajab, Yuggo Afrianto, Muhidin

Program Studi Teknik Elektro, Fakultas Teknik dan Sains,
Universitas Ibn Khaldun Bogor

Abstrak

Meningkatnya angka kriminalitas di Indonesia mendorong kebutuhan akan sistem keamanan yang lebih andal dibandingkan metode konvensional seperti kunci fisik, Personal Identification Number (PIN), dan Radio Frequency Identification (RFID). Teknologi biometrik, khususnya face recognition, dipilih karena kemampuannya mengidentifikasi individu secara akurat dan aman. Penelitian ini bertujuan merancang dan menguji purwarupa sistem keamanan pintu berbasis face recognition dengan bantuan Raspberry Pi, serta mengevaluasi kinerjanya dari segi akurasi, kecepatan identifikasi, kestabilan catu daya, waktu respons, konsumsi daya, dan pencatatan riwayat akses. Metode penelitian meliputi perancangan konsep dan penentuan komponen, pembuatan bentuk fisis, pengawatan, pemrograman sistem menggunakan algoritma Histogram of Oriented Gradients (HOG) yang dikombinasikan dengan Support Vector Machine (SVM) serta Convolutional Neural Network (CNN), dan pengujian kinerja alat. Hasil pengujian menunjukkan bahwa algoritma CNN memiliki akurasi pengenalan wajah yang lebih baik dibandingkan HOG+SVM, dengan jarak validasi ideal 70 cm, waktu respons sistem sekitar 1,1 detik, kecepatan proses awal sebesar 14,3 FPS yang menurun hingga 4,5 FPS saat validasi, serta konsumsi daya yang efisien dan catu daya yang stabil pada seluruh kondisi pengujian. Sistem juga berhasil mencatat riwayat akses berupa identitas pengguna, waktu, dan tanggal akses secara akurat. Purwarupa sistem keamanan pintu berbasis face recognition ini terbukti fungsional, responsif, akurat, efisien daya, serta andal dalam mendukung monitoring keamanan akses pintu.

Kata Kunci: Face Recognition, Sistem Keamanan Pintu, Raspberry Pi, Convolutional Neural Network, Histogram of Oriented Gradients

Abstract

The increasing crime rate in Indonesia has driven the need for a more reliable security system compared to conventional methods such as physical keys, Personal Identification Numbers (PIN), and Radio Frequency Identification (RFID). Biometric technology, particularly face recognition, is selected for its ability to identify individuals accurately and securely. This study aims to design and test a face recognition-based door security prototype assisted by a Raspberry Pi, and to evaluate its performance in terms of accuracy, identification speed, power-supply stability, response time, power consumption, and access-history logging. The research method covers basic concept design and component selection, physical prototype construction, wiring, system programming using the Histogram of Oriented Gradients (HOG) algorithm combined with a Support Vector Machine (SVM) as well as a Convolutional Neural Network (CNN), and device performance testing. The test results show that the CNN algorithm achieves better face-recognition accuracy than HOG+SVM, with an ideal validation distance of 70 cm, a system response time of about 1.1 seconds, an initial processing speed of 14.3 FPS that decreases to 4.5 FPS during validation, efficient power consumption, and a stable power supply under all test conditions. The system also successfully records access history, including user identity, time, and date of access, accurately. This face recognition-based door

security prototype is proven to be functional, responsive, accurate, power-efficient, and reliable in supporting door-access security monitoring.

Keywords: *Face Recognition, Door Security System, Raspberry Pi, Convolutional Neural Network, Histogram of Oriented Gradients*

I. LATAR BELAKANG

Keamanan merupakan aspek penting bagi kehidupan bermasyarakat untuk melindungi tempat atau barang berharga dari ancaman kriminalitas. Berdasarkan data Badan Pusat Statistik (BPS) tahun 2023, tercatat 49.546 kasus pencurian, meningkat 33% dibandingkan tahun 2022 yang sebesar 37.159 kasus [1]. Seiring meningkatnya angka kriminalitas, kebutuhan terhadap sistem keamanan yang lebih baik menjadi semakin penting. Sistem kunci konvensional rentan terhadap manipulasi akses karena mudah diduplikasi, sementara sistem modern seperti PIN dan RFID juga masih memiliki celah keamanan, misalnya ketika PIN bocor atau kartu RFID dicuri.

