

Prototipe Sistem Keamanan Kunci Pintu Rumah Otomatis Dengan Pengenalan Wajah Berbasis IoT

Niam Tamami¹, Achmad Rizky Ramadhani², Hary Oktavianto³, Rifqi Nabila Zufar⁴

niam@pens.ac.id¹, rizkyrama050@gmail.com², hary@pens.ac.id³,

rifqinabilazufar@uinsatu.ac.id⁴

^{1,2,3} Jurusan Teknik Elektro, Politeknik Elektronika Negeri Surabaya

⁴ Jurusan Ilmu Keguruan, UIN Sayyid Ali Rahmatullah Tulungagung

Informasi Artikel

Diterima : 19 Sep 2025
Direvisi : 17 Nov 2025
Disetujui : 3 Des 2025

Kata Kunci

Sistem Kunci Pintu,
Pengenalan Wajah,
Raspberry Pi, Local
Binary Pattern
Histogram.

Abstrak

Dalam era digital yang semakin berkembang, teknologi telah mengubah sistem keamanan dengan menggantikan kunci pintu konvensional dengan kunci pintu pintar yang canggih. Teknologi seperti pengenalan wajah, sidik jari, dan sensor gerak memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan kunci tradisional. Kunci pintu konvensional rentan terhadap risiko pembobolan, kehilangan, atau duplikasi oleh pelaku kejahatan. Sebagai solusi, penulis ingin menciptakan kunci pintu pintar yang dapat membuka pintu dengan pengenalan wajah, *Personal Identification Number (PIN)*, dan melalui *Telegram bot*. Pengenalan wajah pada kunci pintu pintar memastikan bahwa hanya pemilik atau orang yang terdaftar yang dapat membuka pintu. Fitur tambahan berupa penggunaan PIN memberikan lapisan keamanan ekstra. Jika PIN yang salah dimasukkan sebanyak tiga kali, alarm akan berbunyi untuk memberikan peringatan. Selain itu, jika sistem pengenalan wajah tidak dapat mengenali wajah yang sedang dipindai, kamera akan mengambil gambar dan mengirimkannya ke *Telegram bot* di *smartphone* pengguna. Dengan penerapan kunci pintu pintar ini, diharapkan keamanan dan kemudahan akses yang lebih baik dibandingkan dengan kunci pintu konvensional. Hasil pengujian menunjukkan bahwa sistem ini dapat bekerja dengan akurasi pengenalan wajah sebesar 79% dan respon alarm bekerja secara *real-time* melalui integrasi *Telegram bot*.

Keywords

Lock System, Face
Recognition, Raspberry Pi,
Local Binary Pattern
Histogram.

Abstract

In today's rapidly developing digital era, technology has transformed security systems by replacing traditional door locks with advanced smart locks. Technologies such as facial recognition, fingerprint scanning, and motion sensors offer a higher level of security compared to conventional keys. Traditional door locks are vulnerable to break-ins, loss, or duplication by criminals. As a solution, this project aims to develop a smart door lock that can be unlocked using facial recognition, a Personal Identification Number (PIN) code, and through Telegram bot. The facial recognition feature ensures that only the owner or registered users can unlock the door. An additional layer of security is provided through the use of a PIN. If the wrong PIN is entered three times, an alarm will sound as a warning. Furthermore, if the system fails to recognize a face, the camera will capture an image and send it to the user's smartphone via Telegram bot. With this smart door lock, it is expected that security and ease of access will be improved compared to conventional locks. Testing results show that the system operates with a facial recognition accuracy of 79%, and the alarm responds in real-time through Telegram bot integration.

A. Pendahuluan

Dalam era digital yang semakin berkembang pesat seperti sekarang ini, teknologi telah menjadi bagian tak terpisahkan dari kehidupan manusia[1]. Perkembangan teknologi yang sangat pesat memberikan manfaat yang sangat besar dalam kehidupan manusia, di mana pekerjaan manusia menjadi lebih mudah dan efisien setiap harinya[2]. Teknologi telah mempengaruhi hampir semua aspek kehidupan manusia, termasuk dalam bidang keamanan. Dengan adanya teknologi, sistem keamanan saat ini semakin canggih dan efektif dalam mencegah tindakan kriminal dan melindungi aset manusia[3]. Contoh penerapan teknologi pada bidang keamanan adalah pada kunci, seperti pada kunci pintu, lemari, brankas, dan lainnya. Teknologi saat ini telah menghasilkan berbagai inovasi pada sistem keamanan kunci pintu, di mana sekarang penggunaan kunci tradisional semakin digantikan oleh teknologi canggih seperti pengenalan wajah, sidik jari, sensor gerak dan lain-lain.

