Automated Portal Security Prototype Using Facial Recognition System [Prototipe Keamanan Portal Otomatis Menggunakan Sistem Pengenalan Wajah]

Mohammad Tetuko Putra Maulana Riu[1)], Indah Sulistyowati[2)] , Shazana Dhiya Ayuni[3)] , Syamsudduha Syahrorini[4)]

[1)]Program Studi Teknik Elektro, Universitas Muhammadiyah Sidoarjo, Indonesia
[2)]Program Studi Teknik Elektro, Universitas Muhammadiyah Sidoarjo, Indonesia
[3)]Program Studi Teknik Elektro, Universitas Muhammadiyah Sidoarjo, Indonesia
[4)]Program Studi Teknik Elektro, Universitas Muhammadiyah Sidoarjo, Indonesia
*Email Penulis Korespondensi: indah_sulistiyowati@umsida.ac.id

Abstract. *This research discusses the development of a prototype automatic portal security system using an ESP32-CAM based facial recognition system. The aim of this research is to explore the use of facial recognition technology to improve security and efficiency in access control systems in various environments. The ESP32-CAM functions as the main camera and processor, capturing facial images, and processing them using image processing libraries. Face detection algorithms identify facial features in images and match them with data stored in a database. The MCU32 node controls the servo motor that opens the portal when a face is recognized. The system is powered by a 5V USB power bank to activate the ESP32 module via face detection signal*

Keywords *- Prototype, Arduino, Servo.*

Abstrak. *Penelitian ini membahas pengembangan prototype sistem keamanan portal otomatis menggunakan sistem pengenalan wajah berbasis ESP32-CAM. Tujuan penelitian ini untuk mengeksplorasi penggunaan teknologi pengenalan wajah untuk meningkatkan keamanan dan efisiensi dalam sistem kontrol akses di berbagai lingkungan. ESP32-CAM berfungsi sebagai kamera dan prosesor utama, menangkap gambar wajah, dan memprosesnya menggunakan pustaka pemrosesan gambar. Algoritma deteksi wajah mengidentifikasi fitur wajah pada gambar dan mencocokkannya dengan data yang tersimpan di basis data. Node MCU32 mengontrol servo motor yang membuka portal ketika wajah dikenali. Sistem didukung oleh bank daya USB 5V untuk mengaktifkan modul ESP32 melalui sinyal deteksi wajah*

Kata Kunci *- Prototype, Arduino, Servo.*

I. PENDAHULUAN

Di era teknolologi modern, keamanan menjadi perhatian utama di segala bidang, mulai dari keamanan data hingga keamanan fisik (Sulistiyowati, Sugiarto, & Jamaaluddin, 2020). Dalam Rahmawati menunjukkan bahwa terjadi pembobolan data dan pencurian identitas pada situs belanja online di mana pada tanggal 1, 6 dan 10 terjadi kebocoran data pengguna di beberapa aplikasi belanja online, tidak hanya kebocoran namun data tersebut juga ditawarkan untuk dijual. Dampak yang akan timbul dari kejadian tersebut yakni adanya potensi hilangnya kepercayaan pengguna terhadap aplikasi yang digunakan, selain itu juga berpotensi merugikan konsumen dan perusahaan. Pada sisi keamanan fisik, seringkali terdapat kontrol akses untuk individu tertentu, seperti kantor, laboratorium, atau bahkan rumah, untuk memastikan bahwa hanya mereka yang memiliki otoritas yang diperlukan yang diizinkan memasuki area tersebut (Zulwidad & Sulistiyowati, 2023). Hal ini biasanya dilakukan dengan menggunakan kartu, kunci atau kode akses (Nasar, Setyawan, Faruq, & Sulistiyowati, 2019). Namun, setiap metode memiliki kelemahan masing-masing yakni dapat hilang, dicuri atau bahkan disalahgunakan (Munir, Ehsan, & Mohsin, 2019).

Sistem pengenalan wajah adalah salah satu jenis pengenalan biometrik yang populer karena wajah manusia memiliki banyak krakteristik unit yang menjadikannya alat yang sangat akurat dan sulit dipalsukan (Pawar, Kithani, Ahuja, & Sahu, 2018).

Pada konteks ini, penelitian tentang "prototipe keamanan portal otomatis dengan sistem pengenalan wajah" menjadi sangat relevan (Khunchai & Thongchaisuratkrul, 2020). Hal tersebut dikarenakan seseorang atau pihak tertentu dapat meningkatkan keamanan lokasi dengan sistem ini sekaligus mengurangi risiko yang terkait dengan metode akses konvensional (Paikaray & Parikh, 2022).

