

Implementasi Metode Deteksi Objek Pada Sistem Pagar Pintar Berbasis ESP32-CAM Dengan Fitur Akses Tamu Via OTP

Akhun Ihsan Hia^{1*}, Mhd. Basri²

^{1,2} Program Studi Teknologi Informasi, Fakultas Ilmu Komputer Dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, Jl. Kapten Muchtar Basri No.3, Glugur Darat II, Kec. Medan Tim., Kota Medan, Sumatera Utara 20238

*Penulis Korespondensi: akhunbaru01@gmail.com, mhd.basri@umsu.ac.id

Abstract. *Conventional security systems for residential and institutional gates and doors still have vulnerabilities related to human error, lost keys, and limited remote monitoring. This study aims to design and implement a Smart Gate System based on the Internet of Things (IoT) and Computer Vision to improve the efficiency, flexibility, and reliability of gate security. The methods used include an ESP32-CAM equipped with an OV2640 camera to capture images in real-time, the YOLOv5 algorithm for human object detection, and the Local Binary Pattern Histogram (LBPH) method through OpenCV for face recognition. The system also implements Two-Factor Authentication (2FA) using a dynamic One-Time Password (OTP) sent through the Telegram Bot API as a guest access verification mechanism. The monitoring process, activity logging, and OTP verification are centrally controlled through a web-based dashboard using Streamlit. The results show that the system is capable of integrating human detection, face recognition, and OTP verification to control actuators consisting of a 5V relay, Solenoid Door Lock, and MG996R Servo Motor for gate access, thereby improving security and reducing the risk of unauthorized access.*

Keywords: *Smart Gate; ESP32-CAM; YOLOv5; LBPH; OTP; Telegram Bot API; Streamlit.*

Abstrak. Sistem keamanan konvensional pada pagar dan pintu perumahan maupun instansi masih memiliki kerentanan terhadap kelalaian manusia, kehilangan kunci, serta keterbatasan pemantauan jarak jauh. Penelitian ini bertujuan untuk merancang dan mengimplementasikan *Smart Gate System* berbasis *Internet of Things* (IoT) dan *Computer Vision* guna meningkatkan efisiensi, fleksibilitas, dan keandalan pengamanan gerbang. Metode yang digunakan meliputi ESP32-CAM dengan kamera OV2640 untuk menangkap citra secara *real-time*, algoritma YOLOv5 untuk mendeteksi objek manusia, serta metode *Local Binary Pattern Histogram* (LBPH) melalui OpenCV untuk pengenalan wajah. Sistem juga menerapkan *Two-Factor Authentication* (2FA) berupa *One-Time Password* (OTP) yang dikirim melalui Telegram Bot API sebagai verifikasi akses tamu. Seluruh proses monitoring, pencatatan aktivitas, dan verifikasi OTP dikendalikan melalui *dashboard* berbasis web menggunakan Streamlit. Hasil penelitian menunjukkan bahwa sistem mampu mengintegrasikan deteksi manusia, pengenalan wajah, dan verifikasi OTP untuk mengendalikan aktuator berupa Relay 5V, *Solenoid Door Lock*, dan Motor Servo MG996R dalam proses pembukaan gerbang, sehingga dapat meningkatkan keamanan dan mengurangi risiko akses tidak sah.

Kata kunci: *Smart Gate; ESP32-CAM; YOLOv5; LBPH; OTP; Telegram Bot API; Streamlit.*

1. LATAR BELAKANG

Keamanan hunian merupakan aspek fundamental yang menjadi prioritas utama bagi setiap pemilik rumah di tengah meningkatnya angka kriminalitas, khususnya kasus pencurian pada rumah kosong di area perkotaan. Seiring dengan perkembangan teknologi, sistem keamanan fisik seperti pagar rumah tidak lagi cukup apabila hanya mengandalkan mekanisme penguncian manual yang bersifat statis. Oleh karena itu, diperlukan sebuah transformasi sistem keamanan hunian yang mampu memanfaatkan

teknologi modern berbasis *Internet of Things* (IoT) sehingga dapat bekerja secara otomatis, cerdas, dan mampu memberikan pengawasan secara terus-menerus selama 24 jam (Rumere & Manullang, 2024).

Permasalahan utama pada sistem pagar otomatis yang banyak digunakan saat ini adalah keterbatasannya dalam mengenali identitas individu yang berada di depan pintu masuk. Sebagian besar sistem hanya memanfaatkan sensor gerak atau *remote control* tanpa adanya proses verifikasi identitas secara visual. Kondisi tersebut menyebabkan potensi penyalahgunaan akses masih cukup tinggi, karena sistem tidak mampu membedakan antara pemilik rumah, tamu, maupun orang asing. Selain itu, pemilik rumah sering mengalami kesulitan dalam memberikan akses kepada tamu atau kerabat ketika tidak berada di rumah, sehingga diperlukan suatu sistem yang mampu memberikan kontrol akses secara jarak jauh berbasis teknologi *Internet of Things* (IoT) (Santoso & Kristianto, 2020).