Teknologi biometrik membuka peluang untuk sistem keamanan yang lebih andal karena mengandalkan autentikasi berbasis karakteristik fisik yang unik pada setiap individu, seperti sidik jari, bentuk tangan, struktur wajah, retina, dan iris mata. Salah satu penerapan biometrik yang banyak digunakan adalah face recognition, yang bekerja secara real-time dengan mengombinasikan pengolahan citra dan machine learning untuk mendeteksi serta mengautentikasi wajah secara akurat [2]. Selain aspek autentikasi, pencatatan riwayat akses juga penting untuk mengetahui siapa yang mengakses sistem dan kapan akses tersebut terjadi, sehingga dapat mendukung audit keamanan [3].

Untuk menjalankan sistem face recognition secara optimal, diperlukan perangkat keras dengan kemampuan komputasi yang memadai. Penelitian sebelumnya menunjukkan bahwa sistem face recognition berbasis mikrokontroler ESP32-Cam hanya mampu beroperasi pada performa sekitar 4–5 FPS [4], memiliki delay hingga 5 detik dalam mendeteksi wajah [5], dan akurasi yang terbatas sekitar 80% dengan waktu respons rata-rata 0,5 detik pada penerapan lain berbasis IoT [6]. Berdasarkan keterbatasan tersebut, penelitian ini menggunakan mikrokontroler Raspberry Pi sebagai pengendali utama untuk meningkatkan keandalan dan kinerja sistem keamanan pintu berbasis face recognition, sekaligus membandingkan kinerja dua algoritma pengenalan wajah, yaitu HOG yang dikombinasikan dengan SVM, serta CNN.

II. METODE PENELITIAN

Penelitian ini dilakukan melalui beberapa tahapan yang saling berurutan, yaitu:

1. Identifikasi masalah dan tujuan penelitian, dilanjutkan dengan studi literatur terkait sistem keamanan pintu dan teknologi face recognition;
2. Perancangan konsep dasar sistem dan penentuan komponen perangkat keras dan perangkat lunak yang digunakan;
3. Pembuatan bentuk fisis purwarupa menggunakan bahan akrilik sebagai wadah komponen;
4. Pengawatan seluruh komponen elektronik (mikrokontroler, kamera, relay, solenoid, dan LED) sesuai rancangan sistem;

Pemrograman sistem face recognition menggunakan bahasa Python, mencakup tahap pengumpulan data (dataset wajah), normalisasi, ekstraksi fitur dan encoding (data training), pemuatan model, penangkapan data wajah baru secara real-time, proses inferensi, hingga integrasi hasil prediksi dengan perangkat keras (relay, LED) serta basis data riwayat akses;

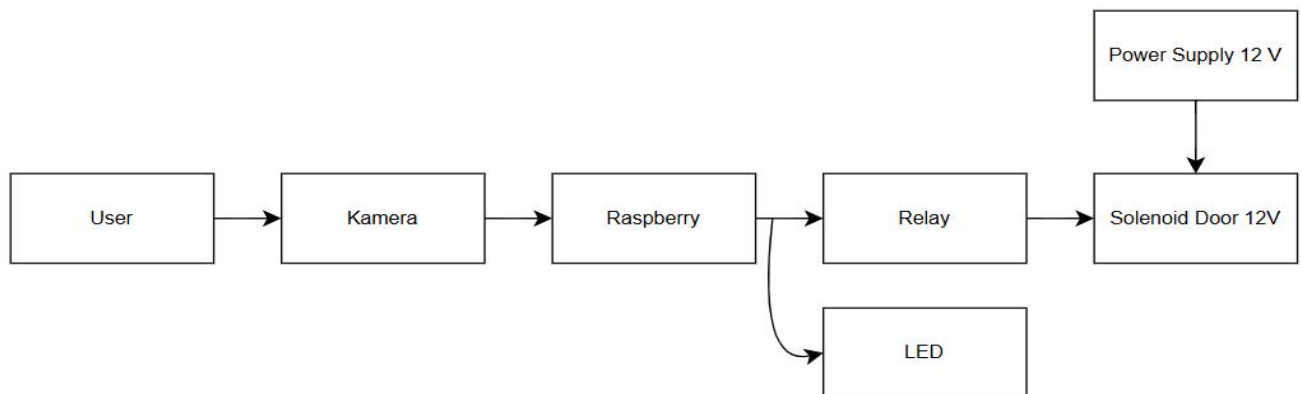
Pengujian kinerja purwarupa yang meliputi pengukuran akurasi pengenalan wajah pada dua algoritma (HOG+SVM dan CNN), kecepatan proses, kestabilan power supply, waktu respons sistem dan sinyal kontrol, konsumsi daya, serta kemampuan monitoring riwayat akses;