Kunci memiliki fungsi yang sangat penting dalam menjaga keamanan pada pintu yang merupakan sebuah akses untuk memasuki sebuah ruangan. Kunci menjaga segala sesuatu yang ada di dalam ruangan agar tetap aman. Dengan keamanan kunci yang baik, pemilik akan merasa lebih aman saat meninggalkan rumah tanpa rasa khawatir. Saat ini, penggunaan kunci pintu konvensional berbentuk fisik masih mendominasi sistem pengamanan rumah. Meskipun mudah dioperasikan dan berbiaya rendah, sistem ini memiliki kelemahan signifikan karena rentan terhadap tindakan pembobolan. Selain itu, kunci konvensional dengan anak kunci yang masih berbentuk fisik juga rawan sekali tertinggal, hilang, diduplikasi pelaku kejahatan, bahkan dapat saja rusak sehingga mengakibatkan kita menjadi kesulitan untuk mengakses ruangan yang sedang terkunci[4].

Penelitian sebelumnya telah mengembangkan sistem keamanan pintu otomatis berbasis *Arduino UNO* dan *ESP32-CAM*, yang menggabungkan teknologi pengenalan wajah dengan autentikasi *Personal Identification Number (PIN)*. Sistem ini terdiri dari beberapa komponen utama seperti *keypad* untuk input PIN, *Liquid Crystal Display (LCD)* untuk menampilkan informasi status, *relay* sebagai saklar, serta *solenoid door lock* sebagai pengunci pintu otomatis. *ESP32-CAM* digunakan untuk mendeteksi dan mengenali wajah pengguna, sementara *Arduino UNO* berperan sebagai pusat kendali seluruh proses. Hasil dari penelitian tersebut menunjukkan bahwa sistem mampu meningkatkan keamanan dibandingkan kunci konvensional. Namun, sistem tersebut belum dilengkapi fitur notifikasi jarak jauh, seperti integrasi dengan aplikasi komunikasi atau sistem alarm otomatis, yang menjadi peluang pengembangan lebih lanjut dalam meningkatkan keamanan dan kenyamanan pengguna.

Oleh karena itu, penulis ingin membuat sebuah kunci pintu pintar yang dapat dibuka menggunakan pengenalan wajah, PIN, dan juga *Telegram bot*, sehingga diharapkan dapat meningkatkan keamanan kunci pintu dibandingkan menggunakan kunci pintu konvensional. Dengan menerapkan pengenalan wajah pada kunci pintu, maka kunci hanya dapat dibuka oleh wajah pemilik atau wajah orang yang sudah terdaftar saja karena semua orang memiliki karakteristik wajah yang berbeda[5][6]. Fitur keamanan tambahan pada kunci pintu pintar mencakup sistem autentikasi berbasis PIN. Apabila terjadi kesalahan dalam memasukkan PIN sebanyak tiga kali, alarm akan menyala secara otomatis sebagai mekanisme pencegahan terhadap upaya pembobolan. Pada saat sistem pengenalan wajah tidak

dapat mengenali wajah yang sedang dipindai maka kamera akan mengambil gambar secara otomatis lalu kemudian mengirimkan gambar tersebut ke *Telegram bot* pada *smartphone* pengguna.

Hasil pengujian sistem menunjukkan bahwa fitur pengenalan wajah mampu bekerja dengan akurasi sebesar 79%, sementara sistem alarm dapat merespons secara *real-time* saat PIN salah dimasukkan atau wajah tidak dikenali. Selain itu, integrasi dengan berhasil mengirimkan gambar dan notifikasi ke *smartphone* pengguna dengan respon cepat dan stabil. Dengan hasil tersebut, kunci pintu pintar ini diharapkan dapat memberikan tingkat keamanan dan kemudahan akses yang lebih baik dibandingkan kunci pintu konvensional yang mayoritas masih digunakan saat ini.

B. Perancangan dan Desain Sistem

Tahap awal dalam penelitian ini adalah akuisisi citra, yang merupakan proses penting untuk mendapatkan citra digital. Langkah ini bertujuan untuk menentukan kebutuhan data sekaligus memilih metode yang tepat dalam perekaman citra digital [7]. Dalam penelitian ini, webcam digunakan sebagai perangkat utama untuk menangkap citra digital. Algoritma *Haar-cascade Classifier* diterapkan untuk mendeteksi wajah manusia secara *real-time* dengan efisiensi tinggi, memanfaatkan jumlah piksel dalam area persegi pada citra. Sementara itu, metode *Local Binary Pattern Histogram (LBPH)* digunakan untuk pengenalan wajah karena keunggulannya dalam memberikan akurasi yang tinggi. Penelitian ini mencakup empat tahapan utama, yaitu deteksi wajah menggunakan *Haar-cascade Classifier*, pengenalan wajah dengan LBPH, serta perancangan sistem dan perancangan perangkat keras, yang akan dijelaskan lebih rinci pada bagian berikutnya.

