Terbit *online* pada laman: https://ejurnal.umri.ac.id/index.php/JST

Jurnal Surya Teknika

| ISSN (Print) 2354-6751 | ISSN (Online) 2723-7222 |

Research Article

Integrasi Face Detector dengan IoT untuk Sistem Keamanan Pintu Rumah Pintar

Felista Jaka Pramana*, Rini Pujiastutik

Universitas Muhammadiyah Gresik Jl. Sumatera No. 101 GKB, Kabupaten Gresik, Jawa Timur, Indonesia

INFORMASI ARTIKEL

Diserahkan : 8 April 2026
Diterima : 8 Mei 2026
Diterbitkan : 11 Juni 2026

KATA KUNCI

Keamanan rumah, Deteksi wajah, Internet of Things, ESP32, Notifikasi real-time

KORESPONDENSI

*E-mail: jaka.lcd1234@gmail.com

A B S T R A K

Tingginya kasus pencurian rumah di Indonesia mendorong perlunya pengembangan sistem keamanan yang lebih modern dan efektif dibandingkan dengan kunci manual konvensional yang masih memiliki banyak kelemahan. Penelitian ini mengembangkan sistem keamanan pintu rumah berbasis Internet of Things (IoT) dengan menerapkan metode deteksi wajah sebagai sistem autentikasi utama. Sistem dirancang menggunakan ESP32 sebagai kontroler utama yang terintegrasi dengan ESP32-CAM untuk proses pengenalan wajah, keypad 4x4 sebagai media input PIN, sensor getar SW-420 untuk mendeteksi upaya pembobolan paksa, buzzer sebagai alarm peringatan, serta solenoid door lock sebagai aktuator pembuka dan pengunci pintu. Sistem bekerja dengan dua mekanisme autentikasi, yaitu pengenalan wajah dan input PIN, sehingga memberikan keamanan berlapis. Apabila proses autentikasi berhasil, pintu akan terbuka secara otomatis dan sistem akan mengirimkan notifikasi "Pintu terbuka, selamat datang" melalui aplikasi Telegram kepada pemilik rumah. Sebaliknya, jika autentikasi gagal atau sensor getar mendeteksi adanya getaran yang mengindikasikan upaya pembobolan, sistem akan mengaktifkan buzzer sebagai alarm lokal dan mengirimkan pesan peringatan "Tanda bahaya, ada orang asing di rumah" secara real-time. Hasil pengujian menunjukkan bahwa sistem mampu mengenali wajah terdaftar dengan tingkat akurasi yang baik serta mengirimkan notifikasi dengan waktu tunda kurang dari 3 detik. Dengan fitur autentikasi ganda dan notifikasi real-time, sistem ini dinilai mampu meningkatkan keamanan rumah secara signifikan dibandingkan metode konvensional.

A B S T R A C T

The high incidence of home burglaries in Indonesia has driven the need for the development of more modern and effective security systems compared to conventional manual locks, which still have many weaknesses. This research develops an Internet of Things (IoT)-based home door security system by implementing face detection as the primary authentication method. The system is designed using an ESP32 as the main controller, integrated with an ESP32-CAM for face recognition, a 4x4 keypad as a PIN input medium, an SW-420 vibration sensor to detect forced break-in attempts, a buzzer as a warning alarm, and a solenoid door lock as the door-opening and locking actuator. The system operates with two authentication mechanisms, namely face recognition and PIN input, thereby providing layered security. If the authentication process is successful, the door will open automatically and the system will send a notification reading "Door opened, welcome" via the Telegram application to the homeowner. Conversely, if authentication fails or the vibration sensor detects vibrations indicating a break-in attempt, the system will activate the buzzer as a local alarm and send a real-time warning message reading "Danger alert, there is an unauthorized person at the house." Test results show that the system is capable of recognizing registered faces with a good level of accuracy and sending notifications with a delay of less than 3 seconds. With its dual authentication features and real-time notifications, this system is considered capable of significantly improving home security compared to conventional methods.