Perkembangan teknologi *Artificial Intelligence* (AI) khususnya pada bidang *Computer Vision* memberikan peluang besar untuk meningkatkan efektivitas sistem keamanan hunian. Salah satu algoritma yang tangguh dalam proses deteksi objek adalah YOLOv5 (*You Only Look Once* versi 5), yang memiliki kemampuan memproses *frame* gambar secara *real-time* dengan tingkat komputasi yang cepat. Dengan memanfaatkan algoritma YOLOv5 sebagai pra-deteksi, sistem dapat memfilter dan mengidentifikasi keberadaan manusia secara presisi, sehingga mampu meminimalisir kesalahan deteksi yang sering terjadi pada sensor gerak konvensional akibat pergerakan hewan peliharaan atau benda mati (Yusup Efendi, Wulanningrum, & Bagus Setiawan, 2024).

Untuk melengkapi kemampuan pengenalan identitas, penelitian ini mengintegrasikan metode *Face Recognition* menggunakan pustaka OpenCV. Melalui algoritma *Local Binary Pattern Histogram* (LBPH), sistem mampu melakukan ekstraksi pola wajah secara *real-time* dengan tingkat stabilitas yang baik terhadap variasi pencahayaan. Meskipun teknologi ini menawarkan identifikasi otomatis, sistem kamera 2D konvensional memiliki kerentanan keamanan terhadap serangan pemalsuan (*spoofing attack*), di mana sensor dapat dikelabui menggunakan foto cetak atau tampilan wajah dari layar digital milik pihak yang tidak bertanggung jawab (Faturrachman & Yustiana, 2021).

Guna mengatasi celah keamanan *spoofing* tersebut, penelitian ini mengimplementasikan mekanisme *One-Time Password* (OTP) secara menyeluruh

sebagai bentuk *Two-Factor Authentication* (2FA). Kode OTP tidak hanya diposisikan sebagai alat verifikasi bagi tamu yang tidak dikenali, melainkan juga diwajibkan bagi pemilik rumah meskipun wajahnya telah terverifikasi oleh algoritma LBPH. Melalui pendekatan otentikasi ganda ini, akses pembukaan pagar tidak lagi bergantung pada pemindaian biometrik semata, melainkan membutuhkan validasi token dinamis yang hanya dimiliki oleh otoritas pengguna aslinya, sehingga mampu mencegah akses masuk ilegal secara mutlak (Ilham, Mashudi, & Prihanto, 2024).

Selanjutnya, penelitian ini membahas sistem yang mengirimkan notifikasi kepada pemilik rumah melalui aplikasi Telegram Bot berupa gambar tamu yang terdeteksi beserta kode OTP dinamis. Pemilik rumah dapat meninjau identitas tamu secara visual melalui Telegram, namun kendali akses dan input kode OTP dilakukan melalui dashboard monitoring berbasis web. Bagi pemilik rumah yang datang, kode OTP tersebut tetap wajib dimasukkan melalui antarmuka web sebagai validasi keamanan ganda (*Two-Factor Authentication*). Dengan integrasi teknologi IoT, Artificial Intelligence (YOLOv5 & LBPH), serta sistem monitoring terpusat, diharapkan rancangan ini mampu meningkatkan keamanan hunian sekaligus memberikan kemudahan kontrol akses yang lebih efektif, efisien, dan terorganisir.

2. KAJIAN TEORITIS

A. Komunikasi Two-Factor Authentication

Two-Factor Authentication (2FA) adalah metode keamanan yang mengharuskan pengguna menyediakan dua faktor pembuktian identitas yang berbeda sebelum diberikan akses ke suatu sistem. Faktor ini biasanya dikategorikan menjadi sesuatu yang diketahui (seperti kata sandi), sesuatu yang dimiliki (seperti perangkat seluler), atau sesuatu yang melekat pada diri (seperti biometrik wajah atau sidik jari). Dengan menggabungkan dua elemen independen ini, misalnya pengenalan wajah sebagai faktor pertama dan kode sandi sebagai faktor kedua. Sistem menciptakan lapisan perlindungan ganda yang jauh lebih kuat dibandingkan hanya mengandalkan kredensial tunggal, sehingga meminimalisir risiko peretasan meskipun salah satu faktor keamanan telah dikompromikan oleh pihak luar (Ilham et al., 2024).

B. Internet of Things (IoT)

Internet of Things (IoT) adalah sebuah konsep di mana perangkat keras atau objek fisik dihubungkan ke jaringan internet untuk saling bertukar data dan dikendalikan secara

jarak jauh melalui aplikasi atau *server*. Dalam sistem keamanan pagar ini, peran IoT sangat dominan karena menjadi jembatan utama yang menghubungkan komponen fisik di lapangan dengan pengguna melalui media nirkabel (Hasibuan & Asih, 2023). Salah satu komponen kunci dalam arsitektur IoT adalah penggunaan ESP32-CAM, sebuah modul mikrokontroler yang mengintegrasikan fitur kamera dan koneksi nirkabel Wi-Fi dalam satu unit kecil. ESP32-CAM bertugas sebagai unit pengambil citra yang kemudian mengirimkan data visual tersebut ke *server* lokal (PC/ Laptop) untuk diproses lebih lanjut menggunakan teknologi *Artificial Intelligence* (AI) (Kusuma, Wijaya, & Nusyirwan, 2023).

