Volume 8 Nomor 1 Januari 2026 JJEEE e-ISSN : 2715-0887
p-ISSN : 2654-7813

*Jambura Journal of Electrical and Electronics Engineering*

# Sistem Keamanan Pintu Rumah Berbasis *Liveness Detection* untuk *Anti-Spoofing* Menggunakan Kamera Intel RealSense F455 dan LBPH

## *Liveness Detection-Based Home Door Security System for Anti-Spoofing Using Intel RealSense F455 Camera and LBPH*

Adi Kurniawan Saputro
Program Studi Teknik Elektro
Universitas Trunojoyo Madura
Bangkalan, Indonesia
adi.kurniawan@trunojoyo.ac.id

Hamzah Arifianto Diputra
Program Studi Teknik Elektro
Univeritas Trunojoyo Madura
Bangkalan, Indonesia
210431100004@student.trunojoyo.ac.id

Achmad Fiqhi Ibadillah
Program Studi Teknik Elektro
Univeritas Trunojoyo Madura
Bangkalan, Indonesia
fiqhi.ibadillah@trunojoyo.ac.id

Achmad Ubaidillah
Program Studi Teknik Elektro
Universitas Trunojoyo Madura
Bangkalan, Indonesia
ubaidillah.ms@trunojoyo.ac.id

Deni Tri Laksono
Program Studi Teknik Elektro
Universitas Trunojoyo Madura
Bangkalan, Indonesia
deni.laksono@trunojoyo.ac.id

Achmad Zain Nur
Program Studi Teknik Elektro
Universitas Trunojoyo Madura
Bangkalan, Indonesia
azain.nur@trunojoyo.ac.id

Diterima : Oktober 2025
Disetujui : Januari 2026
Dipublikasi : Januari 2026

***Abstrak*— Serangan *spoofing* pada sistem keamanan berbasis pengenalan wajah semakin meningkat seiring dengan berkembangnya teknologi rumah cerdas. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan sistem keamanan pintu rumah dengan penerapan teknologi *anti-spoofing* berbasis *liveness detection* menggunakan kamera Intel RealSense F455. Sistem dirancang untuk memverifikasi keaslian wajah pengguna secara real-time dengan mengombinasikan analisis tekstur wajah dan respons fisiologis pengguna. Proses deteksi wajah dilakukan menggunakan algoritma Haarcascade untuk mengekstraksi area wajah berukuran 160×160 piksel, sedangkan pengenalan wajah menggunakan metode Local Binary Pattern Histogram (LBPH) yang relatif stabil terhadap variasi pencahayaan dan sudut pandang. Mekanisme liveness detection diterapkan secara mekanis dengan memanfaatkan *Haarcascade* Eye untuk mendeteksi pergerakan mata pengguna sebagai indikator kehadiran wajah hidup, sehingga sistem mampu membedakan wajah asli dari media palsu berupa foto statis. Sistem terintegrasi dengan bot Telegram untuk pemantauan akses secara *real-time*, di mana notifikasi otomatis dikirim setiap kali terjadi percobaan akses pintu. Hasil pengujian menunjukkan tingkat akurasi pengenalan wajah mencapai 98,93%, dengan sistem berhasil mendeteksi dan memverifikasi 30 pengguna terdaftar serta menghasilkan nilai *confidence* rata-rata yang konsisten di atas 80% dari batas ambang sistem 60 %. Selain itu, mekanisme *liveness detection* terbukti efektif dalam mencegah serangan spoofing berbasis foto dengan tingkat keberhasilan deteksi yang stabil selama pengujian. Temuan ini menunjukkan bahwa integrasi LBPH dan *eye-based liveness detection* dapat meningkatkan keandalan sistem keamanan pintu berbasis pengenalan wajah.**

**Kata kunci — Pengenalan wajah; *Liveness Detection*; LBPH; *Haarcascade*; Intel RealSense F455.**

***Abstract*— Spoofing attacks on facial recognition-based security systems are increasing along with the development of smart home technology. To address this issue, this study proposes a home door security system with the implementation of liveness detection-based anti-spoofing technology using an Intel RealSense F455 camera. The system is designed to verify the authenticity of a user's face in real-time by combining facial texture analysis and the user's physiological responses. The facial detection process is carried out using the Haarcascade algorithm to extract a 160×160 pixel facial area, while facial recognition uses the Local Binary Pattern Histogram (LBPH) method which is relatively stable to variations in lighting and viewing angles. The liveness detection mechanism is implemented mechanically by utilizing the Haarcascade Eye to detect the user's eye movements as an indicator of the presence of a live face, so that the system is able to distinguish real faces from fake media in the form of static photos. The system is integrated with a Telegram bot for real-time access monitoring, where automatic notifications are sent every time a door access attempt occurs. Test results show a facial recognition accuracy rate of 98.93%, with the system successfully detecting and verifying 30 registered users and producing an average confidence value consistently above 80%. Furthermore, the liveness detection mechanism proved effective in preventing photo-based spoofing attacks, with a stable detection success rate throughout the testing. These findings suggest that the integration***

***of LBPH and eye-based liveness detection can improve the reliability of facial recognition-based door security systems.***

***Keywords— Face recognition; Liveness Detection; LBPH; Haarcascade; Intel RealSense F455.***

## I. PENDAHULUAN

Perkembangan teknologi keamanan mengalami percepatan signifikan seiring dengan meningkatnya kebutuhan masyarakat akan proteksi properti pribadi maupun publik. Urgensi ini didukung oleh data Badan Pusat Statistik (BPS) Indonesia yang mencatat tren peningkatan kriminalitas, dari 22,19% pada tahun 2019 menjadi 23,46% pada tahun 2020, di mana kasus pencurian mendominasi sekitar 36-45% dari total kejahatan [1]. Statistik ini mengindikasikan bahwa metode keamanan konvensional, seperti kunci mekanik atau kartu akses, memiliki kerentanan tinggi dan tidak lagi memadai. Metode tradisional tersebut mudah dipelajari, digandakan, atau dimanipulasi oleh pihak tidak berwenang. Sebagai alternatif, teknologi biometrik pengenalan wajah (*face recognition*) semakin banyak diadopsi karena karakteristik unik setiap individu dan kenyamanan penggunaannya [2], [3]. Namun, sistem pengenalan wajah standar memiliki kelemahan fatal, yakni kerentanan terhadap serangan *spoofing* di mana foto, video, atau topeng dapat digunakan untuk mengecoh sistem jika tidak dilengkapi mekanisme verifikasi yang kuat [4], [5], [6].

Untuk merespons tantangan tersebut, berbagai penelitian dalam lima tahun terakhir telah mengeksplorasi kombinasi algoritma *Haar Cascade* untuk deteksi wajah dan *Local Binary Pattern Histogram* (LBPH) untuk pengenalan wajah. Penelitian "Human Face Identification Using Haar Cascade Classifier and LBPH Based on Lighting Intensity" menunjukkan bahwa metode ini mampu memberikan akurasi yang baik dalam variasi kondisi pencahayaan (terang, normal, gelap) [7]. Studi lain mengenai efisiensi memori pada robot resepsionis juga membuktikan bahwa LBPH efektif diterapkan pada perangkat dengan sumber daya terbatas melalui optimasi *preprocessing* [8]. Secara umum, literatur menujukkan bahwa kombinasi *Haarcascade* dan LBPH sangat responsif dan layak untuk implementasi *real-time* [9] , [10][11], [12].

Mayoritas studi sebelumnya hanya berfokus pada akurasi pencocokan identitas (*face matching*) tanpa mengintegrasikan mekanisme *liveness detection* secara *real-time*. Akibatnya, sistem yang dihasilkan memang akurat dalam mengenali "siapa" subjeknya, namun gagal memverifikasi "keaslian" fisik subjek tersebut, sehingga rentan dibobol menggunakan media cetak atau digital (anti-spoofing). Selain itu, belum banyak studi yang menggabungkan algoritma pengenalan wajah yang ringan ini dengan sistem monitoring aktif berbasis *Internet of Things* (IoT) dalam satu kesatuan sistem keamanan rumah.