Sistem pengenalan wajah pada penelitian ini terbagi menjadi dua tahap utama. Pada tahap pelatihan (training), citra wajah dari dataset diekstraksi fiturnya dan diubah menjadi representasi numerik berupa vektor berdimensi 128 menggunakan pustaka `face_recognition`, kemudian disimpan bersama label nama sebagai model (`encodings.pickle`). Pada tahap prediksi (inferensi), kamera menangkap data wajah secara real-time, setiap frame diproses untuk mendeteksi dan mengekstraksi fitur wajah, kemudian dibandingkan dengan data model yang tersimpan. Apabila hasil pengenalan konsisten selama beberapa frame validasi berturut-turut, sistem akan mengaktifkan relay dan solenoid door lock untuk membuka akses, menyalakan LED indikator sesuai status akses (diterima/ditolak), serta mencatat hasil akses ke dalam basis data dan backend aplikasi.

III. HASIL DAN PEMBAHASAN

3.1 Rancangan Konsep Dasar dan Penentuan Komponen

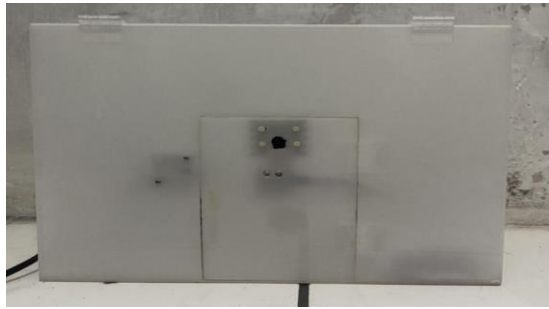
Sistem keamanan pintu dibangun dengan konsep integrasi antara input, kontroler, dan output. Kamera berfungsi sebagai input yang menangkap citra wajah, kemudian data diproses oleh Raspberry Pi sebagai pusat kendali. Hasil identifikasi wajah menentukan aksi sistem, yaitu mengaktifkan solenoid door lock melalui modul relay serta LED sebagai indikator status akses. Solenoid disuplai oleh power supply 12 V tersendiri agar tidak membebani suplai daya mikrokontroler. Diagram blok sistem ditunjukkan pada Gambar 1.



Gambar 1. Diagram blok sistem

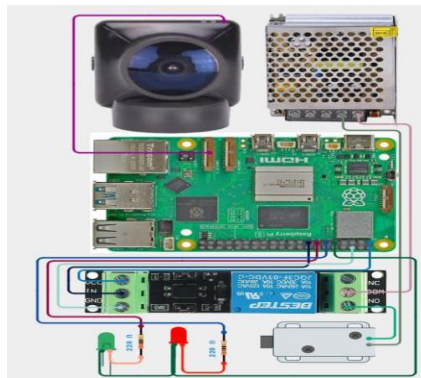
3.2 Pembuatan Bentuk Fisis dan Pengawatan

Purwarupa dirancang menggunakan bahan akrilik berukuran A4 yang dibentuk menyerupai balok, sehingga memudahkan penataan komponen utama seperti Raspberry Pi, modul kamera, relay, solenoid door lock, dan LED secara sistematis. Bentuk fisis purwarupa ditunjukkan pada Gambar 2.

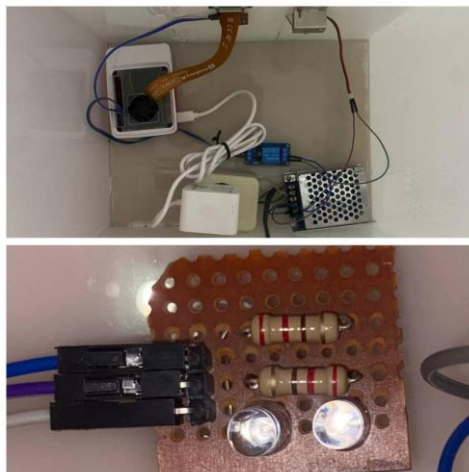


Gambar 2. Bentuk fisis purwarupa

Proses pengawatan menghubungkan seluruh komponen elektronik agar dapat berfungsi sesuai rancangan sistem. Hasil pengawatan menunjukkan bahwa mikrokontroler berhasil terhubung dengan modul kamera, relay, solenoid door lock, serta LED indikator, dengan jalur pengkabelan yang sesuai standar, sebagaimana ditunjukkan pada Gambar 3 dan Gambar 4.