Prototipe ini tidak hanya menawarkan solusi keamanan terkini, tetapi juga mengintegrasikan kemajuan terkini dalam teknologi sensor, pemrosesan gambar dan AI. Teknologi ini juga masih mengadopssi teknologi sebelumnya, perbedannya terletak pada penggunaan perangkat yang lebih praktis. Dengan menggabungkan semua komponen ini,

tujuannya adalah untuk menciptakan sistem yang efisien, kuat dan ramah pengguna bagi pengguna akhir (Candra S, Sunawar, & Hanifah Y, 2020).

Pada sejarah evolusi teknologi keamanan, upaya menjamin identitas individu telah mengalami berbagai transformasi (Das et al., 2022). Secara tradisional, kunci mekanis dan kombinasi numerik telah digunakan sebagai alat keamanan utama untuk mengontrol akses ke area tertentu (Kak & Alfaqi, 2019). Namun, metode ini seringkali rentan terhadap kehilangan, pencurian atau manipulasi (Kak & Alfaqi, 2019). Misalnya, kunci yang hilang dapat dengan mudah ditemukan dan digunakan oleh pihak yang tidak berkepentingan, dan kombinasi angka dapat dilupakan atau bahkan ditebak (Othman & Aydin, 2018).

Menanggapi keterbatasan tersebut, timbul kebutuhan akan solusi yang lebih canggih dan handal (Babu, Neha, Babu, & Pinto, 2022). Pada beberapa dekade terakhir, teknologi biometrik telah menunjukkan potensinya sebagai alternatif yang kuat terhadap sistem keamanan tradisional (Bentahar, Meraoumia, Bendjena, & Abdelhakim, 2022). Teknologi ini memanfaatkan karakteristik unik individu, seperti: sidik jari, suara, pola retina dan wajah sebagai parameter identifikasi (Shahreza, Bassit, Marcel, & Veldhuis, 2023).

Dari berbagai metode biometrik yang tersedia, pengenalan wajah menarik perhatian khusus karena beberapa alasan (Cordoș, Mihăilă, Faragó, & Hintea, 2023). Pertama, proses pengambilan data wajah bersifat non-invasif dan dapat dilakukan dari jarak jauh (Kotkova, 2023). Kedua, dengan kemajuan teknologi kamera dan algoritma pemrosesan gambar, sistem pengenalan wajah kini dapat beroperasi dengan kecepatan dan akurasi yang mengesankan (Balaji et al., 2023). Ketiga, tidak seperti metode biometrik lainnya, wajah sulit dipalsukan tanpa terdeteksi, mengingat kompleksitas struktur dan ekspresi wajah manusia (Vandana & Kaur, 2021).

Namun, terlepas dari potensinya, penerapan praktis sistem pengenalan wajah dalam aplikasi keamanan portal masih memerlukan eksplorasi dan penelitian lebih lanjut (Leyu et al., 2021). Berbagai tantangan perlu diatasi, seperti kemampuan sistem untuk mengenali wajah dalam kondisi pencahayaan, sudut atau perubahan wajah seseorang yang berbeda (misalnya pertumbuhan janggut, perubahan riasan atau cedera) (Bykov, Voronov, Voronova, & Zharov, 2020). Berbagai tantangan tersebut dapat diatasi dengan menggunakan sistem yang lebih baik, di mana setiap proses diberikan program analisis tersendiri sehingga sistem analisis citra dapat terus dibatasi pada citra yang ada pada database.

Mempertimbangkan semua hal yang telah disampaikan, pengembangan "prototipe keamanan portal otomatis menggunakan sistem pengenalan wajah" menjadi sangat penting (Krishna, Sachin, Rather, Vandana, & Vignesh, 2023). Tujuannya adalah untuk memanfaatkan kekuatan teknologi biometrik dan mengatasi keterbatasannya, sehingga menciptakan solusi, keamanan yang lebih andal, efisien dan ramah pengguna bagi masyarakat luas.

Oleh karena itu, penulis melakukan penelitian dengan judul "Prototype Keamanan Portal Otomatis Menggunakan Face Recognition System". Pada jurnal sebelumnya, portal keamanan otomatis hanya memanfaatkan sensor RFID untuk membuka portal di lingkungan perumahan. Meski cara ini cukup efisien, namun tetap terdapat potensi risiko jika kartu RFID hilang atau disalahgunakan. Selain itu, metode tersebut tidak dapat membedakan siapa pemilik kartu, karena setiap orang yang memiliki kartu RFID akan memiliki akses yang sama. Namun, kini perangkat tersebut telah ditingkatkan dengan penggunaan sensor ESP CAM, sehingga memastikan keamanan yang lebih baik karena sensor ESP CAM hanya mengizinkan akses ke kartu tersebut yakni portal melalui pemindaian wajah.Penguji.