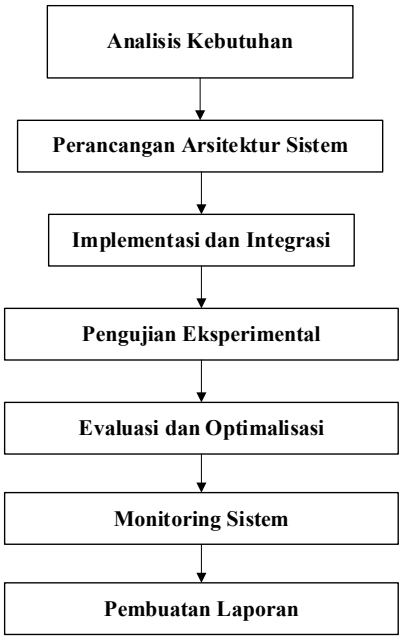
Penelitian ini bertujuan mengisi celah tersebut dengan mengusulkan sistem keamanan pintu rumah yang mengintegrasikan metode LBPH dan *Haarcascade* dengan fitur *Liveness Detection.* Kebaruan (*novelty*) utama dalam penelitian ini dibandingkan studi sebelumnya adalah penerapan analisis perilaku wajah seperti deteksi kedipan mata dan mikro-ekspresi sebagai syarat mutlak otorisasi akses [6]. Alur sistem dirancang mulai dari deteksi wajah, *cropping* citra (160×160 piksel), ekstraksi fitur LBPH, hingga validasi *liveness* untuk memastikan subjek adalah manusia hidup. Penggunaan kamera Intel RealSense F455 dipilih untuk menjamin kualitas akuisisi data visual yang presisi [13][14].

Sebagai nilai tambah, penelitian ini mengintegrasikan bot Telegram untuk monitoring real-time, yang memberikan notifikasi instan saat akses berhasil maupun saat terdeteksi aktivitas mencurigakan. Penggunaan kamera Intel RealSense F455 sebagai penangkap citra diharapkan memberikan kualitas input yang superior untuk proses verifikasi. Dengan penggabungan LBPH, liveness detection, dan monitoring Telegram, sistem ini diharapkan menjadi solusi keamanan yang lebih komprehensif, cerdas, dan tahan terhadap berbagai teknik pemalsuan identitas Integrasi yang menambah lapisan keamanan dan kenyamanan bagi pengguna rumah, berbeda dari banyak sistem sebelumnya yang hanya fokus pada pengenalan wajah tanpa monitoring akses secara aktif.

## II. METODE

### A. Perancangan Sistem

Penelitian ini menerapkan pendekatan eksperimental dalam perancangan sistem keamanan pintu akses biometrik yang mengintegrasikan teknologi liveness detection untuk mencegah serangan *spoofing*. Sistem ini memanfaatkan Kamera *Intel RealSense* F455 sebagai sensor utama untuk menangkap data RGB serta mengimplementasikan algoritma LBPH (*Local Binary Pattern Histogram*) yang ditingkatkan untuk pengenalan wajah. Tahapan penelitian dilakukan secara sistematis melalui eksperimen bertahap dimulai dari analisis kebutuhan keamanan, perancangan arsitektur hardware dan *software*, implementasi sistem terintegrasi, hingga evaluasi performa terhadap berbagai skenario serangan spoofing. Sistem dirancang untuk memberikan autentikasi multi-faktor yang menggabungkan pengenalan wajah dengan verifikasi keaslian wajah secara *real-time*. Tahapan dari perancangan sistem dalam penelitian ini dapat dilihat pada Gambar 1.

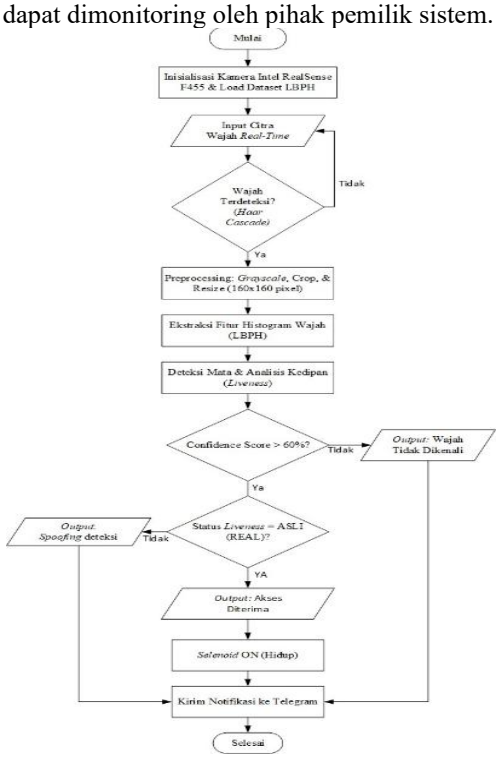



Gambar 1. Perancangan Sistem

*B. Studi Literatur dan Analisa Kebutuhan Alat Bahan*

Tahapan awal dari penelitian ini yaitu melakukan studi literatur terhadap sistem yang relevan, seperti sistem pengenalan wajah (khususnya *Haar Cascade*), fitur anti spoofing dengan *Liveness Detection,* pembentukan arsitektur wajah serta monitoring secara real time pada sistem. Analisa kebutuhan alat dan bahan yang digunakan terdiri dari perangkat keras dan perangkat lunak yaitu laptop, handphone android, aplikasi telegram, software phyton, prototipe rumah , *solenoid doorlock* 12v, relay 5v, Arduino nano, software Arduino IDE, intel realsense f455, p*ower supply* 12v sedangkan bahan yang digunakan adalah dataset wajah yang terdiri dari 30 data user sebagai database awal yang sudah didaftarkan dimana data yang didaftarkan terdiri dari data username, nim, dan umur user. Teknik ini menggunakan video user dengan bebrapa ekspresi dan gerak yang berbeda yang nantinya akan di ekstrak menjadi gambar dan di oleh oleh Haar cascade untuk crop wajah 160 x 160 piksel agar wajah lebih presisi sebelum diolah arsitektur wajahnya dengan metode *Local Binary Pattern Histogram* (LBPH).

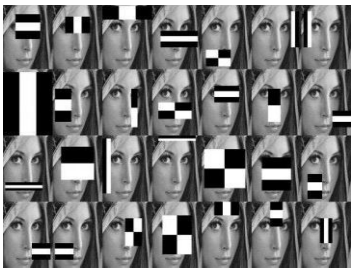
Dilihat pada gambar 2 terdapat flowchart sistem dimana proses sistem melalui segmen pendaftran pada sistem dengan output mp4 juga melalui beberapa proses pengolahan mulai dari crop deteksi wajah *Haar Cascade*, pembentukan Arsitektur wajah dengan *Local Binary Pattern Histogram* (LBPH) serta pencocokan atau verifikasi wajah user pada sistem dengan output bounding box label data user meliputi nama, umur, nim, label *Liveness* keaslian user dengan label real/ *spoofing* dan nilai *confidence score* yang menujukkan kepercayaan sistem terhadap hasil wajah yang terdeteksi pada sistem, dimana jika nilai *confidence* >60% maka sistem menerima user dan mengaktifkan saklar relay untuk membuka *solenoid doorlock* yang difungsikan khusus sebagai pengunci pintu elektronik dengan masukan tegangan 12v [15], [16]. Setelah user tereteksi maka sistem akan mengirimkan informasi kepada bot telegram secara *real-time* agar dapat dimonitoring oleh pihak pemilik sistem.