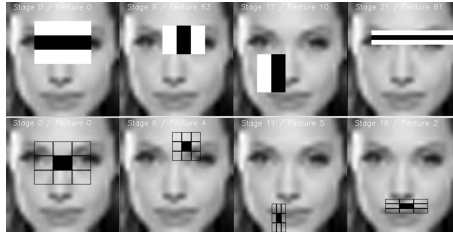
1. Pendeteksi Wajah

Deteksi wajah merupakan salah satu dasar dalam teknologi pengenalan wajah. OpenCV menyediakan algoritma *Haar-cascade Classifier* yang dapat digunakan untuk mendeteksi wajah pada citra digital. Pada penelitian ini, *Haar-cascade* diterapkan sebagai metode utama dalam proses deteksi wajah. Algoritma ini digunakan karena memiliki keunggulan dalam hal kecepatan dan akurasi yang tinggi. *Haar-cascade Classifier* dikembangkan oleh Paul Viola dan Michael Jones, yang melatih algoritma ini menggunakan sejumlah besar citra positif (berisi wajah) dan citra negatif (tanpa wajah) [8], [9], [10]. Setiap fitur adalah nilai tunggal yang diperoleh dengan mengurangi jumlah piksel dibawah persegi panjang putih dari jumlah piksel dibawah persegi panjang hitam. Nilai tunggal untuk fitur Haar dihitung menggunakan persamaan berikut:

$$\text{Nilai tunggal} = \text{hitam} - \text{putih} = \frac{1}{n} \sum_{\text{hitam}}^n I(x) - \frac{1}{n} \sum_{\text{Putih}}^n I(x) \quad (1)$$

Dimana n adalah jumlah piksel dan $I(x)$ adalah nilai sebenarnya yang terdeteksi pada sebuah citra.

Citra wajah dikelompokkan berdasarkan perbedaan antara area terang dan gelap. Sebagai contoh, area sekitar mata biasanya lebih gelap dibandingkan dengan area sekitarnya, seperti yang ditunjukkan pada Gambar 1.

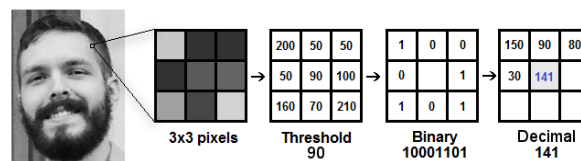


Gambar 1. *Haar-Cascade Classifier*

2. Pengenalan Wajah

Pengenalan wajah adalah proses identifikasi wajah seseorang yang berkaitan dengan sistem penglihatan, dan telah menjadi alat interaksi manusia-komputer yang penting. Teknologi ini banyak digunakan dalam berbagai aplikasi, seperti sistem keamanan, kontrol akses, pengawasan video, area komersial, bahkan pada platform jejaring sosial seperti *Facebook*. Dengan pesatnya perkembangan kecerdasan buatan, pengenalan wajah kembali menarik perhatian karena sifatnya yang tidak mengganggu dan kemampuannya menjadi metode utama identifikasi manusia dibandingkan teknik biometrik lainnya. Teknologi ini dapat digunakan tanpa memerlukan kesadaran subjek[7], [11].

Pada algoritma LBPH, pengolahan citra dimulai dengan tahap preprocessing, salah satunya mengubah citra asli (berwarna/RGB) menjadi citra abu-abu (*grayscale*). Setiap piksel pada citra *grayscale* memiliki nilai intensitas tunggal yang berada dalam rentang 0-255, sedangkan citra berwarna membutuhkan tiga nilai intensitas untuk setiap piksel pada rentang yang sama. Semakin mendekati nilai 255, semakin terang tingkat keabuan piksel tersebut[12], [13]. Setelah itu, nilai intensitas setiap piksel dalam rentang 0-255 dikonversi menjadi nilai biner. Jika nilai intensitas sama atau lebih besar dari nilai tengah, maka piksel diberi nilai biner 1; sebaliknya, jika lebih kecil dari nilai tengah, nilainya adalah 0. Proses konversi intensitas piksel pada citra *grayscale* menjadi biner menggunakan metode LBPH[14], [15], [16] dapat dilihat seperti pada Gambar 2.