DOI: 10.37859/jst.v13i1.11279

1. PENDAHULUAN

Berdasarkan laporan Statistik Kriminal 2024, pencurian masih menjadi salah satu tindak kejahatan dengan angka yang cukup tinggi di Indonesia [1]. Bentuk kejahatan tersebut beragam, mulai dari pencurian ringan hingga perampokan dengan kekerasan yang menimbulkan kerugian besar serta meningkatkan kekhawatiran masyarakat terhadap keamanan lingkungan tempat tinggal. Seiring meningkatnya kebutuhan akan rasa aman, teknologi keamanan rumah mengalami perkembangan pesat dengan memanfaatkan sistem modern seperti teknologi pengenalan wajah yang memiliki tingkat akurasi tinggi dan relatif sulit dimanipulasi dibandingkan kunci konvensional [2]. Salah satu perangkat yang banyak digunakan dalam sistem keamanan modern adalah ESP32-CAM, yang mampu mendeteksi wajah sekaligus mengirimkan peringatan otomatis ke aplikasi Telegram sehingga pemilik rumah dapat memantau aktivitas secara real-time dari jarak jauh [3]. Kemampuan serupa juga ditunjukkan pada penelitian lain yang memanfaatkan ESP32-CAM sebagai media pengiriman notifikasi visual melalui Telegram [4]. Selain itu, pemanfaatan mikrokontroler ESP32 yang terhubung dengan perangkat Android melalui komunikasi Bluetooth menunjukkan penerapan konsep Internet of Things (IoT) yang efektif dalam meningkatkan sistem keamanan, khususnya pada kendaraan bermotor [5]. Untuk memperkuat fungsinya, ESP32 sering dikombinasikan dengan berbagai sensor seperti sensor gerak, sensor getar, dan sensor gas guna mendeteksi ancaman pencurian maupun kebakaran [6]. Penambahan keypad 4x4 sebagai lapisan keamanan tambahan juga terbukti mampu memperkecil kemungkinan pembobolan karena akses dibatasi oleh kode sandi yang valid [7]. Dengan dukungan komunikasi data yang cepat dan stabil, sistem keamanan berbasis ESP32 terus berkembang mencakup penguncian otomatis, notifikasi darurat, serta pemantauan visual yang dikirim langsung melalui aplikasi pesan [8]. Integrasi keypad 4x4 dengan ESP32 juga terbukti meningkatkan efisiensi dan keandalan sistem keamanan secara keseluruhan [9]. Penelitian terbaru menunjukkan bahwa penggunaan ESP32-CAM memungkinkan pengiriman bukti visual ke Telegram secara otomatis sehingga pemilik rumah dapat memantau kondisi rumah kapan pun dan di mana pun [10].

Dalam beberapa Tujuan penelitian penulis ingin membuat system keamanan pintu rumah pintar dengan menggunakan 2 modul dan 1 sensor sebagai input yaitu ESP-32 CAM, keypad 4x4, buzzer dan vibration sensor SW-420 kemudian untuk processor saya mengunakan ESP-32 dan output menggunakan Selenoid Lockdoor.

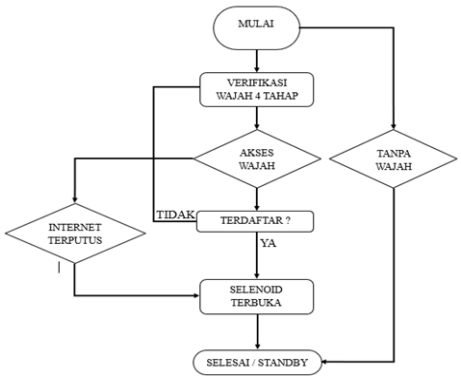
2. METODOLOGI

Metode penelitian dimulai dengan studi literatur, yaitu mencari informasi melalui buku-buku, jurnal, artikel, dan internet yang berhubungan dengan elemen-elemen yang dipakai dalam penelitian ini. Sumber langsung didapatkan dari hasil diskusi maupun konsultasi dengan dosen atau orang yang mempunyai kompetensi di bidang ini. Adapun literatur-literatur yang dipelajari adalah

a. Metode Face Detection
b. Skenario pengujian modul sistem
c. Skenario pengujian keseluruhan alat

2.1. Metode face detector dengan teori LBPH

Perangkat lunak pada sistem keamanan ini dibuat menggunakan metode *face detection* dengan mikrokontroler ESP32 sebagai pusat kendali. Pada tahap awal, program menyiapkan library untuk ESP32-CAM, Keypad 4x4, sensor getar SW-420, buzzer, serta koneksi Wi-Fi yang dipakai untuk menghubungkan sistem dengan aplikasi Telegram. Kamera diatur agar bisa mengenali citra wajah yang sudah tersimpan dan dengan teori LBPH yang bekerja membaca pola tekstur wajah dengan nilai terang dan gelap antar piksel mengunakan software open cv bahasa phyton, sementara keypad digunakan untuk memasukkan kode akses.