Gambar 3. Flowchart proses

*C. Haar Cascade*

*Haar Cascade* merupakan algoritma deteksi objek berbasis *machine learning* yang menggunakan fitur *Haar-like* untuk mengenali pola perbedaan intensitas antar piksel pada area persegi citra. Algoritma ini menghitung jumlah nilai piksel secara efisien melalui *integral image*, yang mempercepat proses perhitungan fitur. Selanjutnya, sistem menggunakan *cascade classifier* bertingkat, di mana setiap tahap menyaring area citra dan memutuskan apakah kumpulan piksel tersebut mengandung objek yang dicari [16]. Pendekatan ini membuat proses deteksi menjadi lebih cepat, efisien, dan akurat dalam mengenali objek tertentu pada gambar.



Gambar 3. Implementasi *Haar like feature*

Gambar wajah dikelompokkan seperti pada gambar 3 pada *Haar like feature* berdasarkan sisi terang dan gelap. Misalnya, area mata terlihat lebih gelap dibandingkan area sekitarnya [17]. Setelah mendeteksi wajah baru melakukan crop sesuai standart sistem 160 x 160 piksel dengan berbentuk persegi. Berikut rumus menghitung nilai individu dari karakteristik *haar like feature* :

$$F(Hear) = \sum Fputih - \sum Fhitam$$

$$F(Hear) = \frac{1}{n}\sum_{hitam}^{n} 1(x) - \frac{1}{n}\sum_{putih}^{n} 1\,(x) \qquad (1)$$

Keterangan :

*F* (Hear) : Nilai fitur keseluruhan

∑ Fputih : Nilai fitur terang

∑ Fhitam : Nilai fitur gelap

N : Jumlah piksel

I(x) : Nilai sebenarnya yang terdeteksi pada citra.

$$FD_{eye}(t) = \begin{cases} 1, \text{jika fitur mata terdeteksi(terbuka)} \\ 0, \text{jika fitur mata tidak terdeteksi(tertutup)} \end{cases} \qquad (2)$$

Adapun poses deteksi *Liveness* dengan menggunakan hasil dari rumus Harcascade eye dimana menerapkan deteksi kedipan mata (eye blink detection) menggunakan algoritma Haar Cascade Classifier. Pendekatan ini memanfaatkan karakteristik biner dari algoritma Haar Cascade, di mana mata yang sedang berkedip (tertutup) akan dianggap sebagai hilangnya objek (loss of target) sementara wajah tetap terdeteksi. Secara matematis, status deteksi mata pada waktu t dinotasikan sebagai fungsi biner $D_{eye}\,(t)$, seperti ditunjukkan pada Persamaan (1):

$$Liveness = \begin{cases} Valid, \text{jika } \mathrm{Th}_{min} \le \sum_{i=1}^{n}(D_{eye}(t_i) = 0) \le \mathrm{Th}_{min} \\ Invalid\ , lainnya \end{cases} \qquad (3)$$

Dimana:

$t$ = merepresentasikan indeks waktu pengambilan *frame* (current frame).
n = adalah jumlah *frame* berturut-turut (*consecutive frames*) dimana mata tidak terdeteksi sementara wajah tetap terkunci.
$Th_{min}$ = adalah ambang batas bawah (ditetapkan sebesar 2 *frame*) untuk mengeliminasi *noise* atau kegagalan deteksi sesaat.
$Th_{max}$ = adalah ambang batas atas (ditetapkan sebesar 10 *frame*) untuk membedakan kedipan alami dengan aktivitas memejamkan mata atau tidur.

### D. *Local Binary Pattern Histogram (LBPH)*

*Local Binary Pattern Histogram* (LBPH) adalah sebuah kombinasi *Local Binary Pattern* (LBP) dengan *Histogram of Oriented Gradients* (HOG) [18]. LBPH bekerja dengan memecah citra wajah menjadi beberapa blok kecil, kemudian menghitung nilai biner berdasarkan intensitas piksel di sekitar piksel tengah dalam setiap blok tersebut. Hasil perhitungan biner ini dikonversi menjadi nilai desimal, yang digunakan untuk membentuk histogram. Untuk menghitung nilai Local Binary Pattern dari sebuah piksel f(x,y)f(x, y)f(x,y), rumusnya adalah sebagai berikut:

$$LBP(x, Y) = \sum_{i=0}^{P-1} 2^i . \delta(\mathcal{F}(X, Y), \mathcal{F}(X_i, Y_i)) \quad (4)$$

Keterangan:

P = Jumlah titik sampel disekitar piksel $\mathcal{F}(X, Y)$

$\mathcal{F}(X, Y)$ = Nilai piksel pusat

$\mathcal{F}(Xi, Yi)$ = Nilai piksel tetangga (di sekitar $\mathcal{F}(X, Y)$)

δ(a,b) = Fungsi yang menghasilkan 1 jika a ≥ b, dan 0 jika a< b.

*Local Binary Pattern Histogram* (LBPH) memiliki 4 parameter yaitu *Radius, Neigbors*, *Grid* x dan *Grid* y [18]. Parameter ini memungkinkan LBPH untuk menyesuaikan sensitivitas dan ketekitian pengenalan wajah, sehingga performa lebih optimal sesuai kebutuhan sistem. Dari hasil perhitungan LBP adapun rumus untuk perhitungan histogram LBP untuk seluruh citra, menggunakan rumus berikut :

$$H = \sum_{i=0}^{N} count\ (LBP_i) \quad (5)$$

Untuk membandingkan dua histogram, digunakan jarak Euclidean, yang dihitung dengan rumus berikut:

$$D = \sqrt{\sum_{i=1}^{n} (hist1_i - hist2_i)^2} \quad (6)$$

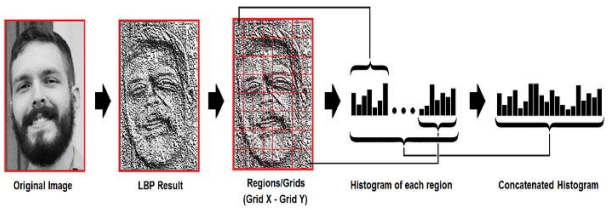
Keterangan:

*D* = Jarak antara dua *histogram*

$hist1_i$ = Nilai *histogram* pada bin ke$-i$ untuk *histogram* 1

$hist2_i$ = Nilai *histogram* pada bin ke$-i$ untuk *histogram* 2

*N* = Jumlah bin pada *histogram*



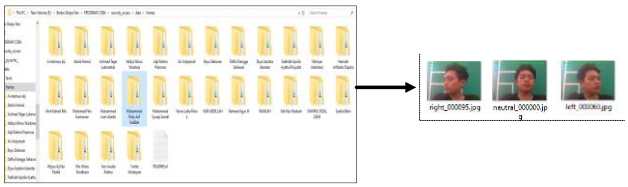

Gambar 5. *Local Binary Pattern Histogram* (LBPH)

### E. *Pengumpulan dan Persiapan Data*

Dataset Diperoleh dari pemgambilan record user yang sudah didaftarkan pada sistem, dataset berupa folder hasil record sistem, folder hasil ektrak gambar wajah dari video record video user, dan folder dataset gambar hasil crop *Haar Cascade* dengan ukuran 160 x 160 piksel dimana pada folder tiap user memiliki data gambar dengan ekspresi yang berbeda beda dan jarak berbeda beda.


Gambar 5. Dataset Folder raw video user

Pada Gambar 5 Merupakan folder yang berisi data user hasil record dari sistem, pada folder terdapat data dengan nama user yang berisi 3 video user dengan kondisi wajah netral (lurus), hadap kanan, hadap kiri.



Gambar 6. Dataset Folder hasil ekstrak foto wajah user

Pada Gambar 6 Merupakan folder yang berisi data user hasil ekstrak foto dari sistem, pada folder terdapat data dengan nama user yang berisi beberapa kondisi wajah user dengan kondisi wajah netral (lurus), hadap kanan, hadap kiri dalam bentuk gambar.

Gambar 7. Dataset Folder hasil crop *Haar Cascade* wajah user

Pada Gambar 7 Merupakan folder yang berisi data user hasil crop deteksi *haar cascade* dari sistem, pada folder terdapat data dengan nama user yang berisi beberapa kondisi wajah user yang masih terdeteksi dalam persegi 160 x 160 piksel.