Gambar 3. Diagram pengawatan



Gambar 4. Instalasi pengawatan

3.3 Pemrograman Sistem Face Recognition

Program sistem face recognition dikembangkan menggunakan bahasa Python dengan bantuan Visual Studio Code sebagai code editor. Program pelatihan model membaca seluruh citra pada folder dataset, mendeteksi lokasi wajah menggunakan model HOG, kemudian menghitung encoding wajah berdimensi 128 dan menyimpannya bersama nama pengguna ke dalam berkas `encodings.pickle`. Sementara itu, program utama (aplikasi face recognition) mengonfigurasi GPIO untuk LED dan relay,

memuat model encoding wajah, menangkap citra dari kamera secara real-time, serta menjalankan mesin status (state machine) idle, validating, access granted, dan access denied. Ketika sebuah wajah dikenali secara konsisten selama beberapa frame berturut-turut (validation frame threshold), sistem akan mengaktifkan relay dan LED hijau apabila wajah terdaftar (granted), atau menyalakan LED merah apabila wajah tidak dikenali (denied), sekaligus mengirim log akses ke basis data PostgreSQL dan backend API Django untuk keperluan monitoring.

3.4 Pengukuran Akurasi Pengenalan Wajah

Pengujian akurasi dilakukan untuk mengetahui tingkat keberhasilan sistem dalam mengenali wajah pengguna terdaftar, menggunakan dua algoritma yaitu HOG yang dikombinasikan dengan SVM, dan CNN. Hasil pengujian variabel objek (lima pengguna, masing-masing 10 kali percobaan) ditunjukkan pada Tabel 3.

Tabel 3. Pengujian akurasi variabel objek menggunakan HOG+SVM dan CNN

Nama	Akurasi HOG+SVM	Akurasi CNN
Roni	100%	100%
Azis	80%	100%
Fikri	80%	90%
Medina	90%	100%
Syahrul	100%	100%

Pengujian juga dilakukan pada kondisi ruangan dengan pencahayaan minim (gelap), sebanyak 10 kali percobaan untuk masing-masing algoritma, dengan hasil ditunjukkan pada Tabel 4.

Tabel 4. Pengujian akurasi pada kondisi ruangan gelap

Algoritma	Percobaan	Benar	Salah	Persentase
HOG+SVM	10	0	10	0%
CNN	10	0	10	0%

Selanjutnya, pengujian akurasi berdasarkan variasi jarak (40 cm, 70 cm, dan 100 cm) dilakukan sebanyak 10 kali percobaan pada tiap jarak untuk masing-masing algoritma, dengan hasil pada Tabel 5.

Tabel 5. Pengujian akurasi berdasarkan jarak

Jarak	Persentase HOG+SVM	Persentase CNN
40 cm	60%	70%
70 cm	100%	100%
100 cm	0%	20%

Berdasarkan dari tabel dan grafik, dapat dilihat bahwa pada jarak 40 cm metode HOG+SVM memiliki persentase sebesar 60%, sedangkan CNN sebesar 70%. Pada jarak 70 cm, kedua metode memiliki

hasil yang sama yaitu 100%. Sementara itu, pada jarak 100 cm, persentase HOG+SVM menurun menjadi 0%, sedangkan CNN masih mencapai 20%. Hal ini menunjukkan bahwa CNN memiliki kinerja yang sedikit lebih baik dibandingkan HOG+SVM dalam mendeteksi objek pada jarak yang berbeda.

3.5 Pengukuran Kecepatan Proses Pengenalan Wajah

Pengujian kecepatan proses mengukur waktu yang dibutuhkan sistem sejak kamera menangkap citra hingga hasil prediksi tersedia. Sistem mampu berjalan pada kecepatan awal 14,3 FPS yang menurun hingga 4,5 FPS saat proses validasi wajah berlangsung. Hasil pengujian waktu proses (lima kali percobaan) untuk masing-masing algoritma ditunjukkan pada Tabel 6.