Gambar 1. Metode Face Detector LBPH

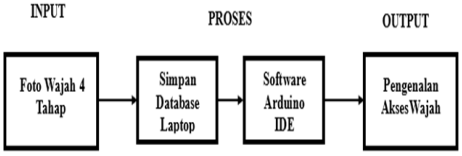
Sistem keamanan pintu rumah pintar ini menerapkan mekanisme autentikasi ganda menggunakan deteksi wajah berbasis ESP32-CAM dan input PIN melalui keypad 4x4. Proses autentikasi bekerja secara **paralel**, di mana sistem secara **fleksibel** bisa proses pengenalan wajah atau pembacaan PIN yang dimasukkan pengguna. Wajah pengguna akan diproses menggunakan metode *Local Binary Pattern Histogram (LBPH),* sedangkan PIN akan diverifikasi berdasarkan data yang tersimpan pada sistem. Pintu hanya akan terbuka apabila salah satu autentikasi tersebut berhasil dilakukan. Jika salah satu autentikasi gagal, maka sistem akan menolak akses dan pintu tetap dalam kondisi terkunci. Mekanisme ini diterapkan untuk meningkatkan tingkat keamanan sistem keamanan rumah berbasis *Internet of Things (IoT).*
Metode Local Binary Pattern Histogram (LBPH) pada penelitian ini dikonfigurasi menggunakan parameter sebagai berikut:

Tabel 1.
Parameter Pada LBPH

Parameter	Nilai
Radius	1
Neighbors	8
Grid_x	8
Grid_y	8
Threshold	60

2.1 Prosedur Perekaman Data

Pada perekaman data disini dilakukan proses pengambilan foto wajah orang minimal **10 orang** dengan pengambilan foto tampak depan, samping kanan dan kiri, belakang. Setelah itu data akan tersimpan di data base laptop yang tersedia dan bisa di lanjut ke proses pembuatan progam di Arduino IDE. Sebagai mana pada gambar diagram di bawah ini :



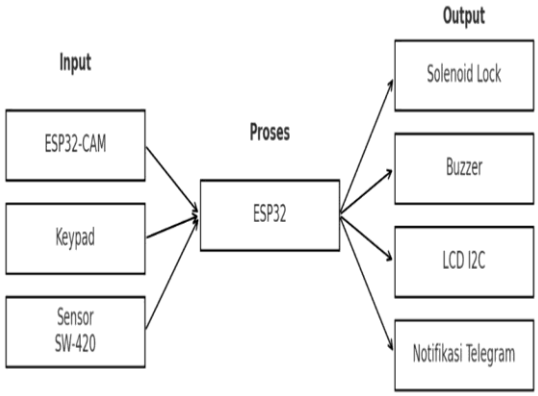
Gambar 2. Diagram alur perekaman data

2.1.1. Etika Prosedur Pengambilan Data

Pengambilan data wajah pada penelitian ini melibatkan partisipan yang merupakan teman dan kerabat peneliti. Sebelum proses pengambilan data dilakukan, setiap partisipan telah diberikan penjelasan mengenai tujuan penelitian, metode yang digunakan, serta pemanfaatan data yang diambil. Seluruh partisipan kemudian memberikan persetujuan secara sadar *(informed consent)* untuk berpartisipasi dalam penelitian ini Data wajah yang dikumpulkan hanya digunakan untuk keperluan pengujian sistem pengenalan wajah dan tidak digunakan untuk tujuan lain di luar penelitian. Untuk menjaga privasi, identitas partisipan tidak dicantumkan dalam publikasi, dan seluruh data disimpan secara lokal oleh peneliti tanpa disebarluaskan kepada pihak lain.
Penelitian ini juga memastikan bahwa proses pengambilan data dilakukan secara sukarela tanpa adanya paksaan, serta tidak menimbulkan risiko atau dampak negatif bagi partisipan. Dengan demikian, penelitian ini telah memperhatikan dan melibatkan manusia yang mengacu pada prinsip etika penelitian manusia yang meliputi persetujuan partisipan, kerahasiaan data, dan penggunaan data secara terbatas.