II. METODE

- Lokasi dan Waktu Penelitian, Alat dan Bahan

Penelitian dan pengujian dilakukan di Laboratorium IMEI Umsida Universitas Muhammadiyah Sidoarjo. Penelitian dilaksanakan pada bulan Desember 2023 sampai Januari 2024.

Objek yang digunakan antara lain:

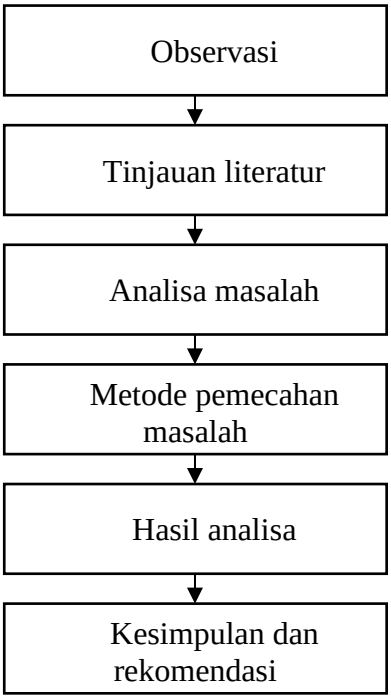
1. Laptop
2. Perangkat lunak Auduino IDE
3. Aplikasi Proteus
4. Obeng Avo Meter (+) dan (-)

Alat penunjang lainnya, yakni:

Kamera ESP32
Servo Motor
Simpul MCU ESP32
FTDI
Kabel
Adaptor 5 volt
Lainnya

- Prosedur Penelitian

Prosedur penelitian merupakan serangkaian langkah yang dapat digunakan untuk mengumpulkan data untuk proses pengembangan *prototype* keamanan portal otomatis menggunakan *face recognition system*. Berikut diagram yang menunjukkan prosedur penelitian:



Gambar 1. Prosedur Penelitian

Berikut uraian dari Gambar 1 prosedur penelitian untuk mengumpulkan data untuk proses pengembangan *prototype* keamanan portal otomatis menggunakan *face recognition system* :

Observasi

Perencanaan dan observasi meliputi pengamatan terhadap permasalahan dan kebutuhan. Dari pengamatan ini, permasalahan utama yang harus diatasi melalui pembuatan alat akan diidentifikasi.

Tinjauan pustaka

Mengumpulkan referensi dari beragam sumber sangat penting untuk mendukung penyelesaian proyek. Membaca jurnal ilmiah, buku, makalah dan literatur relevan lainnya terkait pembuatan alat akan memberikan pemahaman yang jelas dalam mengidentifikasi masalah dan mencari solusi terhadap penelitian yang akan dilakukan.

Analisa masalah

Menganalisis permasalahan yang ingin dipecahkan dengan memeriksa alat dan bahan yang akan digunakan dalam penelitian melalui pengujian dan pemeriksaan untuk memastikan berfungsi secara maksimal.

Metode pemecahan masalah

Memanfaatkan metode pemecahan masalah berdasatkan asumsi-asumsi yang ditinjau dari penelitian sebelumnya dan sebagai tambahan melakukan pengujian terhadap hasil eksperimen alat.

Hasil analisa

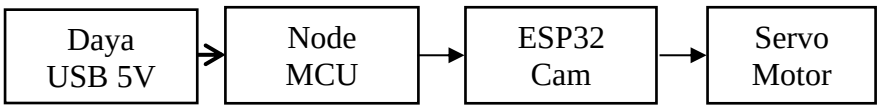
Ini melibatkan pengumpulan data dan melakukan analisis. Analisis tersebut berfungsi sebagai acuan ketika mengevaluasi hasil alat yang akan dibuat.

Kesimpulan dan rekomendasi

Dengan menyimpulkan percobaan, pengumpulan data, pengolahan data dan pengujian alat, dapat diambil kesimpulan dan rekomendasi. Pembaca dapat menggunakan kesimpulan ini untuk menyempurnakan alat dengan meninjau rekomendasi berdasarkan kekurangan dari alat tersebut.

- Diagram Blok

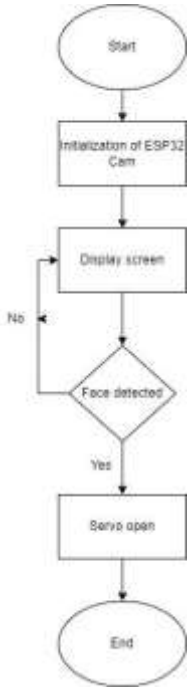
  Untuk memudahkan perancangan dan pengembangan alat, dibuat diagram blok keseluruhan sistem.