C. Metode Local Binary Pattern Histogram (LBPH)

Local Binary Pattern Histogram (LBPH) merupakan salah satu metode yang banyak digunakan dalam sistem pengenalan wajah berbasis pustaka OpenCV. Metode ini bekerja dengan menganalisis pola tekstur lokal pada citra wajah sehingga menghasilkan representasi numerik yang unik untuk setiap individu. Metode LBPH dikenal memiliki keunggulan dalam hal kesederhanaan komputasi algoritma serta kemampuan pengenalan wajah yang sangat stabil meskipun berada pada berbagai kondisi variasi pencahayaan di lingkungan luar (Renhat Ade Prayogo, Kingkin Sulistiana, & Eko Febrianto, 2025).

Dalam implementasinya, metode LBPH memiliki beberapa tahapan utama, yaitu proses konversi citra ke dalam bentuk *grayscale*, ekstraksi pola lokal menggunakan operator *Local Binary Pattern*, serta pembentukan histogram sebagai fitur representasi wajah yang akan digunakan dalam proses identifikasi. Histogram yang dihasilkan kemudian dibandingkan dengan data wajah yang telah tersimpan pada *dataset* pelatihan untuk menentukan tingkat kemiripan (jarak matriks) antara citra wajah yang terdeteksi dengan data wajah yang telah didaftarkan ke dalam sistem (Santoso & Kristianto, 2020).

D. Telegram Bot dan OTP

Telegram Bot merupakan layanan otomatis yang tersedia pada aplikasi Telegram yang memungkinkan sistem komputer untuk mengirim pesan, gambar, maupun notifikasi secara *real-time* kepada pengguna melalui internet. Melalui Telegram Bot, sistem dapat mengirimkan informasi berupa gambar wajah pengunjung (baik pemilik maupun tamu) yang tertangkap kamera, serta bertindak sebagai antarmuka utama untuk pengiriman notifikasi kode otentikasi. Penggunaan Telegram Bot pada sistem berbasis Internet of Things (IoT) terbukti mampu memberikan kemudahan dalam proses penerimaan

informasi keamanan secara efisien (Kusuma et al., 2023).

Salah satu fitur keamanan fundamental yang diintegrasikan dalam sistem ini adalah penggunaan *One-Time Password* (OTP) sebagai metode verifikasi akses lapis kedua. OTP merupakan kode rahasia yang bersifat dinamis dan hanya dapat digunakan satu kali dalam proses autentikasi dengan batas waktu kedaluwarsa tertentu (*timeout*). Pendekatan ini dirancang khusus untuk menutup celah keamanan pemalsuan wajah (*spoofing*), sehingga akses pembukaan pagar tidak akan pernah diberikan secara otomatis hanya dengan mengandalkan kecocokan data biometrik visual semata (Ilham et al., 2024).

E. Dashboard Monitoring Berbasis Web

Dashboard monitoring merupakan antarmuka grafis yang berfungsi sebagai pusat kendali dan visualisasi data dalam ekosistem *Internet of Things* (IoT). Dalam sistem keamanan pintar, penggunaan *dashboard* berbasis web memungkinkan pemilik rumah untuk melakukan pemantauan kondisi pagar secara *real-time* dan interaktif tanpa terbatas oleh kendala instalasi perangkat lunak khusus. Implementasi *dashboard* yang terintegrasi dengan server lokal memberikan kemudahan dalam menyajikan data visual dari kamera pemantau serta menyediakan elemen kendali seperti tombol aksi dan kolom *input* untuk kebutuhan validasi akses pengguna secara terpusat (Syabibi & Subari, 2016).

Salah satu *framework* yang efisien dalam pengembangan antarmuka monitoring ini adalah Streamlit, yang merupakan perpustakaan Python sumber terbuka untuk membangun aplikasi web kustom secara cepat. Penggunaan *dashboard* berbasis web dalam sistem keamanan *2nd-factor authentication* berperan penting sebagai media verifikasi akhir, di mana pemilik rumah memasukkan kode OTP yang diterima dari saluran sekunder untuk mengaktifkan aktuator pagar. Integrasi antara platform web dengan algoritma pemrosesan citra memastikan bahwa seluruh aktivitas akses terekam dan dapat dipantau dengan tingkat responsivitas yang tinggi, sehingga meningkatkan efektivitas pengawasan keamanan hunian (Riyanto, Nurlaila, Haerudin, & Jarastino, 2021).

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode eksperimental yang berfokus pada rancang bangun sistem keamanan pagar pintar dengan mengintegrasikan teknologi *Artificial Intelligence* (AI) dan *Internet of Things* (IoT). Tahap awal dimulai dengan perancangan arsitektur perangkat keras, di mana ESP32-CAM difungsikan

sebagai sensor citra nirkabel yang terhubung dengan aktuator berupa *Solenoid Door Lock* dan Motor Servo. Selanjutnya, pengembangan perangkat lunak dilakukan dengan menerapkan metode deteksi objek YOLOv5 dan algoritma pengenalan wajah LBPH pada OpenCV. Metode pengamanan akhir yang diterapkan dalam penelitian ini adalah mekanisme Two-Factor Authentication (2FA) menggunakan kode OTP yang dikirimkan melalui Telegram Bot. Pengujian dilakukan melalui prosedur Pengujian Akurasi Visi Komputer (Vision), Pengujian Fungsionalitas Sistem dan Konektivitas, dan Pengujian Fungsionalitas Dashboard Web Monitoring.