2.2 Perancangan Sistem

Perancangan sistem keamanan rumah ini menggunakan ESP32 sebagai pusat kendali yang terhubung dengan berbagai perangkat input dan output. ESP32-CAM berfungsi untuk mengenali wajah pengguna yang sudah terdaftar, sedangkan Keypad 4x4 digunakan sebagai sarana memasukkan sandi akses. Kedua autentikasi ini berjalan secara paralel, sehingga pintu hanya terbuka jika wajah teridentifikasi dengan benar dan sandi yang dimasukkan sesuai. Jika autentikasi berhasil, sistem akan mengirimkan notifikasi ke aplikasi Telegram berupa pesan *"Pintu terbuka, selamat datang"*.



Gambar 3. Diagram Blok Sistem

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil pengujian yang telah dilakukan, sistem keamanan pintu rumah berbasis Internet of Things (IoT) yang dirancang dapat berfungsi sesuai dengan tujuan penelitian dan menunjukkan kinerja yang baik dalam mengontrol akses masuk. Seluruh

komponen utama seperti ESP32 sebagai pengendali sistem, ESP32-CAM sebagai modul pengenalan wajah, keypad 4x4 sebagai input PIN, sensor getar SW-420 sebagai pendeteksi pembobolan, buzzer sebagai alarm, serta solenoid door lock sebagai aktuator dapat terintegrasi dan bekerja secara sinkron. Proses pengenalan wajah dilakukan dengan menangkap citra secara real-time dan membandingkannya dengan data wajah yang telah diregistrasi sebelumnya, di mana sistem menunjukkan tingkat keberhasilan yang baik pada kondisi pencahayaan cukup dan jarak optimal antara 30–70 cm, meskipun akurasi dapat menurun pada kondisi cahaya rendah atau sudut wajah yang tidak sejajar dengan kamera. Untuk meningkatkan keamanan, sistem menerapkan autentikasi ganda melalui kombinasi pengenalan wajah dan input PIN, sehingga akses hanya diberikan ketika data yang dimasukkan sesuai dengan database. Ketika autentikasi berhasil, solenoid door lock aktif dan pintu terbuka secara otomatis dalam durasi tertentu sebelum kembali terkunci, sedangkan apabila autentikasi gagal atau sensor getar mendeteksi indikasi pembobolan, buzzer akan aktif dan sistem mengirimkan notifikasi peringatan melalui Telegram dengan waktu tunda kurang dari 3 detik pada jaringan WiFi yang stabil. Secara keseluruhan, integrasi antara proses input, pengolahan data oleh mikrokontroler, serta output berupa aktuator dan notifikasi real-time menunjukkan bahwa sistem yang dirancang memiliki tingkat keandalan yang baik dan mampu memberikan peningkatan keamanan dibandingkan metode kunci konvensional.

3.1 Hasil Pengujian Kondisi Cahaya Dan Sudut Wajah

Pengujian tambahan dilakukan pada beberapa kondisi pencahayaan dan sudut wajah untuk mengetahui tingkat keandalan sistem dalam melakukan proses pengenalan wajah. Berdasarkan hasil pengujian, sistem bekerja optimal pada kondisi pencahayaan cukup dan posisi wajah frontal terhadap kamera. Pada kondisi pencahayaan rendah *(low-light)*, sistem masih mampu melakukan deteksi wajah dengan bantuan flash LED bawaan ESP32-CAM, meskipun performa pengenalan mengalami sedikit penurunan. Selain itu, perubahan sudut wajah hingga ±15° masih dapat dikenali dengan baik, sedangkan pada sudut ±30° akurasi sistem mulai menurun karena sebagian fitur wajah tidak dapat terbaca secara optimal oleh metode *Local Binary Pattern Histogram (LBPH)*.

Tabel 2
Pengujian Kondisi Cahaya

Kondisi Cahaya	Hasil Deteksi
Terang (pagi – siang)	Berhasil
Redup (menjelang sore)	Kurang optimal
Malam + Flash ESP32-CAM	Berhasil

Tabel 3.
Pengujian Sudut Wajah

Sudut Wajah	Hasil
0° (Frontal)	Berhasil
15°	Berhasil
30°	Akurasi menurun
45°	Tidak Terdeteksi

3.2 Hasil Pengujian Sisrem

Berdasarkan Tabel 2, seluruh pengujian menunjukkan bahwa sistem bekerja sesuai dengan yang diharapkan. Autentikasi melalui pengenalan wajah maupun input PIN dapat membuka pintu ketika valid, sedangkan akses tidak sah berhasil ditolak oleh sistem. Sensor getar SW-420 mampu mendeteksi indikasi pembobolan dan mengaktifkan alarm serta notifikasi Telegram secara real-time. Waktu pengiriman notifikasi tercatat memiliki delay kurang dari 3 detik pada kondisi jaringan stabil. Secara keseluruhan, sistem keamanan pintu rumah berbasis IoT ini telah memenuhi tujuan perancangan dengan tingkat respons dan keandalan yang baik.