Tabel 6. Pengujian kecepatan proses pengenalan wajah

Algoritma	Rata-rata Waktu Proses (detik)
CNN	1,66
HOG+SVM	1,81

Algoritma CNN memiliki waktu proses yang lebih cepat sekitar 0,15 detik dibandingkan HOG+SVM untuk menyelesaikan satu siklus validasi hingga sistem terbuka.

3.6 Pengujian Kestabilan Power Supply

Pengujian kestabilan power supply dilakukan untuk memastikan tidak terjadi fluktuasi daya yang dapat menyebabkan error atau kerusakan komponen, pada tiga kondisi operasi (idle, deteksi dan pemrosesan wajah, serta pengiriman sinyal aktivasi relay), untuk kedua algoritma. Hasil rata-rata pengujian pada jalur 5 V (catu daya Raspberry Pi) ditunjukkan pada Tabel 7.

Tabel 7. Pengujian kestabilan power supply 5 V (Raspberry Pi)

Kondisi Operasi	Tegangan CNN (V)	Arus CNN (A)	Tegangan HOG+SVM (V)	Arus HOG+SVM (A)
Idle	5,09	0,08	5,08	0,08
Deteksi dan pemrosesan wajah	5,09	0,07	5,08	0,07
Mengirim sinyal aktivasi relay	5,09	0,06	5,08	0,06

Hasil rata-rata pengujian pada jalur 12 V (catu daya solenoid) ditunjukkan pada Tabel 8. Karena kedua algoritma menggunakan modul solenoid dan relay yang sama, hasil pengujian pada jalur 12 V tidak dibedakan berdasarkan algoritma.

Tabel 8. Pengujian kestabilan power supply 12 V (solenoid)

Kondisi Operasi	Tegangan (V)	Arus (A)
Idle	11,64	0
Deteksi dan pemrosesan wajah	11,64	0
Solenoid terbuka	11,64	0,06

Tegangan output power supply 5 V untuk Raspberry Pi berada pada rentang 5,08–5,09 volt dengan arus stabil antara 0,06 hingga 0,08 ampere pada seluruh kondisi dan algoritma pengujian. Power supply 12 V juga menunjukkan kestabilan pada kisaran 11,63–11,64 volt, dengan arus mendekati nol saat idle dan proses pengenalan wajah, serta meningkat menjadi sekitar 0,06 ampere saat solenoid pintu diaktifkan. Hal ini menunjukkan bahwa kedua catu daya mampu bekerja stabil tanpa fluktuasi signifikan, sehingga mengurangi risiko gangguan fungsi maupun kerusakan komponen.

3.7 Pengukuran Waktu Respons Sistem dan Sinyal Kontrol

Pengujian ini mengukur durasi antara terdeteksinya wajah valid hingga sistem mengaktifkan solenoid door lock. Berdasarkan pengujian menggunakan algoritma CNN maupun HOG+SVM, diperoleh sinyal kontrol dengan level low sekitar 0 V dan level high sekitar 3,07 V, dengan waktu respons rata-rata sebesar 1,1 detik untuk kedua algoritma, sebagaimana dirangkum pada Tabel 9.

Tabel 9. Pengujian waktu respons sistem dan sinyal kontrol

Algoritma	Level Low (V)	Level High (V)	Waktu Respons (detik)
CNN	0	3,07	1,1
HOG+SVM	0	3,07	1,1

Nilai waktu respons yang konsisten dan bervariasi sangat kecil pada setiap percobaan menunjukkan bahwa integrasi antara proses pengenalan wajah dan pengendalian solenoid door lock berjalan responsif dan stabil.

3.8 Pengukuran Konsumsi Daya

Pengujian konsumsi daya dilakukan untuk mengetahui kebutuhan energi sistem pada kondisi idle, saat mendeteksi dan memproses wajah, serta saat solenoid pintu terbuka. Hasil rata-rata pengujian (lima kali percobaan) untuk kedua algoritma ditunjukkan pada Tabel 10.