### F. *Skema dan Tahapan Pengujian*

Terdapat pengujian software dan hardware bertujuan untuk mengetahui kinerja dari sistem serta bahan evaluasi untuk perbaikan dan pengembangan selanjutnya. Pengujian ini dilakukan melalui skenario *real-time*. Sistem diuji dengan

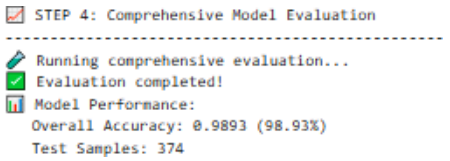
beberapa pareameter mulai dari fungsi *Liveness* menghindari pemalsuan objek, nilai confidence dari kecocokan wajah user, verifikasi terdeteksi user dengan data pendaftar, dan notikasi *realtime* Sistem diuji dengan beberapa parameter kunci, yaitu:

1. Uji Validasi User
   Pengujian validasi pengguna bertujuan memastikan sistem keamanan pintu mampu mengenali dan memverifikasi identitas pengguna terdaftar secara akurat dengan membandingkan data wajah real-time dan data hasil pelatihan pada basis data. Jika wajah sesuai, sistem membuka pintu dan menampilkan informasi nama, NIM, serta umur pada antarmuka GUI; sebaliknya, jika tidak sesuai atau tidak terdaftar, akses ditolak dengan pesan "user tidak dikenali". Pengujian ini digunakan untuk mengevaluasi kinerja autentikasi berbasis wajah dalam membedakan pengguna sah dan tidak dikenal.
2. Uji Akurasi *Confidence*
   Pengujian akurasi *confidence* bertujuan mengukur tingkat keyakinan sistem dalam mencocokkan wajah pengguna dengan data hasil pelatihan menggunakan metode LBPH. Nilai *confidence* dinormalisasi dalam bentuk persentase, di mana nilai yang lebih tinggi menunjukkan tingkat kecocokan yang lebih baik. Pengujian dilakukan dengan variasi pencahayaan dan ekspresi wajah untuk menilai kestabilan sistem. Hasil menunjukkan bahwa wajah dengan nilai *confidence* di atas ambang batas 60% dikenali dengan baik, sedangkan nilai di bawah batas tersebut dinyatakan tidak cocok, sehingga sistem terbukti mampu melakukan identifikasi wajah secara akurat dan konsisten sesuai parameter yang ditetapkan..
3. Uji *Monitoring* Telegram Bot
   Pengujian monitoring Telegram Bot bertujuan memastikan sistem keamanan pintu mampu mengirimkan notifikasi hasil deteksi wajah secara real-time melalui platform Telegram. Sistem mengintegrasikan bot Telegram sebagai sarana pemantauan jarak jauh yang secara otomatis mengirimkan informasi hasil pengenalan wajah, meliputi nama pengguna, umur, NIM, status *liveness*, dan nilai *confidence*. Pengujian dilakukan pada beberapa skenario deteksi untuk memverifikasi kesesuaian dan keserentakan informasi antara tampilan GUI dan pesan yang diterima admin melalui Telegram. Hasil pengujian menunjukkan bahwa notifikasi berhasil dikirim tanpa jeda waktu yang signifikan dengan data yang konsisten, sehingga membuktikan keandalan fitur monitoring Telegram bot dalam mendukung pengawasan dan keamanan sistem.
4. Uji Black Box
   Uji *black box* pada sistem keamanan pintu dilakukan untuk memastikan setiap menu. Pengujian mencakup empat menu utama, yaitu pendaftaran, *training*, deteksi, dan log. Pada menu *training*, pengujian dilakukan terhadap fitur *Training* semua pengguna, *Training* LBPH, ekstraksi citra dari video, *cropping* wajah menggunakan *Haar Cascade*, serta evaluasi model LBPH.Pengujian ini bertujuan memastikan sistem mampu melakukan prapemrosesan data wajah, dan menampilkan hasil evaluasi berupa tingkat akurasi serta status keberhasilan pelatihan.

## III. HASIL DAN PEMBAHASAN

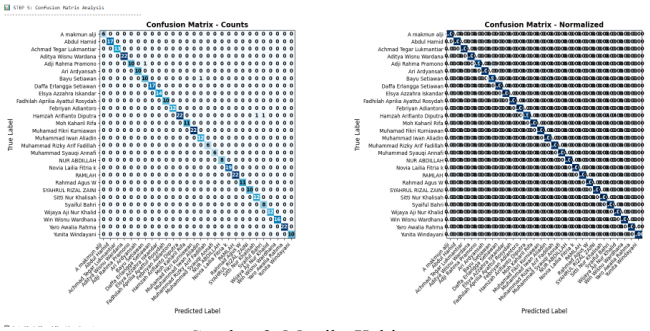
### A. *Hasil Traning Dataset*

Pada penelitian ini, evaluasi dilakukan menggunakan dataset yang bersumber dari proses perekaman wajah (face recording) secara langsung. Dataset mentah telah melalui tahapan preprocessing dan cropping otomatis menggunakan *Haar Cascade* untuk memastikan hanya Region of Interest (ROI) wajah yang digunakan. Total dataset berjumlah 1.866 citra dari 30 subjek (user), yang kemudian dipartisi dengan rasio 80:20, menghasilkan 1.492 data latih (training images) dan 374 data uji (testing images). Distribusi data per user bervariasi antara 27 hingga 119 citra untuk merepresentasikan variasi pose berbeda.



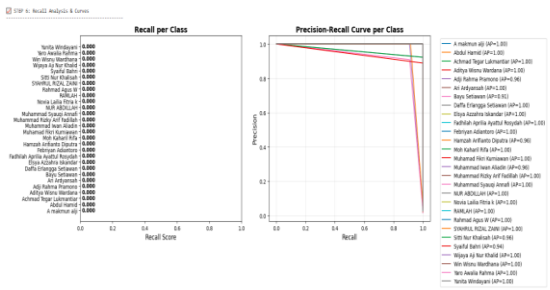

Gambar 8. Parameter Traning

Evaluasi komprehensif model pengenalan wajah yang dilatih menggunakan algoritma LBPH menunjukkan hasil kinerja yang sangat kuat. Model ini dikembangkan untuk mengklasifikasikan 30 pengguna dengan menggunakan sejumlah besar data pelatihan, yaitu 1492 Training Images, dan diuji menggunakan 374 Test Images. Kinerja keseluruhan mencapai Akurasi (*Overall Accuracy*) sebesar 0.9893 (98.93%), menegaskan kapabilitas model dalam tugas identifikasi yang akurat.



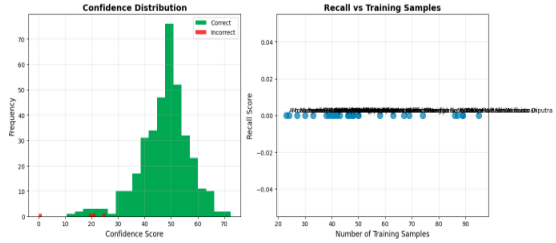

Gambar 9. Matriks Kebingungan

Matriks Kebingungan pada gambar 9 secara visual mengonfirmasi kinerja model yang dominan, ditandai dengan nilai diagonal yang mendekati 1.00 pada matriks yang dinormalisasi. Namun, Matriks Counts menunjukkan adanya beberapa kesalahan klasifikasi, seperti satu sampel Bayu Setiawan yang salah diklasifikasikan sebagai Daffa Erlangga Setiawan. Kesalahan ini disebabkan oleh kemiripan fitur morfologi wajah antar kedua subjek dan faktor pencahayaan yang menciptakan pola bayangan (*shadow*) yang serupa. Karena LBPH bekerja berdasarkan ekstraksi fitur tekstur *grayscale*, kemiripan intensitas piksel akibat pencahayaan yang kurang merata menjadi faktor utama terjadinya *False Positive.* Laporan Klasifikasi Rinci memvalidasi konsistensi model, di mana nilai *Macro Average* dan *Weighted Average* untuk *precision, recall*, dan *f1-score* keduanya stabil di angka 0.99. Mayoritas kelas mencapai nilai 1.00 pada ketiga metrik tersebut. Kelas dengan precision terendah adalah Syaiful Bahri (0.89), meskipun recallnya adalah 1.00.