Tabel 4
Hasil pengujian Sistem Keseluruhan

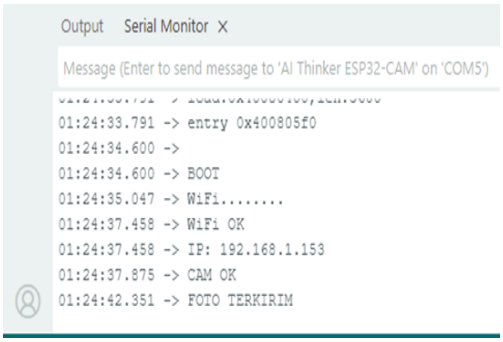
No	Skenario	Input	Output Sistem
1	Wajah Terdaftar	Wajah dikenali	Pintu terbuka + notifikasi Telegram
2	Wajah Tidak Terdaftar	Wajah tidak dikenal	Buzzer aktif + notifikasi bahaya
3	PIN Benar dan Salah	Penyesuaian PIN	Pintu terbuka atau di tolak notifikasi Telegram
4	Deteksi Getaran	Ada getaran	Buzzer aktif + notifikasi bahaya
5	WiFi Stabil	terhubung	Notif terkirim (< 3 detik)

3.3 Pembahasan

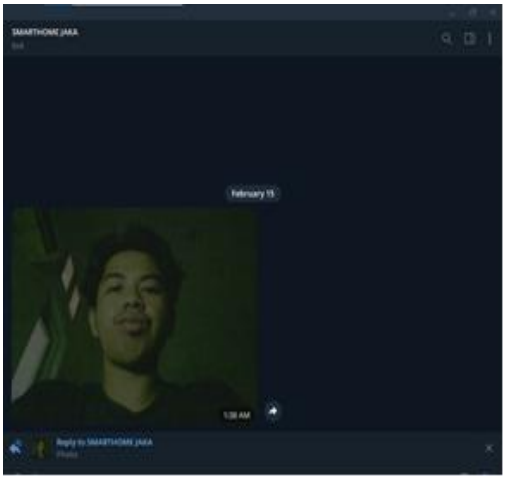
3.3.1 Proses Pengenalan Wajah

Sistem dimulai dari ESP32-CAM yang diprogram menggunakan Arduino IDE. Modul

dikonfigurasi untuk menangkap citra dengan resolusi 640×480 piksel dalam format JPEG. Setelah perangkat terhubung ke jaringan WiFi, sistem akan mengambil gambar ketika dipicu dan mengirimkan file citra tersebut ke Telegram Bot melalui koneksi HTTPS. Proses pengiriman dilakukan menggunakan HTTP request ke API Telegram dengan menyertakan token bot dan chat ID. Keberhasilan pengiriman ditandai dengan status respon HTTP 200 dan citra diterima pada aplikasi Telegram dalam waktu rata-rata ±1,5 detik pada jaringan stabil.



Gambar 4. Hasil Progam Arduino IDE



Gambar 5. Hasil Foto Di kirim Telegram

3.1.1. Pengenalan Wajah Dengan LBPH

Citra yang diterima melalui Telegram kemudian diunduh dan diproses menggunakan *Python* dengan *library Open CV*. Tahap awal adalah konversi citra ke grayscale untuk menyederhanakan informasi warna dan mempercepat proses komputasi. Selanjutnya dilakukan deteksi wajah menggunakan Haar Cascade Classifier untuk menentukan area wajah yang akan dianalisis.Ekstraksi fitur dilakukan menggunakan metode *Local Binary Pattern Histogram* (LBPH). Metode ini bekerja dengan membandingkan intensitas piksel pusat dengan piksel di sekitarnya untuk membentuk pola biner, kemudian pola tersebut dikonversi menjadi histogram distribusi tekstur. Histogram citra uji dibandingkan dengan histogram dataset pelatihan yang telah tersimpan.Keputusan identifikasi ditentukan berdasarkan nilai confidence yang dihasilkan. Sistem menggunakan threshold sebesar 60. Jika nilai confidence ≤ 60, wajah dinyatakan dikenali. Jika nilai confidence > 60, wajah dikategorikan tidak dikenali.