Gambar 2. Diagram Blok

Pada diagram blok, terlihat beberapa komponen *hardware* yang dibutuhkan yakni Node MCU ESP32, ESP32 Cam dan Servo Motor. Pada diagram blok tersebut, terdapat modul Node MCU ESP32 yang berfungsi sebagai koneksi pemrograman dari PC ke modul menggunakan kabel USB. Selanjutnya, terdapat ESP32 Cam sebagai *input device*, serta ada Servo Motor yang berfungsi sebagai *output* atau *drive portal* dan juga sebagai indikator pendeteksi wajah.

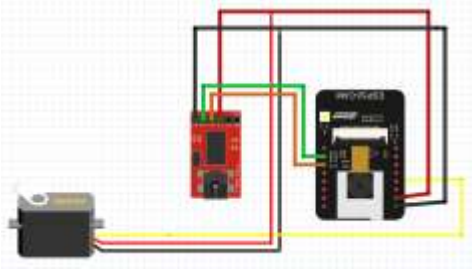
- Flowchart



Gambar 3. *Flowchart*

Pada gambar 3 Flowchart, Flowchart ini menggambarkan alur kerja sistem deteksi wajah menggunakan ESP32 Cam dengan konektivitas 4G. Proses dimulai dengan menghubungkan perangkat keras ke smartphone melalui jaringan internet. Setelah terhubung, modul ESP32 Cam diinisialisasi untuk memastikan koneksi 4G aktif.. Sistem kemudian menampilkan layar yang digunakan untuk menunjukkan status atau hasil dari deteksi wajah. Jika tidak ada wajah yang terdeteksi, sistem akan kembali ke tampilan layar dan terus melakukan pengecekan secara berulang. Namun, jika wajah terdeteksi, sinyal dari ESP32 Cam diteruskan ke perangkat NodeMCU. NodeMCU memproses sinyal tersebut dan mengirimkannya ke Servo Motor, yang kemudian membuka (misalnya, pintu atau perangkat lain yang dikendalikan oleh servo). Setelah servo diaktifkan, proses selesai. Flowchart ini menunjukkan bagaimana sistem secara terus-menerus memeriksa deteksi wajah dan mengendalikan servo berdasarkan hasil deteksi tersebut.

- Wiring System Design Flowchart



Gambar 4. Skema Rangkaian

Rangkaian tersebut didukung bank daya USB 5V sumber tegangan yang akan disalurkan ke berbagai perangkat seperti sensor ESP32 Cam dan Servo Motor. Dari skema rangkaian tersebut tampak bahwa semua modul harus terhubung ke ESP32 agar semua perangkat dapat berfungsi sesuai keinginan. Pin-pin yang terhubung dapat dilihat pada tabel 1, Pin terhubung :

Tabel 1. Pin Terhubung

No	Pin ESP32 Cam	Penggunaan
1	VCC	5V
2	GND	GND
3	GPIO13	Servo

Pemaparan table. 1 Pin ESP32 digunakan untuk menghubungkan sensor ESP32 Cam ke sistem. VCC terhubung ke sumber tegangan 5V untuk menyediakan daya yang dibutuhkan oleh perangkat. GND terhubung ke ground (GND) untuk melengkapi rangkaian listrik dan memastikan kestabilan tegangan. GPIO13 terhubung ke Servo Motor untuk mengendalikan gerakan servo berdasarkan sinyal yang diterima dari ESP32.

III. HASIL DAN PEMBAHASAN

A. PEMBAHASAN

Berikut ini cara menggunakan teknologi pengenalan wajah untuk membuka dengan Node MCU ESP 32, CAM-ESP32 dan Servo Motor. Sistem ini ditenagai oleh *power bank USB*

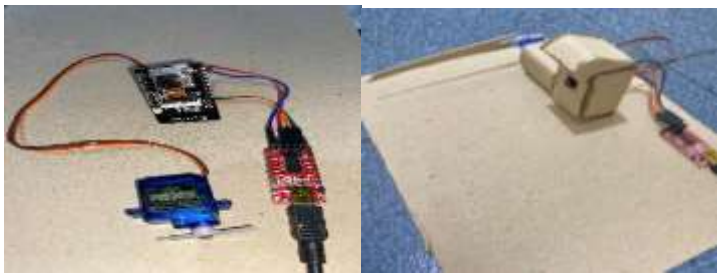
dan menggunakan ESP32 pin 2 untuk mengirimkan sinyal tinggi ketika wajah dikenali, yang akan mengirimkan sinyal untuk membuka portal. Berikut langkah-langkah untuk mengoperasikan prototype mikrokontroler:

1) Pengguna mengaktifkan jaringan Wi-Fi yang terhubung ke mikrokontroler.
2) Sebagai sumber listrik, sambungkan mikrokontroler ke kabel USB.
3) Pengguna kemudian dapat mengakses aplikasi Proteus yang terhubung dengan mikrokontroler.
4) Setelah masuk ke aplikasi Arduino, pengguna diharuskan mengunggah coding mikrokontroler.
5) Pengujian langsung dilakukan dengan memposisikan CAM-ESP32 menghadap wajah pengguna. Jika wajah terdeteksi, servo akan bergerak, menandakan portal gerbang otomatis terbuka.
6) Secara rinci, sistem ini dikonfigurasi dengan Node MCU32 dan CAM-ESP32, yang diatur untuk membuka portal gerbang ketika wajah yang terdeteksi.