4. HASIL DAN PEMBAHASAN

A. Implementasi Sistem

Implementasi Perangkat Keras (Hardware)

Perangkat keras dirancang dalam bentuk prototipe miniatur gerbang geser (*sliding gate*). Komponen utama yang diintegrasikan meliputi:

- 1) Modul *microcontroller* ESP32-CAM diletakkan secara vertikal di bagian tiang penyangga gerbang dengan ketinggian optimal untuk menangkap citra wajah pengunjung secara tegak lurus.
- 2) Komponen aktuator fisik yang terdiri dari *Relay 5V*, *Solenoid Door Lock*, dan Motor Servo MG996R diposisikan di dalam kotak sirkuit pelindung (*enclosure box*) bawah. *Solenoid* bertindak sebagai pengunci mekanis pasif, sedangkan Motor Servo dan Motor DC *Gearbox* dihubungkan ke rel gerbang menggunakan sistem roda gigi untuk mendorong daun pagar saat akses diberikan oleh pemilik rumah.



Gambar 1 Prototipe Sistem Pagar Pintar

Gambar tersebut menunjukkan prototipe sistem pagar pintar (*Smart Gate*) yang dibuat dalam bentuk miniatur gerbang geser (*sliding gate*). Pada prototipe terlihat bagian daun pagar yang dapat bergerak pada jalur atau rel, serta rangkaian elektronika yang digunakan untuk mendukung pengoperasian sistem. Pada bagian depan terdapat ESP32-

CAM yang berfungsi sebagai perangkat pengambil citra, sedangkan rangkaian pada breadboard, kabel jumper, dan sumber daya digunakan sebagai pendukung koneksi serta pengendalian komponen sistem. Prototipe ini dirancang untuk mengintegrasikan proses pengambilan citra, pengenalan pengguna, serta mekanisme penguncian dan pembukaan pagar secara otomatis berdasarkan hasil verifikasi akses

Implementasi Perangkat Lunak (software)

Sisi *server* lokal dijalankan menggunakan laptop berspesifikasi prosesor tingkat tinggi yang mengeksekusi skrip Python via *code editor* Visual Studio Code. Ekosistem perangkat lunak diimplementasikan sebagai berikut:

1) Model Deteksi dan Pengenalan Wajah

Algoritma YOLOv5 dimuat menggunakan pustaka *PyTorch* untuk penyaringan objek manusia secara *real-time*. Pustaka OpenCV dikonfigurasi menggunakan algoritma *Local Binary Pattern Histogram* (LBPH) yang terhubung dengan *dataset* gambar wajah pemilik yang telah melalui proses pelatihan (*training*).

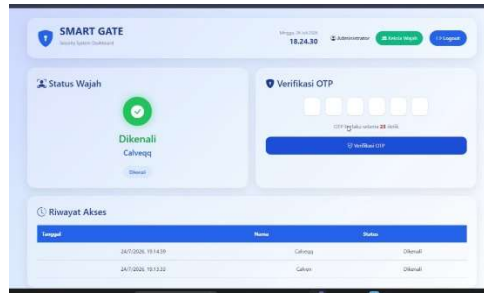
2) Dashboard Web Monitoring (*Streamlit*)

Antarmuka web dibangun menggunakan *framework* Streamlit. Halaman ini berfungsi menampilkan aliran video langsung (*live video streaming*) dari ESP32-CAM, kolom pengisian token dinamis *One-Time Password* (OTP), serta menampilkan tabel riwayat log aktivitas pengguna.

3) Database MySQL & Telegram Bot API

MySQL bertindak sebagai media penyimpanan terstruktur untuk data kredensial, nilai *confidence score* wajah, serta status token OTP. Komunikasi otomatis dengan pemilik rumah dijembatani menggunakan *Universal Telegram Bot Library* melalui protokol HTTPS.

Pada tahap implementasi perangkat lunak, web monitoring pada sistem Smart Gate digunakan sebagai media pemantauan dan verifikasi akses. Dashboard menampilkan *live streaming* dari ESP32-CAM untuk memantau kondisi di sekitar pagar secara langsung. Selain itu, terdapat bagian Status Wajah untuk menampilkan hasil pengenalan wajah, Verifikasi OTP untuk memasukkan kode OTP sebagai proses autentikasi, serta Riwayat Akses untuk mencatat aktivitas pengguna.