Tabel 10. Pengujian konsumsi daya sistem

Kondisi Operasi	Daya rata-rata CNN (W)	Daya rata-rata HOG+SVM (W)
Idle	7,5	7,6
Deteksi dan pemrosesan wajah	7,1	7,0
Solenoid terbuka	11,5	11,4

Konsumsi daya sistem pada kondisi idle berkisar antara 7,4–7,7 watt, menurun sedikit dan relatif stabil sekitar 7,0–7,1 watt saat proses pengenalan wajah berlangsung, kemudian meningkat signifikan menjadi sekitar 11,3–11,8 watt saat solenoid pintu diaktifkan. Hal ini menunjukkan bahwa beban energi terbesar berasal dari aktuasi solenoid door lock, sedangkan proses pengenalan wajah dan kondisi standby relatif hemat daya, sehingga purwarupa ini dapat dikatakan cukup efisien untuk digunakan secara berkelanjutan.

3.9 Monitoring Riwayat Akses

Fungsi monitoring riwayat akses diuji dengan mengamati kemampuan sistem merekam setiap aktivitas pengenalan wajah beserta hasil aksesnya. Data yang tercatat mencakup identitas pengguna,

status akses (granted/denied), serta tanggal dan waktu akses secara presisi hingga satuan mikrodetik, sebagaimana ditunjukkan pada Gambar 5. Hasil pengujian menunjukkan bahwa sistem mampu menyimpan data riwayat akses secara akurat dan konsisten, sehingga dapat mendukung audit keamanan dan penelusuran riwayat akses apabila dibutuhkan.

☐ edit	16	joko	granted	2025-08-09 03:01:10.101202
☐ edit	17	joko	granted	2025-08-09 03:04:14.674046
☐ edit	18	syahrul	granted	2025-08-14 23:15:20.612306
☐ edit	19	syahrul	granted	2025-08-14 23:15:55.497466
☐ edit	20	syahrul	granted	2025-08-14 23:16:29.03532
☐ edit	21	syahrul	granted	2025-08-14 23:17:10.814148
☐ edit	22	syahrul	granted	2025-08-14 23:18:48.05788
☐ edit	23	syahrul	granted	2025-08-14 23:19:29.448176
☐ edit	24	syahrul	granted	2025-08-14 23:20:23.091055
☐ edit	25	syahrul	granted	2025-08-14 23:34:02.633699
☐ edit	26	syahrul	granted	2025-08-14 23:37:28.366843
☐ edit	27	syahrul	granted	2025-08-14 23:40:31.553803
☐ edit	28	syahrul	granted	2025-08-14 23:41:09.228259
☐ edit	29	syahrul	granted	2025-08-14 23:45:16.285972
☐ edit	30	syahrul	granted	2025-08-14 23:46:52.297307
☐ edit	31	syahrul	granted	2025-08-14 23:47:43.239674
☐ edit	32	syahrul	granted	2025-08-14 23:55:11.736487
☐ edit	33	syahrul	granted	2025-08-14 23:56:39.01644

Gambar 5. Pencatatan riwayat akses sistem

IV. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian purwarupa sistem keamanan kunci pintu berbasis face recognition, dapat disimpulkan beberapa hal sebagai berikut. Pertama, sistem keamanan pintu berbasis face recognition berhasil diimplementasikan dan diintegrasikan dengan baik antara perangkat keras dan perangkat lunak, di mana proses pengenalan wajah secara real-time berhasil mengendalikan aktuator solenoid pintu secara fungsional dan responsif. Kedua, algoritma CNN menunjukkan akurasi pengenalan wajah yang lebih baik dibandingkan HOG+SVM dengan jarak validasi ideal 70 cm, meskipun kedua algoritma memiliki keterbatasan yang sama pada kondisi pencahayaan kurang memadai. Kecepatan kinerja sistem berada pada kisaran 14,3 FPS yang menurun hingga 4,5 FPS saat validasi, dengan algoritma CNN sedikit lebih cepat 0,15 detik dibandingkan HOG+SVM, serta waktu respons sistem sejak validasi hingga pengaktifan aktuator sekitar 1,1 detik yang tergolong cepat untuk aplikasi real-time. Konsumsi daya purwarupa bervariasi sesuai kondisi operasi, dengan rata-rata daya idle sekitar 7,5 watt dan meningkat menjadi sekitar 11,5 watt saat solenoid diaktifkan, sementara pengujian kestabilan power supply menunjukkan suplai listrik yang stabil pada seluruh kondisi operasional. Ketiga, sistem berhasil merekam dan menyimpan riwayat akses secara akurat, mencakup identitas pengguna, tanggal, dan waktu akses, sehingga dapat berfungsi sebagai alat pemantauan keamanan yang efektif selain sebagai pengaman fisik. Untuk pengembangan lebih lanjut, disarankan penggunaan modul kamera dengan kemampuan yang lebih baik dalam kondisi pencahayaan minim, serta penambahan sumber daya cadangan agar sistem tetap dapat berfungsi ketika terjadi gangguan pada catu daya utama.