Menggunakan teknologi pengenalan wajah dengan NodeMCU ESP32, CAM-ESP32, dan Servo Motor, yang ditenagai oleh *power bank USB*, memungkinkan sistem otomatis untuk membuka portal saat wajah dikenali. Prosesnya dimulai dengan pengambilan gambar oleh CAM-ESP32, yang kemudian diproses menjadi skala abu-abu dan diuji threshold sebelum dicocokkan dengan data di basis data. Jika kecocokan ditemukan angka 1 warna hijau

NodeMCU ESP32 mengirimkan sinyal tinggi melalui pin untuk mengaktifkan Servo Motor dan membuka portal.

Sedangkan jika nilai 0 dengan warna merah maka servo motor tidak aktif sehingga portal tetap tertutup. Sistem ini mengandalkan kualitas kamera, keakuratan algoritma pengenalan wajah, serta keamanan dan integritas basis data. Pengujian threshold dan greyscale sangat penting untuk mengoptimalkan akurasi pengenalan di berbagai kondisi, sehingga menjadikan sistem ini andal dan efektif untuk kontrol akses otomatis.



Gambar 5. Hasil Realisasi Alat

Pengujian dilakukan di Lab IMEI untuk mengetahui dan memperoleh hasil dari perangkat yang dibuat. Pada tahap ini pengujian dilakukan dengan beberapa pengujian, antara lain:

B. Pengujian Koneksi Wi-Fi ke Node MCU ESP32

Tujuan dari pengujian ini adalah untuk memastikan bahwa Node MCU ESP32 dapat terhubung ke jaringan Wi-Fi dengan cepat dan stabil dalam waktu 5 hingga 7 detik. Koneksi Wi-Fi yang stabil sangat penting untuk komunikasi antara modul ESP32 dan sistem kontrol lainnya. Dalam jangka waktu 5 hingga 7 detik, koneksi Wi-Fi ke Node MCU ESP32 diuji, dan hasilnya ditampilkan pada Tabel 1. Berdasarkan temuan penelitian, ESP32 menunjukkan kemampuan untuk membangun jaringan nirkabel yang stabil. Seperti yang ditunjukkan pada tabel berikut:

Tabel 2. Menguji Koneksi Wi-Fi ke ESP32

Pengujian ke-	Wi-Fi ke ESP32		Akurasi (%)
	Kondisi	Waktu Tunggu	
Tes pertama	Terhubung	7	Sedang
Tes ke-2	Terhubung	7	Sedang
Tes ke-3	Terhubung	6	Sedang
Tes ke-4	Terhubung	6	Sedang
Tes ke-5	Terhubung	5	Sedang

Tabel 2 menunjukkan bahwa pengujian dilakukan sebanyak 5 kali pengujian. Dalam 5 pengujian tersebut, ditemukan bahwa ESP32 Node MCU dapat terhubung dengan stabil. Waktu tunggu yang dihasilkan antara 5 sampai 7 detik. Dengan hasil tersebut, dapat disimpulkan bahwa ESP32 Node MCU memiliki tingkat akurasi yang sedang, dan masih direkomendasikan untuk digunakan.

C. Pengujian Deteksi Wajah pada Modul ESP32

Pengujian ini bertujuan untuk memastikan bahwa modul ESP32 dapat mendeteksi wajah dengan akurat setelah diupload dengan kode dari aplikasi Proteus. Keberhasilan deteksi wajah sangat penting untuk memicu aktivasi sistem kontrol akses. Pengujian deteksi wajah pada modul ESP32 terjadi ketika ESP sudah di*upload* dengan *coding* dari aplikasi Proteus. Modul ESP32 akan aktif ketika ada wajah yang terdeteksi, sehingga mampu mengirimkan sinyal terbuka ke Servo Motor. Pengujian deteksi wajah juga dilakukn dalam 5 kali uji yang dapat dilihat pada tabel berikut:

Tabel 3. Menguji Saat ESP Mendeteksi Wajah

Pengujian ke	ESP32 *Output*
1	1
2	1
3	0
4	1
5	1

Berdasarkan tabel 3, tampak bahwa dari 5 kali uji coba yang dilakukan menunjukkan bahwa sistem mampu membaca kehadiran wajah sebanyak 4 kali dan 1 kali wajah tidak terbaca yakni pada percobaan ke 3. Dengan hasil tersebut, maka sistem dikatakan dapat membaca di atas 80%. Hasil tersebut merupakan hasil yang baik dan dapat direkomendasikan untuk digunakan. Hasil ini dianggap baik karena menunjukkan bahwa sistem memiliki keandalan yang tinggi dalam kondisi pengujian. Tingkat keberhasilan di atas 80% menunjukkan bahwa algoritma pengenalan wajah, prapemrosesan gambar (seperti konversi ke skala abu-abu dan pengujian threshold), serta kualitas perangkat keras seperti CAM-ESP32 dan NodeMCU ESP32 bekerja dengan baik untuk mendeteksi wajah secara konsisten.

D. Pengujian Servo Motor

Pengujian ini bertujuan untuk memastikan bahwa servo motor dapat merespon sinyal dari modul ESP32 dengan benar dan membuka gerbang portal saat sinyal diterima. Pengujian dilakukan ketika Servo Motor telah menerima sinyal dari modul SP32, sehingga Servo Motor akan merespon sinyal ESP32 dengan cara bergerak membuka gerbang portal. Hasil pengujian dapat dilihat pada tabel berikut:

Tabel 4. Pengujian Pada Saat Servo Motor Menerima Sinyal

Pengujian ke	Servo Motor *Output*
1	1
2	1
3	0
4	1
5	1

Pada tabel 4, diketahui bahwa terdapat nilai 1 dan 0 dari Servo Motor. Dalam konteks penggunaan Servo Motor yang dikendalikan oleh sistem pengenalan wajah, nilai 1 dan nilai 0 memiliki makna sebagai berikut:

- Nilai 1: Merupakan sinyal yang diterima oleh Servo Motor saat sistem berhasil mendeteksi wajah. Ketika wajah terdeteksi dengan benar oleh sistem pengenalan, ini mengakibatkan Servo Motor memberikan respons untuk membuka (misalnya, membuka pintu atau gerakan lain yang diinginkan).

- Nilai 0: Merupakan sinyal yang diterima oleh Servo Motor saat sistem tidak berhasil mendeteksi wajah. Ketika wajah tidak terdeteksi atau gagal terbaca oleh sistem pengenalan, Servo Motor tidak memberikan respons atau tetap dalam keadaan default (misalnya, tidak membuka pintu). Pemicu Servo Motor tersebut berdasarkan pembacaan wajah yang telah diuji pada tabel 3. Pada tabel 3, sistem membaca keberadaan wajah sebanyak 4 kali dan 1 kali tidak terbaca serta pada sistem Servo Motor tersebut memiliki nilai 1 sebanyak 4 kali dan nilai 0 hanya 1 kali. Untuk menghitung akurasi, kita menggunakan rumus:

Akurasi = jumlah prediksi benar ÷ jumlah prediksi total x 100 %
Akurasi = 4/5 × 100 %
= 0,8
= 80 %
Prediksi benar (nilai 1) = 4 kali
Prediksi salah (nilai 0) = 1 kali
Jumlah prediksi total = 5 kali
Hasilnya Servo Motor memilik akurasi 80 % dan hasilnya sangat bagus.

Berdasarkan pengujian yang telah dilakukan, sistem keamanan portal otomatis menunjukkan kinerja yang baik dalam hal koneksi Wi-Fi, deteksi wajah, dan respon servo motor. Namun, beberapa tantangan dan kegagalan masih perlu diatasi untuk mencapai tingkat keberhasilan yang lebih tinggi. Tingkat keberhasilan keseluruhan sistem adalah 80%, yang menunjukkan potensi untuk digunakan sebagai solusi keamanan dengan pengembangan lebih lanjut untuk mengatasi bug dan meningkatkan akurasi deteksi wajah. Pada tabel 4, diketahui bahwa terdapat nilai 1 dan 0 dari Servo Motor. Pemicu Servo Motor tersebut berdasarkan pembacaan wajah yang telah diuji pada tabel 3. Pada tabel 3, sistem membaca keberadaan wajah sebanyak 4 kali dan 1 kali tidak terbaca serta pada sistem Servo Motor tersebut memiliki nilai 1 sebanyak 4 kali dan nilai 0 hanya 1 kali. Terkait demikian, Servo Motor memiliki 80% dan hasilnya sangat bagus.

Gambar 6 Sampel munculnya nilai 1 warna hijau, nilai 0 warna merah

Pada sistem pengenalan wajah ini, hasil pengujian ditampilkan dengan indikator warna untuk memudahkan interpretasi:

-Nilai 1 (Warna Hijau): Menunjukkan bahwa wajah berhasil dideteksi. Warna hijau digunakan untuk menandai hasil positif, menunjukkan bahwa sistem mengenali wajah dengan benar.