Gambar 10. Kurva Kinerja dan Recall per Kelas

Evaluasi lebih rinci terhadap kinerja per kelas disajikan dalam kurva *Precision-Recall* pada Gambar 10. Mayoritas kelas mencapai skor sempurna, namun terdapat penurunan performa pada subjek tertentu.Namun, terdapat beberapa pengecualian yang menunjukkan adanya tantangan minor dalam identifikasi, seperti Bayu Setiawan (AP=0.91), Syaiful Bahri (AP=0.94), dan Sitti Nur Khalisah (AP=0.96). Penurunan nilai AP ini mengindikasikan adanya tantangan dalam membedakan fitur wajah subjek tersebut dengan subjek lain yang memiliki kemiripan morfologi (*inter-class similarity*). Meskipun terdapat bug visualisasi pada garis kurva Recall per kelas akibat limitasi *plotting threshold*, performa sensitivitas model sesungguhnya tervalidasi kuat melalui Matriks Kebingungan Gambar 9. Pada matriks tersebut, hampir seluruh sampel uji terklasifikasi dengan benar ke label masing-masing (Diagonal Matrix dominan), yang secara matematis membuktikan bahwa nilai Recall aktual berada di kisaran >98%, selaras dengan akurasi global model.




Gambar 11.a Dataset Folder hasil crop *Haar Cascade* wajah user

Berdasarkan diagram *Confidence Distribution*, Grafik ini menunjukkan separasi (pemisahan) yang jelas antara prediksi benar dan salah. Prediksi yang Benar (*Correct*) terkonsentrasi pada skor kepercayaan tinggi (range 45–70), sedangkan prediksi Salah (*Incorrect*) berkumpul pada skor rendah <30. Fenomena ini sangat positif karena menunjukkan bahwa model memiliki "kesadaran" terhadap ketidakpastiannya, saat model salah menebak, tingkat keyakinannya rendah. Karakteristik ini penting untuk penerapan *threshold* keamanan, di mana sistem dapat diatur untuk menolak akses jika skor kepercayaan berada di bawah ambang batas tertentu untuk meminimalkan risiko pembobolan.

```
FINAL RESULTS SUMMARY:
Accuracy: 0.9893 (98.93%)
Training Images: 1492
Test Images: 374
Model Saved: /content/drive/MyDrive/Traning facenet/models/lbph_model.xml
```

Gambar 11.b Dataset Folder hasil crop *Haar Cascade* wajah user

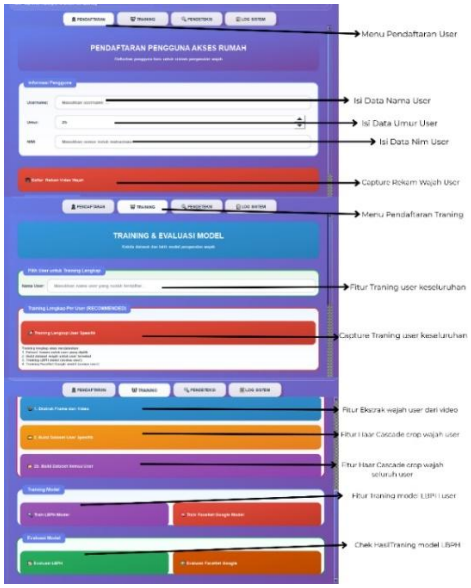
Gambar 11 menunjukkan ringkasan akhir proses pelatihan model yang menandakan keberhasilan seluruh *pipeline* pelatihan, dengan akurasi akhir sebesar 0,9893 (98,93%). Model dilatih untuk mengenali 30 pengguna menggunakan 1.492 citra pelatihan dan diuji pada 374 citra pengujian.

Meskipun akurasi yang diperoleh tergolong tinggi, metode *Local Binary Pattern Histogram* (LBPH) memiliki keterbatasan dibandingkan metode berbasis *deep learning* seperti FaceNet atau YOLOv5, terutama sensitivitas terhadap pencahayaan ekstrem dan variasi pose wajah non-frontal. Kesalahan klasifikasi umumnya disebabkan oleh perubahan intensitas cahaya dan sudut wajah yang memengaruhi histogram lokal. Namun demikian, LBPH tetap dipilih karena keunggulan efisiensi komputasi dan latensi rendah, sehingga mampu berjalan optimal pada perangkat *embedded* atau mini PC tanpa memerlukan GPU berperforma tinggi, dan sesuai untuk implementasi sistem keamanan pintu berbasis IoT yang menuntut respons cepat.

## *B. Tampilan Software dan Hardware*

1. Tampilan *Graphical User Interface* (GUI) Sistem

Pada bagian tampilan *Graphical User Interface* (GUI), desain antarmuka dirancang menyesuaikan dengan fungsi dan fitur yang terdapat pada setiap menu sistem. Serial komunikasi antar perangkat GUI (*Graphical User Interface*) sebagai interface sistem agar dapat berinteraksi dengan pengguna melalui elemen visual [20]. Setiap elemen pada GUI disusun secara sistematis agar pengguna dapat mengakses dan memahami alur kerja sistem dengan mudah. Tampilan ini tidak hanya berfungsi sebagai media interaksi antara pengguna dan sistem, tetapi juga merepresentasikan fungsi utama dari masing-masing menu seperti pendaftaran, traning, deteksi, dan log aktivitas. Penjelasan lebih detail mengenai fitur serta kegunaan setiap komponen pada antarmuka sistem dapat dilihat pada Gambar 12.




Gambar 12. Tampilan GUI menu Sistem

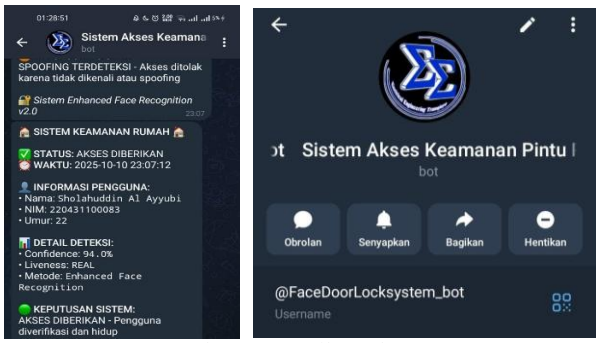
Menu pendaftaran pengguna berfungsi untuk memasukkan data pengguna baru yang berhak mengakses sistem, meliputi nama, umur, dan NIM, serta diakhiri dengan proses perekaman wajah sebagai data awal. Selanjutnya, menu *Training* dan Evaluasi Model memungkinkan administrator melatih model pengenalan wajah berbasis LBPH, baik untuk pengguna

tertentu maupun seluruh pengguna. Menu ini juga menyediakan fitur ekstraksi frame dari video dan *cropping* wajah menggunakan *Haar Cascade* sebagai tahap prapemrosesan dataset, serta evaluasi kinerja model hasil pelatihan.

Menu Pendeteksi Wajah *Real-Time* merupakan inti operasional sistem yang menyediakan proses verifikasi pengguna secara langsung menggunakan metode LBPH dengan *enhanced anti-spoofing*. Proses login, status *anti-spoofing*, dan pelatihan model, serta dilengkapi fitur penyimpanan dan penghapusan data log.