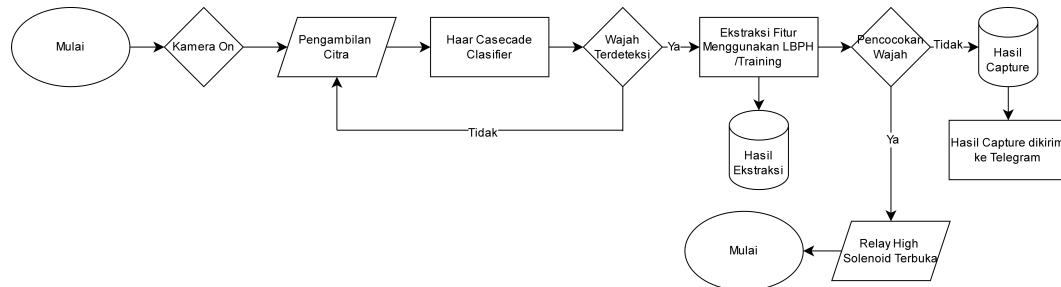
Gambar 2. Ekstraksi Fitur Tekstur Citra

3. Perancangan Sistem

Penelitian ini menggunakan bahasa pemrograman *Python* dan aplikasi *Telegram* yang dioperasikan melalui *smartphone*. Tahapan awal dimulai dengan pengambilan citra wajah yang akan digunakan sebagai data pelatihan. Setelah itu, dilakukan proses pelatihan (*training*) dengan mengekstraksi fitur-fitur utama dari citra wajah tersebut menggunakan algoritma pengenalan wajah, lalu menyimpannya dalam database sebagai data referensi.

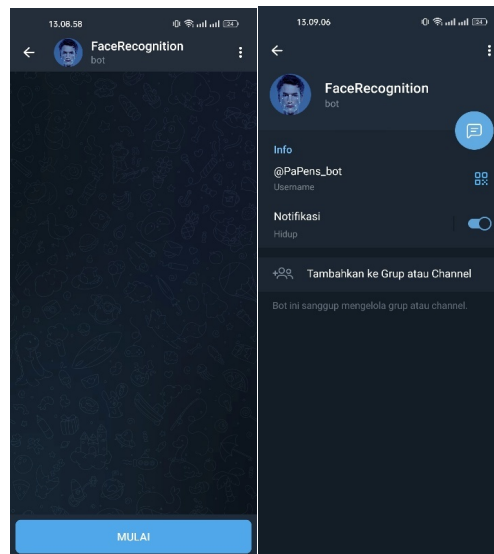
Setelah perangkat diaktifkan, sistem secara *real-time* akan melakukan pendeteksian wajah menggunakan kamera. Jika wajah terdeteksi, sistem akan menangkap citra wajah tersebut, mengekstraksi fitur-fiturnya, dan mencocokkannya dengan data yang tersimpan di *database*. Jika terdapat kecocokan,

Raspberry Pi akan mengaktifkan *relay* untuk mengalirkan arus ke *solenoid* yang digunakan mekanisme pembuka kunci pintu. Sebaliknya, jika citra wajah yang diproses tidak cocok dengan data dalam database, *Raspberry Pi* akan mengirimkan notifikasi kepada pemilik rumah melalui aplikasi *Telegram*, disertai dengan gambar wajah yang terdeteksi tidak dikenali. Diagram alur dari keseluruhan sistem yang diusulkan ditampilkan pada Gambar 3.



Gambar 3. Diagram Alir Sistem

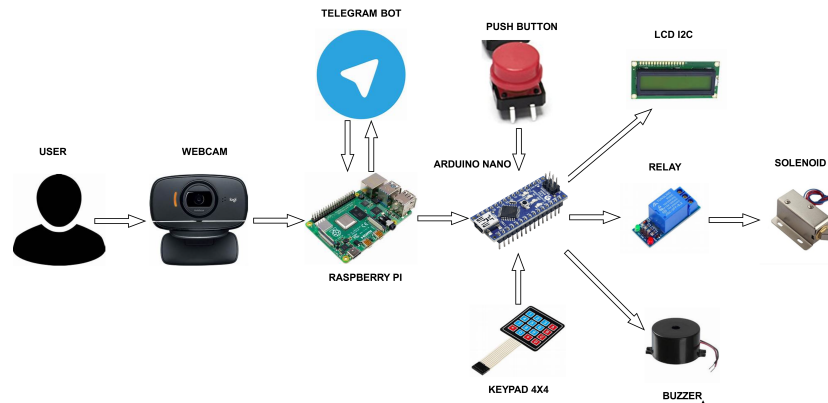
Aplikasi yang digunakan dalam sistem ini yaitu dengan menggunakan *Telegram bot*. *Telegram bot* yang dirancang berfungsi untuk memonitoring wajah yang tidak dikenali yang kemudian system otomatis mengcapture dan akan dikirim ke *Telegram bot*, serta bisa digunakan sebagai input untuk membuka kunci pintu berbasis IoT. Desain tampilan *Telegram bot* yang dirancang sebagai berikut:



Gambar 4. Tampilan *Telegram bot*

4. Perancangan Perangkat Keras

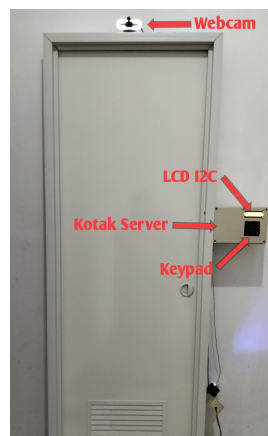
Perancangan perangkat keras meliputi proses konfigurasi sistem, prototipe, mekanik. Dalam tahapan ini akan disajikan dalam blok diagram keseluruhan sistem ditujukan dalam Gambar 5.