V. REFERENSI

- [1] Badan Pusat Statistik Indonesia, “Statistik Kriminal 2024,” 12 Desember 2024. [Online]. Tersedia: <https://www.bps.go.id/id/publication/2024/12/12/13317138a55b2f7096589536/statistik-kriminal-2024.html>. [Diakses 7 Juni 2025].
- [2] J. Nasir, A. A. Ramli, dan M. Michael, “Design of door security system based on face recognition with arduino,” *Int. J. Informatics Visualization*, vol. 3, no. 2, hlm. 127–131, 2019.
- [3] A. Hanuebi, S. R. U. A. Sompie, dan F. D. Kambey, “Aplikasi Pengenalan Wajah Untuk Membuka Pintu Berbasis Raspberry Pi,” *Jurnal Teknik Informatika*, vol. 14, no. 2, hlm. 243–252, 2019.
- [4] W. Budiharto, E. Irwansyah, J. S. Suroso, dan A. A. S. Gunawan, “Low-cost vision-based face recognition using ESP32-CAM for tracked robot,” *ICIC Express Letters Part B: Applications*, vol. 13, no. 3, hlm. 321–327, 2022.
- [5] A. Ipanhar, T. K. Wijaya, dan P. Gunoto, “Perancangan sistem monitoring pintu otomatis berbasis IoT menggunakan ESP32-CAM,” *Sigma Teknika*, vol. 5, no. 2, hlm. 333–350, 2022.
- [6] D. R. Ahwadi dan A. P. Setiawan, “Sistem Keamanan Pintu Rumah Menggunakan Face Recognition Berbasis IoT,” *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis*, 2025.
- [7] Z. Munawar, M. Hasnawi, I. S. Beno, I. W. A. S. Darma, C. K. Sastradipraja, N. P. Sutramiani, dkk., *Visi Komputer: Konsep, Metode, dan Aplikasi*. Jakarta: Kaizen Media Publishing, 2023.
- [8] D. Kurniawan, *Pengenalan Machine Learning dengan Python*. Jakarta: Elex Media Komputindo, 2022.
- [9] F. A. I. A. Putra, A. G. Sulaksono, L. T. Utomo, dan A. R. Khamdani, “Klasifikasi Buah dan Sayur menggunakan fitur ekstraksi HOG dan Metode KNN,” *Jurnal Informatika Polinema*, vol. 10, no. 1, 2023.
- [10] J. P. Tanjung dan M. Muhathir, “Classification of facial expressions using SVM and HOG,” *Journal of Informatics and Telecommunication Engineering*, vol. 3, no. 2, hlm. 210–215, 2020.
- [11] K. Azmi, S. Defit, dan S. Sumijan, “Implementasi Convolutional Neural Network (CNN) untuk Klasifikasi Batik Tanah Liat Sumatera Barat,” *Jurnal Unitek*, vol. 16, no. 1, hlm. 28–40, 2023.
- [12] Y. Goyal, “Comparative Study of Microcontrollers: Arduino UNO, Raspberry Pi 4, ESP32,” *International Journal for Research in Applied Science and Engineering Technology*, vol. 6, 2024.
- [13] S. Monk, *Programming the Raspberry Pi: Getting Started with Python*. New York, NY, USA: McGraw-Hill Education TAB, 2021.
- [14] M. Saleh dan M. Haryanti, “Rancang Bangun Sistem Keamanan Rumah Menggunakan Relay,” *Jurnal Teknologi Elektro*, vol. 8, no. 2, hlm. 87–94, 2017.
- [15] F. A. Yaqin, D. Rahmawati, A. F. Ibadillah, dan K. A. Wibisono, “Perancangan Power Supply Switching dengan Power Factor Correction (PFC) untuk Mengoptimalkan Daya Output dan Pengaman Proteksi Hubung Singkat,” *Jurnal Arus Elektro Indonesia*, vol. 7, no. 2, hlm. 42–50, 2021.