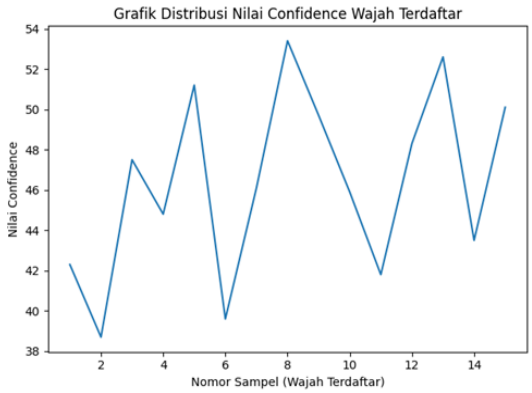
Gambar 6. Hasil Pengenalan Wajah Dikenal Dan tidak

3.1.2. Analisis Nilai Confidence Dan Akurasi Sistem

Pengujian sistem dilakukan terhadap 20 subjek yang telah terdaftar pada database serta beberapa wajah yang tidak terdaftar. Setiap subjek diuji sebanyak 5 kali pada kondisi pencahayaan normal dengan jarak 30–70 cm dari kamera. Berikut merupakan hasil pengujian nilai confidence yang diperoleh dari proses identifikasi menggunakan metode LBPH.

Tabel 5.
Nilai Confidence Wajah Di Kenali

No	Person	Confidence	Threshold	Status Sistem
1	User 1	42.3	< 60	Dikenali
2	User 2	38.7	< 60	Dikenali
3	User 3	47.5	< 60	Dikenali
4	User 4	44.8	< 60	Dikenali
5	User 5	51.2	< 60	Dikenali
6	User 6	39.6	< 60	Dikenali
7	User 7	46.1	< 60	Dikenali
8	User 8	53.4	< 60	Dikenali
9	User 9	49.7	< 60	Dikenali
10	User 10	45.9	< 60	Dikenali
11	User 11	41.8	< 60	Dikenali
12	User 12	48.3	< 60	Dikenali
13	User 13	52.6	< 60	Dikenali
14	User 14	43.5	< 60	Dikenali
15	User 15	50.1	< 60	Dikenali

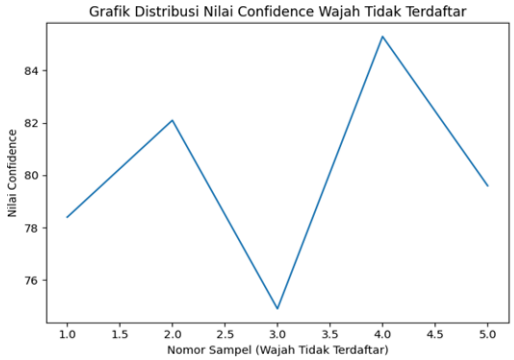


Gambar 7. Grafik Nilai Confidence Yang Terdaftar

Rata-rata confidence wajah terdaftar adalah 45,92 yang berada di bawah threshold 60 sehingga seluruh subjek berhasil dikenali sistem. Pengujian juga dilakukan terhadap wajah yang tidak terdaftar pada database.

Tabel 6.
Nilai Confidence Wajah Asing

No	Person	Confidence	Threeshold	Status Sistem
1	**User 16**	**78.4**	**> 60**	**Tidak dikenali**
2	**User 17**	**82.1**	**> 60**	**Tidak dikenali**
3	**User 18**	**74.9**	**> 60**	**Tidak dikenali**
4	**User 19**	**85.3**	**> 60**	**Tidak dikenali**
5	**User 20**	**79.6**	**> 60**	**Tidak dikenali**



Gambar 8 Grafik Confidence Wajah Asing

Berdasarkan grafik distribusi nilai confidence, terlihat adanya perbedaan yang signifikan antara wajah terdaftar dan tidak terdaftar. Wajah terdaftar memiliki rata-rata nilai confidence sebesar 45,92 yang berada di bawah threshold 60, sedangkan wajah tidak terdaftar memiliki rata-rata sebesar 80,06 yang berada di atas threshold. Jarak nilai ini menunjukkan bahwa threshold yang digunakan mampu memisahkan kedua kategori secara jelas.