Gambar 2 Tampilan Web Monitoring Smart Gate

B. Hasil Pengujian Sistem

Pengujian Akurasi Visi Komputer (Vision)

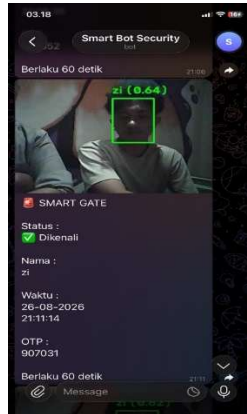
Pengujian ini mengevaluasi performa deteksi manusia oleh model YOLOv5 dan akurasi pengenalan wajah (*face recognition*) pemilik rumah menggunakan metode LBPH OpenCV pada variasi jarak serta intensitas cahaya. Batas ambang (*threshold*) pengenalan wajah diatur pada nilai matriks jarak (*distance score*) < 50 .

Hasil Pengujian Akurasi Deteksi dan Pengenalan Wajah

Tabel 1 Hasil Pengujian Akurasi Deteksi dan Pengenalan Wajah

No.	Parameter Pengujian	Jarak	Kondisi Cahaya	Hasil Deteksi Manusia (YOLOv5)	Hasil Pengenalan Wajah (OpenCV LBPH)	Status Validasi Sistem
1.	Pengujian Jarak Dekat	0.5 m	Cahaya Pagi Alami	Terdeteksi (<i>Person</i>)	Dikenali (Pemilik)	Sukses (Kirim Foto dan OTP)
2.	Pengujian Jarak Ideal	1.0 m	Cahaya Pagi Alami	Terdeteksi (<i>Person</i>)	Dikenali (Pemilik)	Sukses (Kirim Foto dan OTP)
3.	Pengujian Jarak Sedang	1.5 m	Cahaya Pagi Alami	Terdeteksi (<i>Person</i>)	Dikenali (Pemilik)	Sukses (Kirim Foto dan OTP)
4.	Pengujian Batas Maksimal	2.0 m	Cahaya Pagi Alami	Terdeteksi (<i>Person</i>)	Tidak Dikenali (<i>Unknown</i>)	Sukses (Kirim Foto + OTP)
5.	Pengujian Jarak Jauh	2.5 m	Cahaya Pagi Alami	Terdeteksi (<i>Person</i>)	Tidak Terdeteksi Wajah	Gagal Mengunci Wajah
6.	Pengujian Jarak Ekstrem	3.0 m	Cahaya Pagi Alami	Terdeteksi (<i>Person</i>)	Tidak Terdeteksi Wajah	Gagal Mengunci Wajah
7.	Pengujian Malam Hari	0.5 m	Cahaya Lampu Teras	Terdeteksi (<i>Person</i>)	Dikenali (Pemilik)	Sukses (Kirim Foto + OTP)
8.	Pengujian	1.0 m	Cahaya	Terdeteksi	Dikenali	Sukses

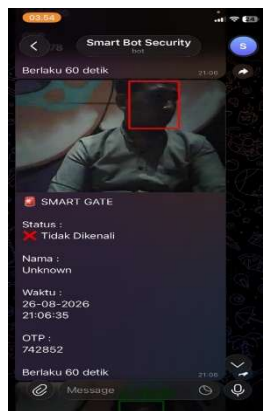
	Malam Hari		Lampu Teras	(<i>Person</i>)	(Pemilik)	(Kirim Foto + OTP)
9.	Pengujian Malam Hari	1.5 m	Cahaya Lampu Teras	Terdeteksi (<i>Person</i>)	Tidak Dikenali (<i>Unknown</i>)	Sukses (Kirim Foto + OTP)
10.	Pengujian Malam Hari	2.0 m	Cahaya Lampu Teras	Terdeteksi (<i>Person</i>)	Tidak Terdeteksi Wajah	Gagal Mengunci Wajah



Gambar 3 Hasil Pengenalan Wajah Pemilik

Sumber: Dokumentasi hasil pengujian sistem

Gambar tersebut menunjukkan ketika sistem menerima citra wajah pemilik yang telah terdaftar pada dataset. Setelah objek manusia berhasil dideteksi oleh YOLOv5, citra wajah diproses menggunakan OpenCV dengan metode Local Binary Pattern Histogram (LBPH). Sistem memberikan label identitas “Pemilik” pada wajah yang memiliki tingkat kemiripan dengan data wajah yang telah tersimpan. Hasil tersebut menunjukkan bahwa proses pengenalan wajah dapat bekerja sesuai dengan fungsi yang dirancang sebelum sistem melanjutkan ke proses autentikasi menggunakan kode OTP.



Gambar 4 Hasil Pengenalan Wajah Tidak Dikenali

Sumber: Dokumentasi hasil pengujian sistem

Pada gambar tersebut menunjukkan hasil pengujian ketika sistem mendeteksi wajah seseorang yang tidak terdapat dalam dataset wajah pemilik. Setelah proses deteksi objek manusia dilakukan oleh YOLOv5, sistem melanjutkan proses pengenalan wajah menggunakan metode LBPH. Karena wajah yang terdeteksi tidak memiliki kecocokan yang memenuhi batas pengenalan dengan dataset yang tersedia, sistem memberikan label “**Unknown**”. Pada kondisi tersebut, sistem tidak langsung membuka pagar, tetapi melanjutkan proses pengamanan dengan mengirimkan foto pengunjung dan kode OTP kepada pemilik melalui Telegram untuk proses verifikasi lebih lanjut.