- Nilai 0 (Warna Merah): Menunjukkan bahwa wajah tidak terdeteksi. Warna merah digunakan untuk menandai hasil negatif, menunjukkan bahwa sistem gagal mengenali wajah dalam percobaan tersebut.

Indikator warna ini memberikan cara visual yang cepat untuk memahami performa sistem dalam mendeteksi wajah selama pengujian. Hasil ini membantu dalam evaluasi keandalan dan efektivitas sistem pengenalan wajah.

(1)

IV. SIMPULAN

Penelitian ini bertujuan untuk mengimplementasikan sistem pengenalan wajah menggunakan NodeMCU ESP32, CAM-ESP32, dan Servo Motor dalam konteks kontrol akses otomatis. Permasalahan utama adalah mengevaluasi keberhasilan sistem dalam mendeteksi wajah dengan akurasi tinggi untuk mengaktifkan Servo Motor. Hasil penelitian menunjukkan bahwa sistem mampu mendeteksi wajah dengan tingkat keberhasilan 80%, di mana dari 5 kali uji coba, sistem berhasil membaca keberadaan wajah sebanyak 4 kali dan gagal 1 kali. Nilai 1 yang diterima Servo Motor menandakan bahwa wajah berhasil terdeteksi, yang mengakibatkan Servo Motor membuka sesuai program. Sebaliknya, nilai 0 menunjukkan bahwa Servo Motor tidak memberikan respons karena ketiadaan deteksi wajah.

Rekomendasi untuk penelitian selanjutnya adalah melakukan optimasi lebih lanjut pada algoritma pengenalan wajah untuk meningkatkan akurasi deteksi. Pengujian yang lebih luas dan berbagai kondisi pencahayaan

dapat membantu mengidentifikasi dan mengatasi tantangan dalam deteksi wajah yang lebih kompleks. Mempertimbangkan integrasi dengan teknologi keamanan tambahan seperti enkripsi data dan otentikasi ganda dapat meningkatkan keamanan.

.

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, sehingga saya dapat menyelesaikan artikel ini dengan baik. Saya juga ingin menyampaikan terima kasih yang sebesar-besarnya kepada orang tua saya yang selalu memberikan dukungan, kasih sayang, dan doa yang tiada henti, serta teman-teman saya yang selalu ada untuk memberikan semangat dan bantuan ketika saya merasa lelah dan hampir menyerah dalam proses pencarian sumber dan penulisan artikel ini. Tidak lupa, saya juga ingin mengucapkan terima kasih yang tulus kepada Sivitas Akademika Universitas Muhammadiyah Sidoarjo, yang telah memberikan bimbingan, pengetahuan, dan arahan yang sangat berharga sepanjang penyusunan artikel ini. Bantuan dan dukungan dari berbagai pihak telah menjadi motivasi utama yang mendorong saya untuk terus berusaha dan menyelesaikan artikel ini dengan sebaik-baiknya. Semoga artikel ini dapat memberikan manfaat dan kontribusi positif bagi pembaca serta menjadi amal kebaikan bagi semua pihak yang terlibat.

REFERENSI

[1] I. Sulistiyowati, A. R. Sugiarto, and J. Jamaaluddin, “Smart Laboratory Based on Internet of Things in the Faculty of Electrical Engineering, University of Muhammadiyah Sidoarjo,” *IOP Conf Ser Mater Sci Eng*, vol. 874, no. 1, 2020, doi: 10.1088/1757-899X/874/1/012007.

[2] M. H. Zulwidad and I. Sulistiyowati, “Efficiency Through Automation: A Single System for Multiple Railway Guard Posts,” *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 5, no. 3, pp. 407–416, Oct. 2023, doi: 10.12928/biste.v5i3.9001.

[3] M. Nasar, N. Setyawan, A. Faruq, and I. Sulistiyowati, “A Simple Real-Time Energy Analytics Model for Smart Building Using Open IoT Platforms,” *Jurnal Elektronika dan Telekomunikasi*, vol. 19, no. 2, p. 83, 2019, doi: 10.14203/jet.v19.83-90.

[4] A. Munir, S. K. Ehsan, S. M. M. Raza, and M. Mudassir, “Face and Speech Recognition Based Smart Home,” in *2019 International Conference on Engineering and Emerging Technologies (ICEET)*, 2019, pp. 1–5. doi: 10.1109/CEET1.2019.8711849.

[5] S. Pawar, V. Kithani, S. Ahuja, and S. Sahu, “Smart Home Security Using IoT and Face Recognition,” in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018, pp. 1–6. doi: 10.1109/ICCUBEA.2018.8697695.