2. Tampilan Telegram Bot

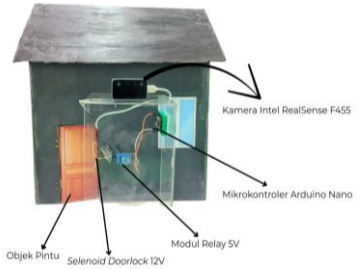
Pada bagian sistem Telegram Bot dirancang secara spesifik untuk berfungsi sebagai monitoring dan pengirim notifikasi real-time yang *independen*. Fungsi ini memastikan bahwa setiap peristiwa deteksi akses segera diketahui oleh pengelola sistem. Begitu seorang pengguna terdeteksi, Telegram Bot akan secara otomatis mengirimkan hasil verifikasi yang komprehensif. Notifikasi yang dikirimkan ini meliputi data pengguna yang telah diverifikasi (diambil dari data pendaftaran), yaitu Nama, NIM, dan Umur, disertai dengan hasil analisis real-time yang krusial: Status *Liveness* (yang mengonfirmasi keaslian wajah dan mencegah spoofing), serta Confidence (skor keyakinan model terhadap identitas yang terdeteksi). Dengan demikian, Telegram Bot menyediakan laporan aktivitas yang lengkap dan *up-to-date* untuk monitoring akses tanpa harus memantau GUI secara terus-menerus.




Gambar 13. Tampilan Telegram Bot

2. Hasil *Prototype* Rumah

Pada bagian hardware terdapat *prototype* atau miniature rumah sebagai simulasi sistem skala kecil.




Gambar 14. *Prototype* miniature rumah

Prototipe sistem akses rumah dirancang dalam bentuk miniatur yang merepresentasikan integrasi komponen elektronik untuk fungsi deteksi wajah dan kontrol pintu. Kamera Intel RealSense F455 berperan sebagai sensor utama yang dipasang di atas miniatur pintu untuk menangkap data wajah secara *real-time* serta mendukung analisis *anti-spoofing*. Mikrokontroler Arduino Nano berfungsi sebagai pusat kendali yang memproses hasil verifikasi wajah dan mengirimkan sinyal ke modul relay 5V. Modul *relay* bertindak sebagai sakelar elektronik untuk mengendalikan *solenoid doorlock* 12V sebagai aktuator pengunci pintu. Ketika proses verifikasi wajah dinyatakan berhasil, sistem mengaktifkan relay sehingga *solenoid doorlock* terbuka dan akses masuk diberikan.

## C. *Hasil Pengujian dan Kinerja Sistem*

1. Pengujian Validasi User dan confidence

Pengujian validasi user pada sistem keamanan rumah ini dilakukan dengan mengintegrasikan metode pengenalan wajah LBPH (*Local Binary Patterns Histograms*) dan *liveness detection* untuk memastikan keakuratan identifikasi. Sistem bekerja dengan mendeteksi wajah melalui kamera, kemudian mencocokkannya dengan data wajah yang telah dilatih dalam dataset menggunakan algoritma LBPH.


Gambar 15. Hasil *bounding box* Deteksi

Hasil deteksi ditampilkan dalam bentuk *bounding box* seperti gambar 15 yang dilengkapi dengan informasi identitas user berupa nama, NIM, dan umur. Selain itu, sistem juga mampu membedakan antara wajah asli (*real*) dan upaya penipuan (*spoofing*) melalui *liveness detection*, sambil memberikan nilai *confidence* yang mencerminkan tingkat kepercayaan sistem terhadap kecocokan identitas yang terverifikasi. Hasil pengujian dapat dilihat pada tabel 1 yang sudah di lampirkan, dimana tabel ini memberikan informasi nilai *confidence* dan kecocokan user pada sistem serta status *real*/palsu user.

TABEL 1.HASIL PENGUJIAN VALIDASI USER DAN CONFIDENCE

| Username | *Status Liveness* | *Nilai Confidence* |
|---|---|---|
| Hamzah Arifianto Diputra | Real Face | 87,9% |
| Bayu Setiawan | Real Face | 92,9% |
| Ari Ardyansah | Real Face | 90,2% |
| Febriyan Ardiantoro | Real Face | 93,5% |
| Syaiful Bahri | Real Face | 94,5% |
| Yunita Windayani | Real Face | 91,6% |
| Rahmad Agus W | Real Face | 90,6% |
| Sitti Nur Khalisah | Real Face | 91,7% |
| Adji Rahma Pramono | Real Face | 92,3% |
| A Makmum Alji | Real Face | 90,0% |
| Muhammad Rizky Arif Fadillah | Real Face | 90,2% |
| NUR ABDILLAH | Real Face | 91,5% |

| | | |
|---|---|---|
| SYAHRUL RIZAL ZAIN | Real Face | 89,2% |
| Moh Kaharil Rifa | Real Face | 89,8% |
| Abdul Hamid | Real Face | 90,4% |
| Win Wisnu Wardhana | Real Face | 95,1% |
| Novia Lailia Fitria k | Real Face | 93,5% |
| RAMLAH | Real Face | 94,2% |
| Elsya Azzahra Iskandar | Real Face | 89,5% |
| Daffa Erlangga Setiawan | Real Face | 92,1% |
| Muhammad Syauqi Annafi | Real Face | 88,4% |
| Achmad Tegar Lukmantiar | Real Face | 87,9% |
| Muhamad Fikri Kurniawan | Real Face | 88,3% |
| Muhammad Iwan Aliadin | Real Face | 91,5% |
| Aditya Wisnu Wardana | Real Face | 89,3% |
| Hani Dwi Pratiwi | Unknown | 57% |
| Yaro Awalia Rahma | Real Face | 90,9% |
| Fadhilah Aprilia Ayattul Rosydah | Real Face | 88,1% |
| Sholahuddin Al Ayyubi | Real Face | 93,5% |
| Alifnasyem | Real Face | 89,9% |

Berdasarkan hasil pengujian validasi pengguna pada tabel, Sebanyak 29 pengguna terdeteksi sebagai *Real Face* dengan nilai *confidence* konsisten di atas 87%, sedangkan 1 pengguna terdeteksi sebagai *Unknown* karena nilai *confidence* tidak mencapai ambang batas 60%. Nilai *confidence* tertinggi sebesar 95,5% diperoleh oleh pengguna Win Wisnu Wardhana. Hasil ini menunjukkan bahwa integrasi metode pengenalan wajah LBPH dan *liveness detection* berfungsi optimal dalam mengidentifikasi keaslian wajah serta mencegah upaya *spoofing*. Konsistensi nilai *confidence* yang tinggi menegaskan bahwa model LBPH telah terlatih dengan baik dan mampu memberikan hasil identifikasi yang akurat serta andal dalam pengamanan akses rumah.

2. Pengujian *Monitoring* Telegram Bot

Pengujian monitoring Telegram Bot bertujuan memvalidasi kemampuan sistem dalam mengirimkan notifikasi *real-time* kepada administrator melalui platform Telegram. Pengujian ini memastikan bahwa setiap hasil deteksi wajah, baik terverifikasi maupun mencurigakan, dapat dikirim secara tepat waktu dengan informasi lengkap, meliputi nama, NIM, umur, status *liveness* (*Real Face* atau *Spoofing*), hasil akses (diterima/ditolak), dan nilai *confidence*. Hasil pengujian menunjukkan bahwa seluruh notifikasi yang dikirim sesuai dengan tampilan pada antarmuka sistem dan diterima tanpa keterlambatan yang signifikan, sehingga membuktikan keandalan integrasi antara modul deteksi wajah dan sistem notifikasi sebagai bagian dari monitoring keamanan pintu secara *real-time.*