Hasil Pengujian Kemampuan Klasifikasi & Ketahanan Atribut

Tabel 2 Hasil Pengujian Kemampuan Klasifikasi & Ketahanan Atribut

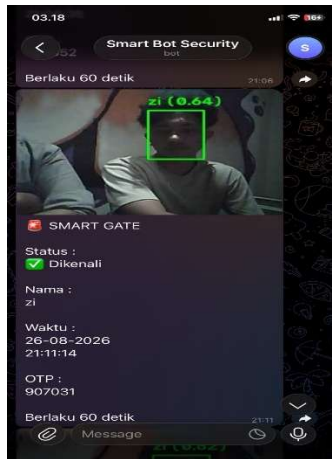
No.	Subjek Uji	Aksesoris Atribut /	Label Prediksi Sistem	Tindakan Bot Telegram	Keterangan
1.	Tamu A	Tanpa Atribut	Unknown	Kirim Foto + Kode OTP	Sesuai Kriteria
2.	Tamu B	Tanpa Atribut	Unknown	Kirim Foto + Kode OTP	Sesuai Kriteria
3.	Tamu C	Tanpa Atribut	Unknown	Kirim Foto + Kode OTP	Sesuai Kriteria
4.	Pemilik	Menggunakan Topi	Pemilik	Kirim Kode OTP	Fitur Wajah Terbuka
5.	Pemilik	Menggunakan Kacamata Hitam	Unknown	Kirim Foto + Kode OTP	Area Mata Tertutup
6	Pemilik	Menggunakan Masker Medis	Unknown	Kirim Foto + Kode OTP	Mayoritas Fitur Tertutup

Pengujian Fungsionalitas Sistem dan Konektivitas

Tabel 3 Pengujian Fungsionalitas Sistem dan Konektivitas

No	Fitur / Komponen	Skenario Pengujian	Parameter Ukur	Waktu Respon	Standar Keberhasilan	Status
1.	Notifikasi <i>Real-Time</i>	Memicu deteksi tamu tidak dikenal di depan kamera	Pengiriman foto dan token OTP ke Telegram	2.4 Detik	< 5.0 Detik	Berhasil
2.	Respon <i>Relay & Solenoid</i>	Menginputkan kode OTP valid pada antarmuka web	Perubahan mekanik kunci elektromagnetik	1.1 Detik	Aktuator langsung terbuka	Berhasil
3.	Validasi Kode OTP	Memasukkan kode OTP yang cocok dengan data <i>server</i>	Otorisasi pembukaan gerbang	0.8 Detik	Pagar terbuka otomatis	Berhasil
4.	Keamanan	Memasukkan	Penolakan	0.5	Pagar tetap	Berhasil

	Akses	kode OTP yang salah/tidak sesuai	akses fisik	Detik	terkunci, sistem <i>error</i>	
5.	<i>Fail-Safe Jaringan</i>	Memutus jaringan internet Wi-Fi secara sengaja	Respon sistem offline	-	Sistem memberikan indikator pemutusan	Berhasil



Gambar 5 Notifikasi Telegram

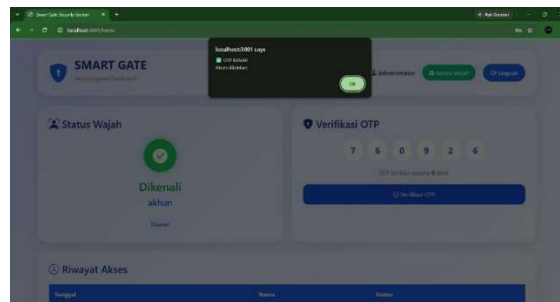
Pada gambar tersebut menunjukkan hasil pengiriman notifikasi dari sistem kepada pengguna melalui Telegram Bot. Ketika sistem mendeteksi pengunjung dan menyelesaikan proses pengenalan wajah, sistem mengirimkan informasi berupa foto hasil tangkapan kamera serta kode OTP. Kode tersebut digunakan sebagai faktor autentikasi kedua sebelum pengguna memberikan perintah pembukaan pagar melalui dashboard web monitoring. Berdasarkan hasil pengujian, notifikasi dapat diterima oleh pengguna sesuai dengan alur komunikasi yang telah dirancang.

Pengujian Fungsionalitas Dashboard Web Monitoring

Tabel 4 Hasil Pengujian Fungsionalitas Antarmuka Web (Streamlit)

No.	Parameter Pengujian	Prosedur Langkah Kerja	Hasil yang Diharapkan	Status (B/G)
1.	Akses Jaringan	Memasukkan alamat IP <i>server</i> lokal pada <i>web browser</i>	Halaman utama <i>dashboard monitoring</i> terbuka sempurna	Berhasil (B)
2.	Visualisasi Video	Mengaktifkan tombol <i>streaming</i> visual kamera	Menampilkan aliran video lancar dengan <i>delay</i> minimal	Berhasil (B)
3.	Validasi OTP Benar	Memasukkan 6 digit kode OTP sesuai notifikasi Telegram	<i>Relay</i> aktif, <i>solenoid</i> terbuka, motor bergerak	Berhasil (B)
4.	Validasi	Memasukkan digit kode	Pagar terkunci,	Berhasil