Gambar 5. Konfigurasi Hardware

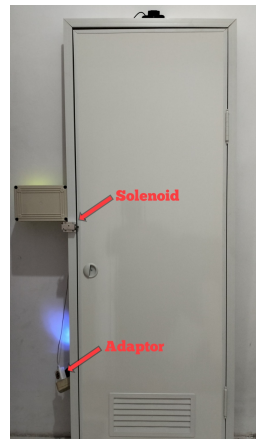
Gambar 5 menunjukkan konfigurasi hardware dari alat yang dirancang, yang mengintegrasikan berbagai komponen dan konsep input utama untuk mendukung fungsionalitas sistem. Konfigurasi ini mencakup empat sumber input utama, yaitu kamera, *Telegram bot*, tombol, dan *keypad*, yang masing-masing diproses oleh *Raspberry Pi*, *Arduino Nano* untuk mengontrol *solenoid* sebagai sistem penguncian. Sistem ini dirancang agar fleksibel, aman, dan mampu memberikan notifikasi serta informasi status melalui *Liquid Crystal Display (LCD)* modul antarmuka *Inter-Integrated Circuit (I2C)* dan *Telegram bot*.

Selanjutnya, desain prototipe alat dirancang untuk mengimplementasikan konfigurasi hardware tersebut dalam dua bagian, yaitu bagian luar dan bagian dalam ruangan.



Gambar 6. Prototipe Bagian Luar

Gambar 6 menampilkan desain prototipe bagian luar, yang mencakup dua sistem input: *Webcam* untuk pengenalan wajah dan *keypad 4x4* untuk pembukaan pintu menggunakan password. Selain itu, LCD-I2C ditempatkan untuk menampilkan indikator status sistem serta tombol yang ditekan pada *keypad*.



Gambar 7. Prototipe Bagian Dalam

Gambar 7 menampilkan desain prototipe bagian dalam ruangan. Pada bagian ini terdapat satu sistem input berupa *Push Button* yang memungkinkan pembukaan pintu dari dalam, serta satu sistem output berupa *Solenoid Door Lock* yang berfungsi sebagai mekanisme penguncian pintu. Desain prototipe ini memastikan bahwa seluruh komponen hardware dapat bekerja secara terintegrasi dan mendukung fungsi keamanan yang dirancang.

C. Hasil dan Pembahasan

1. Dataset

Data citra wajah didapatkan Ketika proses *capture* yang diambil dari *webcam* secara *real-time* selama 15 kali penangkapan citra wajah sampai proses berakhir. Pengambilan data citra wajah diambil dengan posisi wajah menghadap lurus kedepan kamera agar mendapatkan tangkapan wajah secara maksimal. Berikut ini adalah *dataset* yang akan dilakukan proses *training*.

Tabel 1. Dataset

Nama	Dataset
Anonim R	
Anonim S	
Anonim U	
Anonim A	

Anonim K



2. Pengujian Jarak pendeteksian Wajah

Pengujian ini bertujuan untuk mengetahui kemampuan sistem dalam mendeteksi wajah manusia dengan membuat kotak pada wajah yang terdeteksi serta jarak deteksi.

Tabel 2. Pengujian Jarak Pendeteksian Wajah

Nama	Jarak Pengukuran (cm)	Persentase Error
Anonim R	60	Terdeteksi
	120	Terdeteksi
	180	Terdeteksi
	240	Terdeteksi
	300	Terdeteksi
	360	Terdeteksi Tidak Stabil
	420	Terdeteksi Tidak Stabil
	480	Tidak Terdeteksi
	60	Terdeteksi
Anonim A	120	Terdeteksi
	180	Terdeteksi
	240	Terdeteksi
	300	Terdeteksi
	360	Terdeteksi Tidak Stabil
	420	Terdeteksi Tidak Stabil
	480	Tidak Terdeteksi
	60	Terdeteksi
	120	Terdeteksi
Anonim K	180	Terdeteksi
	240	Terdeteksi
	300	Terdeteksi
	360	Terdeteksi Tidak Stabil
	420	Terdeteksi Tidak Stabil
	480	Tidak Terdeteksi
	60	Terdeteksi
	120	Terdeteksi
	180	Terdeteksi
Anonim U	240	Terdeteksi
	300	Terdeteksi
	360	Terdeteksi Tidak Stabil
	420	Terdeteksi Tidak Stabil
	480	Tidak Terdeteksi
	60	Terdeteksi
	120	Terdeteksi
	180	Terdeteksi
	240	Terdeteksi
Anonim S	300	Terdeteksi
	360	Terdeteksi Tidak Stabil
Anonim S	420	Terdeteksi Tidak Stabil
	480	Tidak Terdeteksi
Anonim S	60	Terdeteksi
	120	Terdeteksi