TABEL 2.HASIL PENGUJIAN *MONITORING* TELEGRAM BOT

| Username | Hasil Monitoring Telegram Bot | Akses |
|---|---|---|
| Hamzah Arifianto Diputra | Nama :Hamzah Arifianto Diputra<br>Nim : 210431100004<br>Confidence :87,9%<br>Liveness : REAL | Diterima |
| Bayu Setiawan | Nama : Bayu Setiawan<br>Nim : 240481100050<br>Confidence :92,9%<br>Liveness : REAL | Diterima |
| Ari Ardyansah | Nama : Ari Ardyansah<br>Nim : 230431100019<br>Confidence :90,2%<br>Liveness : REAL | Diterima |
| Febriyan Ardiantoro | Nama : Febriyan Ardiantoro<br>Nim : 230481100063<br>Confidence :93,5%<br>Liveness : REAL | Diterima |
| Syaiful Bahri | Nama : Syaiful Bahri<br>Nim : 230431100045<br>Confidence :94,5%<br>Liveness : REAL | Diterima |
| Yunita Windayani | Nama : Yunita Windayani<br>Nim : 230421100069<br>Confidence :91,6%<br>Liveness : REAL | Diterima |
| Rahmad Agus W | Nama : Rahmad Agus W<br>Nim : 230491100024<br>Confidence :90,6%<br>Liveness : REAL | Diterima |
| Sitti Nur Khalisah | Nama : Sitti Nur Khalisah<br>Nim : 220411100123<br>Confidence :91,7%<br>Liveness : REAL | Diterima |
| Adji Rahma Pramono | Nama : Adji Rahma Pramono<br>Nim : 230431100007<br>Confidence :92,3%<br>Liveness : REAL | Diterima |
| A Makmum Alji | Nama : A Makmum Alji<br>Nim : 210411100241<br>Confidence :90,0%<br>Liveness : REAL | Diterima |
| Muhammad Rizky Arif Fadillah | Nama : Muhammad Rizky Arif Fadillah<br>Nim : 210431100003<br>Confidence :90,2%<br>Liveness : REAL | Diterima |
| NUR ABDILLAH | Nama : NUR ABDILLAH<br>Nim : 210431100026<br>Confidence :91,5%<br>Liveness : REAL | Diterima |
| SYAHRUL RIZAL ZAINI | Nama : SYAHRUL RIZAL ZAINI<br>Nim : 210431100079<br>Confidence :89,2%<br>Liveness : REAL | Diterima |
| Moh Kaharil Rifa | Nama : Moh Kaharil Rifa<br>Nim : 210431100057<br>Confidence :89,8%<br>Liveness : REAL | Diterima |
| Abdul Hamid | Nama : Abdul Hamid<br>Nim : 210431100082<br>Umur :23<br>Confidence :90,4%<br>Liveness : REAL | Diterima |
| Win Wisnu Wardhana | Nama : Win Wisnu Wardhana<br>Nim : 210431100007<br>Umur :22 | Diterima |

| Username | Hasil Monitoring Telegram Bot | Akses |
|---|---|---|
| | Confidence :95,5%<br>Liveness : REAL | |
| Novia Lailia Fitria k | Nama : Novia Lailia Fitria k<br>Nim : 240531100002<br>Umur :20<br>Confidence :93,5%<br>Liveness : REAL | Diterima |
| RAMLAH | Nama : RAMLAH<br>Nim : 230241100007<br>Umur :22<br>Confidence :94,2%<br>Liveness : REAL | Diterima |
| Elsya Azzahra Iskandar | Nama : Elsya Azzahra Iskandar<br>Nim : 240231100061<br>Umur :19<br>Confidence :89,5%<br>Liveness : REAL | Diterima |
| Daffa Erlangga Setiawan | Nama : Daffa Erlangga Setiawan<br>Nim : 240431100073<br>Umur :20<br>Confidence :92,1%<br>Liveness : REAL | Diterima |
| Muhammad Syauqi Annafi | Nama : Muhammad Syauqi Annafi<br>Nim : 210431100016<br>Umur :22<br>Confidence :88,4%<br>Liveness : REAL | Diterima |
| Achmad Tegar Lukmantiar | Nama : Achmad Tegar Lukmantiar<br>Nim : 210431100012<br>Umur :22<br>Confidence :87,9%<br>Liveness : REAL | Diterima |
| Muhamad Fikri Kurniawan | Nama : Muhamad Fikri Kurniawan<br>Nim : 230431100103<br>Umur :20<br>Confidence :88,3%<br>Liveness : REAL | Diterima |
| Muhammad Iwan Aliadin | Nama : Muhammad Iwan Aliadin<br>Nim : 230431100006<br>Umur :20<br>Confidence :91,5%<br>Liveness : REAL | Diterima |
| Aditya Wisnu Wardana | Nama : Aditya Wisnu Wardana<br>Nim : 230431100048<br>Umur :21<br>Confidence :89,3%<br>Liveness : REAL | Diterima |
| Wijaya Aji Nur Khalid | Nama : Wijaya Aji Nur Khalid<br>Nim : 230431100003<br>Umur :20<br>Confidence :93,2%<br>Liveness : REAL | Diterima |
| Yaro Awalia Rahma | Nama : Yaro Awalia Rahma<br>Nim : 240421100041<br>Umur :19<br>Confidence :90,9%<br>Liveness : REAL | Diterima |
| Fadhilah Aprilia Ayattul Rosydah | Nama : Fadhilah Aprilia Ayattul Rosydah<br>Nim : 230421100019<br>Confidence :88,1%<br>Liveness : REAL | Diterima |
| Sholahuddin Al Ayyubi | Nama : Sholahuddin A<br>Nim : 220431100083 | Diterima |
| | Confidence :93,5%<br>Liveness : REAL | |
| Alifnasyem | Nama : Alifnasyem<br>Nim : 220431100072<br>Confidence :89,9%<br>Liveness : REAL | Diterima |

Berdasarkan hasil pengujian *monitoring* Telegram Bot yang tercantum pada Tabel 2, dapat disimpulkan bahwa sistem notifikasi *real-time* berfungsi dengan sangat optimal. Seluruh pengguna terdaftar yang berhasil terverifikasi oleh sistem deteksi wajah LBPH + *Enhanced Anti-Spoofing* berhasil memicu pengiriman notifikasi secara instan ke Telegram Bot.

3. Pengujian *Black Box*

Pengujian menggunakan metode *black box* dilakukan untuk mengevaluasi fungsi dari setiap fitur pada sistem guna mengetahui efektivitas kinerjannya, serta memastikan sistem dapat berfungsi dengan baik. Hasil pengujian pada tabel.. menunjukkan semua fitur berfungsi dengan baik sesuai yang diharapkan.

TABEL 3.HASIL PENGUJIAN SISTEM DENGAN METODE *BLACK BOX*

| Parameter Pengujian | Bentuk Pengujian | Hasil Yang di Harapkan | Hasil |
|---|---|---|---|
| Membuka Sistem GUI | Run program untuk mejalankan GUI sistem | Tampilan GUI muncul dengan responsfi dengan menu | Valid |
| Pendaftaran User & Penyimpanan Data | Input data pengguna lengkap (Nama, Umur, NIM) dan klik Daftar Rekam Wajah User. | Data identitas pengguna dan sampel rekaman wajah berhasil tersimpan di *database*. | Valid |
| Pelatihan Model LBPH | Memilih user dan menjalankan proses *Training* LBPH Model. | Model LBPH berhasil dilatih dan file model berhasil disimpan, siap untuk evaluasi | Valid |
| Deteksi User Terdaftar dengan *Anti-Spoofing* | User terdaftar menghadap kamera saat mode Deteksi dengan LBPH + *Enhanced Anti-Spoofing* aktif. | Sistem berhasil mengidentifikasi user, status anti-spoofing LULUS, dan akses diberikan. | Valid |
| Pencatatan Log Aktivitas Deteksi | Melakukan event deteksi (misal: verifikasi sukses). | Log aktivitas sistem mencatat timestamp dan deskripsi hasil deteksi/verifikas | Valid |
| Fumgsi Menu | Klik seluruh fitur yang ada pada menu | Fitur bekerja sesuai fungsi yang telah ditentukan | Valid |