	OTP Salah	OTP acak secara sengaja	memunculkan notifikasi " <i>Kode Salah</i> "	(B)
5.	<i>Input Kosong</i>	Mengklik tombol " <i>Kirim</i> " tanpa mengisi form angka	Sistem memblokir proses, memunculkan peringatan wajib isi	Berhasil (B)
6.	Latensi Sistem	Menghitung waktu respons dari klik tombol hingga aktuator bergerak	Total waktu pemrosesan data di bawah 3.0 detik (1.7 detik)	Berhasil (B)
7.	Keamanan Kode	Menginputkan kode OTP yang sama untuk kedua kalinya (<i>expired</i>)	Sistem menolak akses karena status <i>session state</i> telah disetel ulang	Berhasil (B)



Gambar 6 Hasil Verifikasi OTP pada Web Monitoring

Gambar tersebut menunjukkan proses verifikasi kode OTP pada dashboard web monitoring. Pada kondisi kode OTP yang dimasukkan sesuai dengan kode yang diberikan oleh sistem, proses autentikasi dinyatakan berhasil sehingga relay aktif, solenoid door lock terbuka, dan motor penggerak menjalankan mekanisme pembukaan pagar. Sebaliknya, apabila kode OTP yang dimasukkan tidak sesuai, sistem menolak permintaan akses dan mempertahankan pagar dalam kondisi terkunci. Hasil pengujian tersebut menunjukkan bahwa mekanisme verifikasi OTP telah bekerja sesuai dengan rancangan sistem dan mampu membedakan antara permintaan akses yang valid dan tidak valid.

C. Pembahasan Analitis

Berdasarkan hasil pengujian terstruktur yang telah dipaparkan, terdapat beberapa poin pembahasan ilmiah krusial mengenai performa integrasi sistem pagar pintar (*smart gate system*) ini:

- 1) Analisis Deteksi Objek Real-Time (YOLOv5): Model Deep Learning YOLOv5 terbukti sangat tangguh dalam menyaring keberadaan objek manusia (*person*). Pada seluruh variasi jarak (0.5 meter hingga 3.0 meter) baik siang maupun malam hari, model ini secara konsisten mampu mendeteksi keberadaan manusia dengan tingkat akurasi tinggi. Hal ini berhasil meminimalkan kesalahan deteksi (*false alarm*) yang

biasanya terjadi pada sensor gerak inframerah konvensional (seperti sensor PIR) akibat gangguan eksternal seperti pergerakan dedaunan atau hewan peliharaan.

- 2) Keterbatasan Jarak dan Cahaya pada Metode Face Recognition (OpenCV LBPH): Berbeda dengan YOLOv5 yang stabil di berbagai jarak, performa algoritma pengenalan wajah LBPH sangat dipengaruhi oleh jarak subjek dan intensitas pencahayaan alami di lingkungan luar. Jarak ideal bagi kamera ESP32-CAM (sensor OV2640 2D) untuk mengenali wajah pemilik secara tepat dengan tingkat *confidence score* terbaik (<50) berada pada rentang 0.5 meter hingga 1.5 meter. Ketika subjek berada pada jarak lebih dari 2.0 meter, kerapatan piksel wajah menurun secara drastis sehingga sistem mengklasifikasikannya sebagai objek tidak dikenal (*unknown*). Begitu pula pada malam hari, penurunan intensitas cahaya menyebabkan reduksi detail tekstur wajah, yang mengakibatkan batasan pengenalan wajah menyusut hingga jarak maksimal 1.0 meter saja.
- 3) Ketahanan Atribut Visual Terhadap Serangan Pemalsuan (*Spoofing Attack*): Hasil pengujian pada Tabel 2 memperlihatkan bahwa penggunaan aksesoris yang menutupi komponen utama wajah (seperti kacamata hitam dan masker medis) menyebabkan nilai matriks jarak LBPH membengkak melewati ambang batas, sehingga sistem otomatis merubah label identitas menjadi *unknown*. Kondisi ini awalnya dianggap sebagai kelemahan dalam sistem biometrik murni. Namun, dalam arsitektur penelitian ini, celah tersebut berhasil diatasi secara mutlak melalui metode pengamanan ganda *Two-Factor Authentication* (2FA).
- 4) Efektivitas Mekanisme Otentikasi Ganda (2FA via OTP & Telegram): Implementasi token dinamis *One-Time Password* (OTP) terbukti krusial dalam memperkuat keamanan gerbang. Ketika wajah pemilik rumah gagal dikenali karena faktor aksesoris, ataupun jika terjadi upaya peretasan visual menggunakan foto cetak dua dimensi milik pemilik rumah (*spoofing attack*), sistem tidak akan pernah membuka pagar secara otomatis. Sistem akan menangguhkan akses mekanis dan langsung mengalihkan prosedur keamanan dengan mengirimkan notifikasi peringatan visual (foto tangkapan kamera) serta 6 digit kode OTP dinamis menuju aplikasi Telegram pemilik rumah.
- 5) Analisis Latensi dan Manajemen Sesi Web: Dari segi performa komputasi, integrasi backend menggunakan skrip Python tergolong sangat responsif. Rata-rata waktu

pemrosesan dari mulai input kode OTP pada *dashboard* Streamlit hingga penarikan kunci *solenoid* secara fisik hanya membutuhkan waktu 1.7 detik. Fitur penghapusan data otomatis (*session reset*) pasca-verifikasi terbukti efektif mengamankan sistem dari serangan siber berupa pemutaran ulang kode (*replay attack*), karena satu token OTP unik yang telah dibangkitkan hanya valid untuk satu kali siklus eksekusi dalam jendela waktu terbatas.