180	Terdeteksi
240	Terdeteksi
300	Terdeteksi
360	Terdeteksi Tidak Stabil
420	Terdeteksi Tidak Stabil
480	Tidak Terdeteksi

Berdasarkan hasil pengujian jarak pendeteksian wajah terhadap lima wajah yang berbeda, sistem menunjukkan performa deteksi yang optimal pada rentang jarak antara 60 cm hingga 300 cm. Pada rentang ini, wajah dapat terdeteksi dengan baik dan stabil oleh sistem. Namun, ketika jarak mencapai 360 cm, sistem mulai mendeteksi wajah secara tidak stabil, yang mengindikasikan bahwa sistem mulai kehilangan akurasi dan konsistensi dalam mendeteksi wajah. Sementara itu, pada jarak 420 cm hingga 480 cm, sistem tidak dapat mendeteksi wajah, menunjukkan bahwa performa sistem menurun drastis pada jarak yang lebih jauh. Kemampuan sistem dalam mendeteksi wajah sangat dipengaruhi oleh jarak antara kamera dengan objek wajah, dengan jarak optimal ≤ 300 cm untuk hasil deteksi yang maksimal.

3. Pengujian Pengenalan Wajah

Berdasarkan hasil pelatihan dan pengujian yang telah dilakukan untuk mengetahui tingkat akurasi kinerja sistem keseluruhan berdasarkan sampel data uji, maka dilakukan pendekatan statistik yang berhubungan dengan efektivitas sistem dengan melakukan perbandingan variabel pengujian yang dapat dilihat pada Gambar 5 sebagai berikut:

A k t u a l	Anonim R	9	0	1	0	0	0	0	0	0	0	10
	Anonim S	0	10	0	0	0	0	0	0	0	0	9
	Anonim U	4	0	6	0	0	0	0	0	0	0	8
	Anonim A	1	0	0	8	1	0	0	0	0	0	7
	Anonim K	1	0	0	2	7	0	0	0	0	0	6
	Anonim T	0	0	0	0	0	8	2	0	0	0	5
	Anonim N	0	0	0	0	0	0	9	0	0	0	4
	Anonim Av	0	0	0	0	0	1	1	8	0	0	3
	Anonim Y	0	0	0	0	0	0	2	0	8	0	2
	Anonim Ar	2	0	0	0	0	0	0	0	0	6	1
		AnonimR	AnonimS	AnonimU	AnonimA	AnonimK	AnonimT	AnonimN	AnonimAv	AnonimY	AnonimAr	0

Gambar 8. Pengukuran Performa Pengenalan Wajah

Berdasarkan Gambar 8 setelah dilakukan sebanyak 10 kali pengujian pada 10 sampel data maka akan dihitung nilai *accuracy*, *precision*, *recall*, dan *F1-score* dengan perhitungan sebagai berikut:

a. Perhitungan nilai accuracy

$$\begin{aligned}
 Accuracy &= \frac{TP+TN}{(TP+TN+FP+FN)} \times 100\% \\
 &= \frac{79+0}{(79+0+18+3)} \times 100\% \\
 &= \frac{79}{100} \times 100\% = 79\%
 \end{aligned}
 \tag{2}$$

b. Perhitungan nilai precision

$$\begin{aligned}
 Precision &= \frac{TP}{(TP+FP)} \times 100\% \\
 &= \frac{79}{(79+18)} \times 100\% \\
 &= \frac{79}{97} \times 100\% = 81,4\%
 \end{aligned}
 \tag{3}$$

c. Perhitungan nilai recall

$$\begin{aligned}
 Recall &= \frac{TP}{(TP+FN)} \times 100\% \\
 &= \frac{79}{(79+3)} \times 100\% \\
 &= \frac{79}{82} \times 100\% = 96,3\%
 \end{aligned}
 \tag{4}$$