[6] S. Khunchai and C. Thongchaisuratkrul, “Development of Application and Face Recognition for Smart Home,” in *2020 International Conference on Power, Energy and Innovations (ICPEI)*, 2020, pp. 105–108. doi: 10.1109/ICPEI49860.2020.9431473.

[7] D. Paikaray and S. Parikh, “A new way of Smart Home Security using ML Face Recognition,” in *2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 2022, pp. 1628–1632. doi: 10.1109/SMART55829.2022.10047397.

[8] P. Das, N. A. Asif, M. M. Hasan, S. H. Abhi, M. J. Tatha, and S. D. Bristi, “Intelligent Door Controller Using Deep Learning-Based Network Pruned Face Recognition,” in *2022 25th International Conference on Computer and Information Technology (ICCIT)*, 2022, pp. 120–124. doi: 10.1109/ICCIT57492.2022.10056094.

[9] S. F. Kak and F. M. Mustafa, “Smart Home Management System Based on Face Recognition Index in Real-time,” in *2019 International Conference on Advanced Science and Engineering (ICOASE)*, 2019, pp. 40–45. doi: 10.1109/ICOASE.2019.8723673.

[10] N. A. Othman and I. Aydin, “A face recognition method in the Internet of Things for security applications in smart homes and cities,” in *2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, 2018, pp. 20–24. doi: 10.1109/SGCF.2018.8408934.

[11] J. A. Babu, H. P. Neha, K. S. Babu, and R. N. Pinto, "Secure Data Retrieval System using Biometric Identification," in *2022 IEEE International Conference on Data Science and Information System (ICDSIS)*, 2022, pp. 1–4. doi: 10.1109/ICDSIS55133.2022.9915968.
[12] A. Bentahar, A. Meraoumia, H. Bendjenna, A. Zeroual, and T. Bentahar, "Combination of Closed-Set and Open-Set Biometric Identification," in *2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, 2022, pp. 1–6. doi: 10.1109/PAIS56586.2022.9946885.
[13] H. O. Shahreza, A. Bassit, S. Marcel, and R. Veldhuis, "Remote Cancelable Biometric System for Verification and Identification Applications," in *2023 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2023, pp. 1–5. doi: 10.1109/BIOSIG58226.2023.10345984.
[14] C.-G. Cordoș, L.-I. Mihăilă, P. Faragó, and S. Hintea, "A Matlab Implementation of a Biometric Identification System Based on Photopletysmograms," in *2023 46th International Conference on Telecommunications and Signal Processing (TSP)*, 2023, pp. 208–211. doi: 10.1109/TSP59544.2023.10197750.
[15] B. Kotkova, "Use of Dynamic Biometric Signature in Communication of Company," in *2023 27th International Conference on Circuits, Systems, Communications and Computers (CSCC)*, 2023, pp. 1–5. doi: 10.1109/CSCC58962.2023.00037.
[16] M. Balaji, P. N, N. Swathi, S. Atheek, M. Manasa, and K. C. Kumar, "Biometric-based Smart Door Locking System using Biometric and OTP," in *2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2023, pp. 898–903. doi: 10.1109/I-SMAC58438.2023.10290425.
[17] Vandana and N. Kaur, "A Study of Biometric Identification and Verification System," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021, pp. 60–64. doi: 10.1109/ICACITE51222.2021.9404735.
[18] Z. Leyu, Z. Xinyou, F. Yunjia, L. Shuyao, B. Jun, and H. Xijia, "Design and Implementation of RFID Access Control System Based on Multiple Biometric Features," in *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, 2021, pp. 570–575. doi: 10.1109/ICCWAMTIP53232.2021.9674127.
[19] A. D. Bykov, V. I. Voronov, L. I. Voronova, and I. A. Zharov, "Web Application Development for Biometric Identification System Based on Neural Network Face Recognition," in *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, 2020, pp. 1–6. doi: 10.1109/IEEECONF48371.2020.9078654.
[20] P. Ramakrishna, K. Sachin, I. A. Rather, M. Vandana, and S. S. Vignesh, "Smart Home Security System Using IoT," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2023, pp. 1–7. doi: 10.1109/ICCCNT56998.2023.10307277.
[21] Shazana Dhiya Ayuni, Syamsudduha Syahrorini, Jamaaluddin Jamaaluddin, "Lapindo Embankment Security Monitoring System Based on IoT," ELINVO (Electronics, Informatics, and Vocational Education), Mei 2021; vol 6 (1): 40-48
ISSN 2580-6424 (printed), ISSN 2477-2399 (online,) DOI: 10.21831/elinvo.v6i1.40429

Conflict of Interest Statement:
The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.