5. KESIMPULAN DAN SARAN

Algoritma YOLOv5 berhasil diimplementasikan secara optimal pada sistem pengawasan berbasis ESP32-CAM untuk mendeteksi kehadiran objek manusia secara *real-time* di area pagar. Model ini terbukti konsisten menyaring objek manusia pada jarak pengawasan hingga 3.0 meter, sehingga efektif menghilangkan risiko kesalahan deteksi (*false alarm*) dari objek non-manusia. Integrasi metode *Face Recognition* berbasis OpenCV (algoritma LBPH) dengan mekanisme keamanan ganda *Two-Factor Authentication* (2FA) via *One-Time Password* (OTP) telah berhasil dibangun dengan keandalan tinggi. Sistem ini mampu mengidentifikasi pemilik rumah pada jarak ideal 0.5–1.5 meter dengan *confidence score* matriks jarak < 50 , serta mampu memitigasi risiko serangan pemalsuan identitas biometrik (*spoofing attack*) secara mutlak dengan mewajibkan validasi token dinamis. Sistem notifikasi otomatis berbasis *Telegram Bot API* dan *Dashboard Monitoring* (Streamlit) telah berhasil dirancang dan berfungsi secara sinkron. Sistem mampu mengirimkan notifikasi teks disertai lampiran foto pengunjung dari area pagar menuju *smartphone* pemilik rumah secara *real-time* dengan rata-rata latensi pengiriman data yang sangat responsif, yaitu sebesar 2.4 detik. Proses verifikasi akhir melalui *interface* web terbukti aman karena didukung sistem penghapusan token otomatis (*session state reset*) demi mencegah kebocoran otorisasi akses.

DAFTAR REFERENSI

- Faturrachman, M., & Yustiana, I. (2021). Faturrachman, M., & Yustiana, I. *Jurnal Teknik Informatika Unika St. Thomas (JTIUST)*, 6(2), 379–385.
- Hasibuan, A. Z., & Asih, S. (2023). Sistem Keamanan Pintu Rumah dengan Sidik Jari Berbasis Internet of Things (IOT). *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKSTRA)*, 5(1).
- Ilham, A., Mashudi, A., & Prihanto, A. (2024). Rancang Bangun Sistem Keamanan Pintu Menggunakan Metode Two-Factor Authentication. *Journal of Informatics and Computer Science*, 6.

- Kusuma, H. A., Wijaya, S. B., & Nusyirwan, D. (2023). SISTEM KEAMANAN RUMAH BERBASIS ESP32-CAM DAN TELEGRAM SEBAGAI NOTIFIKASI. *Infotronik : Jurnal Teknologi Informasi Dan Elektronika*, 8(1), 30. <https://doi.org/10.32897/infotronik.2023.8.1.2291>
- Renhat Ade Prayogo, M., Kingkin Sulistiana, D., & Eko Febrianto, Y. (2025). Sistem Absensi Menggunakan Open CV Berbasis Pengenalan Wajah. *PROSIDING SEMINAR NASIONAL TEKNOLOGI DAN SAINS (SNTS)*, 4(Januari), 713–719.
- Riyanto, J., Nurlaila, F., Haerudin, H., & Jarastino, B. T. (2021). Rancang Bangun Sistem Monitoring Ruang Kelas Berbasis Internet of Things pada Universitas Pamulang. *Jurnal Informatika Universitas Pamulang*, 5(4), 483. <https://doi.org/10.32493/informatika.v5i4.7018>
- Rumere, S., & Manullang, V. (2024). Rancang Bangun Sistem Keamanan Rumah Berbasis Internet Of Things (IoT) Dengan Menggunakan Sensor PIR Dan ESP32-CAM. *Jurnal Teknologi Informasi (JTI)*, 12(1), 9–16.
- Santoso, B., & Kristianto, R. P. (2020). Implementasi Penggunaan OPENCV Pada Face Recognition Untuk Sistem Presentasi Perkuliahan Mahasiswa. *SISTEMASI: Jurnal Sistem Informasi*, 9(2), 352–361.
- Syabibi, M. K., & Subari, A. (2016). Rancang Bangun Sistem Monitoring Keamanan Rumah Berbasis Web Menggunakan Raspberry PI B+ Sebagai Server Dan Media Kontrol. *Gema Teknologi*, 19(1), 22–29.
- Yusup Efendi, M., Wulanningrum, R., & Bagus Setiawan, A. (2024). Rancang Bangun Sistem Deteksi Manusia dengan YOLO pada video CCTV. *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi)*, 1149–1154.