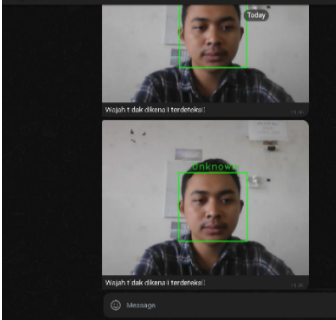
d. Perhitungan nilai F1-score

$$\begin{aligned}
 F1 - score &= 2 \times \frac{(Precision \times Recall)}{Precision + Recall} \\
 &= 2 \times \frac{(81,4 \times 96,3)}{81,4 + 96,3} \\
 &= 2 \times \frac{7838,82}{177,7} = 88,2\%
 \end{aligned}
 \tag{5}$$

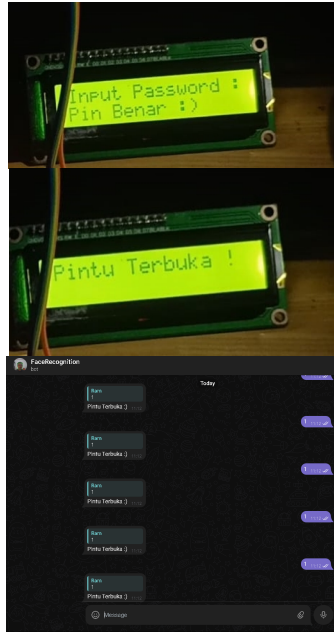
4. Pengujian Integrasi Sistem Keseluruhan

Pengujian ini bertujuan untuk mengetahui kemampuan sistem IoT dalam mengirim pesan ke hardware guna untuk membuka kunci pintu dan menerima pesan ketika wajah yang tidak dikenali terdeteksi.

Tabel 3. Pengujian Integrasi Sistem Keseluruhan

Pengujian	Gambar Hasil Uji	Keterangan
Wajah dikenali		Wajah dikenali oleh sistem, kemudian <i>solenoid door lock</i> terbuka secara otomatis.
Wajah tidak dikenali		Wajah tidak terdaftar terdeteksi, sistem secara otomatis menangkap gambar dan mengirimkan notifikasi melalui <i>Telegram bot</i> .

PIN
menggunakan
keypad



Mengirim
Pesan "1" via
Telegram bot

Pengguna memasukkan
PIN '123' yang telah
diatur sebelumnya,
sistem memberikan akses
dan pintu terbuka.

Sistem menerima
perintah dari *Telegram*
bot dan membuka pintu
secara otomatis

Berdasarkan hasil pengujian integrasi sistem secara menyeluruh menunjukkan bahwa sistem kunci pintu berhasil menjalankan seluruh fitur utama dengan baik, mulai dari pengenalan wajah, penggunaan PIN, hingga kontrol melalui *Telegram bot*. Ketika wajah yang terdaftar dikenali, *solenoid door lock* terbuka secara otomatis, menandakan bahwa proses deteksi dan pencocokan wajah berjalan akurat dan *real-time*. Jika wajah tidak dikenali, sistem otomatis mengambil gambar dan mengirimkannya ke *Telegram bot* sebagai pemberitahuan kepada pengguna dengan pesan "Wajah tidak dikenali terdeteksi!". Penggunaan PIN juga berfungsi dengan baik, memberikan akses saat PIN benar dimasukkan melalui *keypad*. Selain itu, perintah "1" yang dikirim melalui *Telegram bot* juga diterima dan menghasilkan respon "Pintu Terbuka ", yang menunjukkan bahwa sistem berhasil menerima dan memproses perintah untuk membuka pintu dengan benar. Keberhasilan sistem dalam menjalankan seluruh integrasi perangkat keras dan perangkat lunak berjalan optimal.

D. Kesimpulan

Sistem pengenalan wajah yang dikembangkan dengan metode *Local Binary Pattern Histogram (LBPH)* menunjukkan performa yang sangat baik. Sistem berhasil mencapai tingkat akurasi sebesar 79%, *precision* sebesar 81,4%, *recall* sebesar 96,3%, dan *F1-score* sebesar 88,2%. Nilai *F1-score* ini mengindikasikan keseimbangan yang cukup optimal antara kemampuan sistem dalam mengenali wajah yang benar (*precision*) dan mendeteksi seluruh wajah yang relevan (*recall*), meskipun masih terdapat potensi peningkatan akurasi secara keseluruhan. Selain itu, sistem menunjukkan kinerja deteksi yang stabil pada jarak antara 60 cm hingga 300 cm, yang menandakan bahwa kemampuan sistem mampu beroperasi secara efektif dalam rentang jarak tersebut.