## IV. KESIMPULAN

Berdasarkan hasil penelitian, sistem keamanan pintu berbasis *liveness detection* menggunakan kamera Intel RealSense F455 dan algoritma LBPH berhasil diimplementasikan dengan tingkat akurasi pengenalan wajah sebesar 98,93%, di mana sistem mampu memverifikasi 30 pengguna terdaftar dengan nilai *confidence* rata-rata yang konsisten di atas 80%. Mekanisme *liveness detection* berbasis deteksi pergerakan mata menggunakan *Haarcascade Eye* terbukti efektif dalam membedakan wajah asli dari upaya

pemalsuan menggunakan media foto, dengan seluruh pengujian berhasil mengidentifikasi wajah hidup secara konsisten. Kombinasi *Haarcascade* dan LBPH menunjukkan performa yang stabil untuk operasi *real-time*, didukung integrasi sistem yang berjalan baik pada modul pendeteksian, pemrosesan, aktuasi, dan monitoring. Sistem notifikasi berbasis bot Telegram mampu menyajikan informasi akses secara *real-time*, meliputi identitas pengguna, status *liveness*, nilai *confidence*, dan status akses pintu. Implikasi praktis dari penelitian ini adalah penerapan sistem keamanan pintu berbasis pengenalan wajah dengan *liveness detection* yang ringan dan responsif, sedangkan implikasi akademiknya terletak pada kontribusi metode *eye-based liveness detection* sebagai pendekatan sederhana untuk mitigasi serangan *spoofing* pada sistem visi komputer berbasis *embedded*.


## UCAPAN TERIMA KASIH

Penulis menyampaikan penghargaan dan terimkasih kepada seluruh pihak yang sudah berkontribusi dan bekerja sama dalam penelitian ini. Ucapan teimakasih disampaikan kepada para pembimbing yang sudah terlibat dalam penelitian. Selain itu, penghargaan khusus terhadap rekan rekan seperjuangan di Program Studi Teknik Elektro, Universitas Trunojoyo Madura, yang telah memberikan masukan berharga selama proses penelitian ini.


## Refferensi


[1] Galef Prannata Dan 2denny Irawan, "Pengaplikasian E-Ktp Sebagai Alat Keamanan Pintu Digital Berbasis Iot," *Jurnal Zetroem*, Vol. 06, Hlm. 13–17, 2024.

[2] F. Hadi Kusuma, A. Ubaidillah Ms, A. Fiqhi Ibadillah, V. N. Vivin Nahari, K. Joni, Dan A. Kurniawan Saputro, "Sistem Identifikasi Kesegaran Dan Jenis Ikan Dengan Metode K-Nearest Neighbor Berdasarkan Citra Mata Dan Bentuk Ikan," *Jurnal Fortech*, Vol. 4, No. 1, Mar 2023,

[3] S. G. C, K. H. S, S. Shirahatti, Dan S. R. Bangari, "Face Recognition System For Real Time Applications Using Svm Combined With Facenet And Mtcnn," *International Journal Of Electrical Engineering And Technology (Ijeet)*, Vol. 12, No. 6, Hlm. 328–335, 2021, Doi: 10.34218/Ijeet.12.6.2021.031.

[4] F. Intel® Realsensetm Id Solution F450, "Intel_Realsense_Id_Solution_F450_F455_Datasheet_Rev005 (1)," Hlm. 8–36, Mar 2024.

[5] M. Li, "Research And Analysis Of Facial Recognition Based On Facenet, Deepface, And Openface," *Itm Web Of Conferences*, Vol. 70, Hlm. 03009, 2025, Doi: 10.1051/Itmconf/20257003009.

[6] E. D. Yudi, Y. N. Kunang, Dan A. Zarkasi, "The Memory Efficiency In A Receptionist Robot's Face Recognition System Using Lbph Algorithm," *Jurnal Resti*, Vol. 8, No. 6, Hlm. 719–729, Des 2024

[7] H. Hadi, H. Radiles, R. Susanti, Dan M. Mulyono, "Human Face Identification Using Haar Cascade Classifier And Lbph Based On Lighting Intensity," *Indonesian Journal Of Artificial Intelligence And Data Mining*, Vol. 5, No. 1, Hlm. 13, Mei 2022

[8] A. ' Aatieff *Dkk.*, "Face Recognition Based Attendance System Using Haar Cascade And Local Binary Pattern Histogram Algorithm," *Journal Of Advanced Research In Applied Sciences And Engineering Technology Journal Homepage*, Vol. 59, Hlm. 141–153, 2026,

[9] M. Raihan Akbar, "Klasifikasi Pengenalan Wajah Menggunakan Metode Mtcnn Dan Transfer Learning Vgg19 Dalam Pelacakan Posisi Wajah," Universitas Islam Negeri Syarif Hidayatullah Jakarta, 2025.

[10] A. I. Rizki, R. Regasari, M. Putri, Dan N. H. Shaffan, "Sistem Pintu Cerdas Berbasis Pengenalan Wajah Dan Kartu Identitas Menggunakan Yolov8 Dan Optical Character Recognition (Ocr)," 2025.

[11] S. P. D. Prayudha Dan A. D. Putro, "Sistem Absensi Guru Berbasis Pengenalan Wajah Menggunakan Algoritma Yolov8," *Jurikom (Jurnal Riset Komputer)*, Vol. 12, No. 2, Hlm. 118–128, Apr 2025,

[12] C. A. Antipona, R. Magsino, D. R. Dioses, Dan E. K. Mata, "An Enhancement Of Haar Cascade Algorithm Applied To Face Recognition For Gate Pass Security," 2024.

[13] A. A. Nuryono, I. Ardiyanto, Dan S. Wibirama, "Program Studi Pendidikan Matematika Fkip Ums Navigasi Objek Virtual Bergerak Bebas Untuk Augmented Reality Menggunakan Kamera 3d Intel Realsense," 2018.

[14] S. Zhang Dan W. Nie, "Multi-Domain Feature Alignment For Face Anti-Spoofing," *Sensors*, Vol. 23, No. 8, Apr 2023, Doi: 10.3390/S23084077.

[15] A. Febrianti, B. N. Azizah, Dan E. S. Septiani, "Pemanfaatan Telegram Bot Pada Sistem Keamanan Rumah Berbasis Iot Dengan Mikrokontroler Esp32," *Seminar Nasional Teknologi Informasi Dan Bisnis (Senatib)*, No. Issn: 2962-1968, Hlm. 532–539, Jul 2025.

[16] M. N. Syaul, "Rancang Bangun Sistem Keamanan Perumahan Menggunakan Metode Pengenalan Wajah, Local Binary Pattern Histogram Dan Haar Cascade Classifier," Universitas Satya Negara Indonesia, Jakarta, 2024.

[17] Ahmad Jalaluddin, "Rancang Bangun Sistem Pengenalan Wajah Menggunakan Metode Haar Cascade Classifier Dan Local Binary Pattern Histogram (Lbph) Pada Akses Masuk Ruang Dosen," Universitas Islam Sultan Agung, Semarang, 2023.

[18] I. H. Cahyadi, M. A. Hidayatullah, Dan S. N. Ramdan, "Perancangan Sistem Otentikasi Berbasis One Time Passworsd (Otp) Dengan Algoritma Rsa Sebagai Metode Autentikasi: Implementasi Menggunakan Bahasa Pemrograman Phyton," *Jurnal Pendidikan Teknologi Informasi*, Vol. 2, Hlm. 8–13, Jul 2023.

[19] I. Fitri, C. Dewi, Dan J. A. Munif, "Otomatisasi Pintu Dengan Menggunakan Esp32-Cam Berbasis Telegram," *Seminar Nasional Teknologi Informasi Dan Bisnis (Senatib)*, No. Issn: 2962-1968, Hlm. 823–834, Jul 2025.

[20] B. Mursidiyansah, ; Mohammad, Dan N. Mubin, "Prototipe Sistem Akses Pintu Rumah Berbasis Integrasi Biometrik Wajah Dan Rfid," Surakarta, 2025.