3.1.3. Perhitungan Akurasi

Total pengujian dilakukan sebanyak:

- 20 pengujian wajah terdaftar
- 5 pengujian wajah tidak terdaftar

Jumlah identifikasi benar : 15
Jumlah pengujian total : 20
Akurasi dihitung menggunakan persamaan:
Akurasi = (Jumlah Identifikasi Benar / Total Pengujian) × 100%
Akurasi = (15 / 20) × 100% = 75 %

Nilai akurasi sebesar 75% dipengaruhi oleh kondisi pencahayaan, posisi wajah terhadap kamera, serta keterbatasan jumlah data pelatihan yang digunakan. Metode Local Binary Pattern Histogram (LBPH) yang diterapkan pada penelitian ini memiliki sensitivitas terhadap perubahan intensitas cahaya dan orientasi wajah sehingga performa sistem dapat menurun pada kondisi low-light atau sudut wajah yang tidak sejajar dengan kamera. Sistem bekerja optimal pada kondisi pencahayaan cukup, khususnya pada pagi hingga sore hari dengan jarak pengambilan citra sekitar 30–70 cm, sedangkan pada kondisi minim cahaya sistem memanfaatkan fitur flash LED bawaan ESP32-CAM sebagai pencahayaan tambahan saat proses deteksi wajah dilakukan. Selain itu, dataset wajah yang masih terbatas menyebabkan variasi ekspresi dan sudut wajah belum sepenuhnya terakomodasi dalam proses training sistem. Meskipun demikian, sistem tetap mampu menjalankan autentikasi wajah dengan baik dan dapat diterapkan sebagai sistem keamanan pintu rumah pintar berbasis Internet of Things (IoT).

3.1.4. Analisis Error Sistem Menggunakan FAR dan FRR

Selain pengujian akurasi, penelitian ini juga melakukan analisis error menggunakan parameter *False Acceptance Rate (FAR)* dan *False Rejection Rate (FRR)*. *FAR* merupakan kondisi ketika sistem salah menerima wajah yang tidak terdaftar sebagai pengguna valid, sedangkan *FRR* merupakan kondisi ketika sistem gagal mengenali pengguna yang sebenarnya telah terdaftar.
Berdasarkan hasil pengujian, sistem menunjukkan nilai *FAR* yang rendah karena wajah yang tidak terdaftar sebagian besar berhasil ditolak oleh sistem. Namun, pada kondisi pencahayaan rendah *(low-light)* dan sudut wajah tertentu, sistem mengalami false rejection sehingga nilai *FRR* meningkat. Hal ini disebabkan metode *Local Binary Pattern Histogram (LBPH)* sensitif terhadap perubahan pencahayaan dan orientasi wajah.

Secara keseluruhan, sistem bekerja lebih optimal pada kondisi pencahayaan cukup dan posisi wajah frontal terhadap kamera.

Tabel 7
Analisis FAR dan FRR

Parameter	Hasil	Keterangan
FAR	Rendah	Wajah tidak terdaftar dan di tolak
FRR	Sedang	kondisi low-light dan sudut wajah tertentu
Penyebab Error	Pencahayaan dan sudut wajah	Pengaruh proses pengenalan wajah

Rumus FAR dan FRR

False Acceptance Rate (FAR):

$$FAR = \frac{\text{False Acceptance}}{\text{Total Unauthorized Access Attempts}} \times 100\%$$

False Rejection Rate (FRR):

$$FRR = \frac{\text{False Rejection}}{\text{Total Authorized Access Attempts}} \times 100\%$$

Keterangan:

- False Acceptance = jumlah wajah asing yang salah dikenali sistem.
- False Rejection = jumlah wajah terdaftar yang gagal dikenali sistem.

Tabel 8
Contoh Eror Sistem

Error	Kondisi	Dampak
FRR	Low-light	Pengguna valid gagal dikenali
FRR	Sudut wajah ±45°	Autentikasi gagal
FAR	Wajah asing mirip database	Pintu berpotensi terbuka

Pada bagian Tabel 5, error sistem beberapa terjadi pada kondisi pencahayaan rendah dan sudut wajah yang tidak sejajar dengan kamera. Kondisi tersebut mempengaruhi proses ekstraksi fitur wajah oleh metode LBPH sehingga menyebabkan penurunan performa sistem pengenalan wajah Untuk meningkatkan performa sistem, penelitian selanjutnya dapat menggunakan preprocessing citra dan metode deep learning agar sistem lebih adaptif terhadap perubahan pencahayaan dan orientasi wajah