E. Referensi

- [1] D. Sudiantini, A. Naiwasha, A. Izzati, A. A. W., B. P. A., and C. Rindiani, "Penggunaan Teknologi Pada Manajemen Sumber Daya Manusia Di Dalam Era Digital Sekarang," *Digital Business: Jurnal Publikasi Ilmu Manajemen dan E-Commerce*, vol. 2, no. 2, pp. 262–269, May 2023, doi: 10.30640/digital.v2i2.1082.
- [2] C. A. Cholik, "Perkembangan Teknologi Informasi Komunikasi (ICT) Dalam Berbagai Bidang," *Jurnal Fakultas Teknik UNISA Kuningan*, vol. 2, no. 2, pp. 39–46, 2021.
- [3] T. G. Laksana and S. Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *Jurnal Ilmiah Multidisiplin*, vol. 3, no. 01, Art. no. 01, Jan. 2024, doi: 10.56127/jukim.v3i01.1143.
- [4] "Rancang Bangun Sistem Kunci Pintu Digital Berbasis Arduino Mega 2560," *Widyakala Journal: Journal of Pembangunan Jaya University*. Accessed: Jan. 10, 2025. [Online]. Available: http://www.ojs.upj.ac.id/index.php/journal_widya/article/view/83
- [5] M. Ansori, "Sistem Keamanan Pintu Rumah Menggunakan Kamera ESP32 Berbasis Website," bachelor thesis, Universitas Nasional, 2023. Accessed: Jan. 10, 2025. [Online]. Available: <http://repository.unas.ac.id/11361/>
- [6] R. Dwi Cahyo Putro, "Sistem Implementasi Keamanan Pintu Rumah Menggunakan Face Lock Secara Visual Berbasis Internet of Things (IoT)," diploma thesis, Politeknik Negeri Jember, 2023. Accessed: Jan. 15, 2025. [Online]. Available: <https://sipora.polije.ac.id/25356/>
- [7] S. Sunardi, A. Yudhana, and M. A. Talib, "Perancangan Sistem Pengenalan Wajah Untuk Keamanan Ruangan Menggunakan Metode Local Binary Pattern Histogram," *Jurnal Teknologi Elektro*, vol. 13, no. 2, p. 123, Jun. 2022, doi: 10.22441/jte.2022.v13i2.010.
- [8] P. Kenda, "Sistem Presensi Berbasis Wajah Dengan Metode Haar Cascade," *Konstelasi: Konvergensi Teknologi dan Sistem Informasi*, vol. 1, no. 2, Art. no. 2, Apr. 2021, doi: 10.24002/konstelasi.v1i2.4305.
- [9] B. Santoso and R. P. Kristianto, "Implementasi Penggunaan OpenCV Pada Face Recognition Untuk Sistem Presensi Perkuliahan Mahasiswa," *Sistemasi: Jurnal Sistem Informasi*, vol. 9, no. 2, Art. no. 2, May 2020, doi: 10.32520/stmsi.v9i2.822.
- [10] F. Utami, S. Suhendri, and M. A. Mujib, "Implementasi Algoritma Haar Cascade Pada Aplikasi Pengenalan Wajah Personel," *Journal of Information Technology*, vol. 3, no. 1, pp. 33–38, Mar. 2021, doi: 10.47292/joint.v3i1.45.
- [11] A. Suryansah, R. Habibi, and R. M. Awangga, *Penggunaan Face Recognition Untuk Akses Ruangan. Kreatif*, 2020.
- [12] Arnita, F. Marpaung, F. Aulia, and R. C. Nabila, *Computer Vision dan Pengolahan Citra Digital*. Surabaya: Pustaka Aksara, 2022. Accessed: Jun. 11, 2025. [Online]. Available: <https://digilib.unimed.ac.id/id/eprint/53012/>
- [13] H. Fitriyah and R. C. Wihandika, *Dasar-Dasar Pengolahan Citra Digital*. Universitas Brawijaya Press, 2021.
- [14] A. M. Muchtamar, "Sistem Deteksi Pelat Nomor Kendaraan Roda Dua Berdasarkan Variabel Kecepatan," other thesis, Universitas Hasanuddin, 2021.

Accessed: Jun. 11, 2025. [Online]. Available:
<https://repository.unhas.ac.id/id/eprint/18212/>

- [15] A. H. Muhammad, G. Mandar, and R. Irwan, "Pengembangan Teknologi Pengenalan Wajah Pada Sistem Tiket Kapal Sebagai Solusi Optimal Untuk Mengurangi Antrian Boarding Pass," *Indonesian Journal of Information Systems (IJIS)*, vol. 9, no. 2, Art. no. 2, Sep. 2024, doi: 10.36549/ijis.v9i2.346.
- [16] I. A. Tarigan and A. Kurniawan, "Prototipe Pendeteksi dan Pengenalan Wajah Berbasis Web Menggunakan Algoritma Local Binary Pattern Histogram Untuk Absensi," *Multinetics*, vol. 8, no. 1, Art. no. 1, Nov. 2022, doi: 10.32722/multinetics.v8i1.4591.