4. SIMPULAN

Penelitian ini bisa jadi inspirasi sistem keamanan pintu rumah pintar berbasis Internet of Things (IoT) yang lebih canggih dibandingkan penggunaan kunci konvensional. Dengan menggabungkan teknologi pengenalan wajah menggunakan metode Local Binary Pattern Histogram (LBPH) dan input PIN melalui keypad 4x4, sistem ini mampu menerapkan autentikasi ganda sehingga pintu hanya dapat dibuka apabila kedua proses autentikasi berhasil dilakukan secara bersamaan. Seluruh komponen yang digunakan, mulai dari ESP32 sebagai pengendali utama, ESP32-CAM, sensor getar SW-420, buzzer, relay, hingga solenoid door lock, terbukti dapat bekerja secara terintegrasi dalam satu sistem. Dari sisi performa, sistem mampu mengenali wajah terdaftar dengan akurasi sebesar 75% pada kondisi pencahayaan normal dan jarak pengambilan citra sekitar 30–70 cm. Selain itu, nilai rata-rata confidence wajah terdaftar sebesar 45,92 dan wajah tidak terdaftar sebesar 80,06 menunjukkan bahwa sistem cukup baik dalam membedakan pengguna terdaftar dan tidak terdaftar.

Tentu sistem ini masih punya ruang untuk dikembangkan lebih lanjut, terutama dalam hal akurasi pengenalan wajah di kondisi pencahayaan buruk atau sudut wajah yang miring. Namun secara keseluruhan, sistem yang dirancang ini cukup menjadi solusi.

DAFTAR PUSTAKA

[1] Trophy Endah Rahayu, "STATISTIK KRIMINAL 2024," *badan Pus. Stat.*, vol. 15, pp. 3–210, Dec. 2024.

[2] A. Arifudin, "Rancang Bangun Sistem Keamanan Pintu Rumah Menggunakan Metode Segitiga Wajah (triangle face) Berbasis Raspberry Pi," *J. Teknol. Elektro*, vol. 12, no. 1, p. 29, Jan. 2021, doi: 10.22441/jte.2021.v12i1.006.

[3] R. Muwardi and R. R. Adisaputro, "Design Sistem Keamanan Pintu Menggunakan Face Detection," *J. Teknol. Elektro*, vol. 12, no. 3, p. 120, Oct. 2021, doi: 10.22441/jte.2021.v12i3.004.

[4] J. Arifin and J. Frenando, "Sistem Keamanan Pintu

Rumah Berbasis Internet of Things via Pesan Telegram Home Door Security System Based on Internet of Things Through Telegram Message," *TELKA*, vol. 8, no. 1, pp. 49–59, 2022.

[5] F. A. Aryatama and S. Samsugi, "Sistem Keamanan Kendaraan Bermotor Dengan ESP32 Menggunakan Kontrol Android," *SMATIKA J.*, vol. 14, no. 01, pp. 167–181, Jul. 2024, doi: 10.32664/smatika.v14i01.1267.

[6] H. Jurnal, D. Setiawan, A. Dianta, and D. Kurniawan, "JURNAL INFORMATIKA DAN TEKONOLOGI KOMPUTER SISTEM KEAMANAN RUANGAN LABORATORIUM KOMPUTER MENGGUNAKAN SENSOR PIR, MQ-7, SW420 DAN RFID BERBASIS SMS," vol. 1, no. 3, pp. 47–56, 2021.

[7] R. Riskawati *et al.*, "Desain Sistem Deteksi Password pada Keypad dan LCD dengan Arduino melalui Tinkercard untuk Pembelajaran Elektronika," *J. Artif. Inform. dan Sist. Inf.*, vol. 3, no. 1, pp. 69–78, Apr. 2025, doi: 10.54065/artificial.686.

[8] Fachma Oktafiani and Dandun Widhiantoro, "Studi Literatur Penggunaan ESP32 untuk Sistem Keamanan Lingkungan Rumah," *Semin. Nas. Inov. Vokasi*, vol. 4, no. 1, pp. 267–274, Jun. 2025.

[9] G. Aji Pangestu and M. Yusuf Asyhari, "Sistem Keamanan Rumah Berbasis Internet of Things (IoT) Menggunakan Notifikasi Bot Telegram untuk Pendeteksian Gerak," *J. Smart Syst.*, vol. 4, no. 1, Jul. 2024.

[10] E. Alfonsius, A. S. Ruitan, and D. Liuw, "Pengembangan Sistem Keamanan Pintu Menggunakan Metode Prototype Berbasis RFID dan Keypad 4x4 dengan Arduino Nano," *J. Ilm. Inform. dan Ilmu Komput.*, vol. 3, no. 2, pp. 110–123, Sep. 2024, doi: 10.58602/jima-ilkom.v3i2.33.