

Integrasi Kamera dan YOLOv5 pada Sistem Keamanan *Safety Box* Berbasis IoT

Kgs.M.Dian Akbar Rizky Tarmizi^{1*}, Ahmad Taqwa¹, Abdul Rakhman¹

¹ Sarjana Terapan Teknik Telekomunikasi, Jurusan Teknik Elektro, Politeknik Negeri Sriwijaya
Jl. Sriwijaya Negara, Bukit Besar, Palembang, Sumatera Selatan 30139
E-mail: dianakbar21@gmail.com

Naskah Masuk: 26 Juni 2025; Diterima: 04 Juli 2025; Terbit: 31 Agustus 2025

ABSTRAK

Abstrak - Peningkatan keamanan terhadap akses fisik menjadi isu penting dalam pengembangan sistem berbasis *Internet of Things* (IoT), khususnya pada aplikasi autentikasi biometrik. Penelitian ini bertujuan untuk mengembangkan sistem keamanan *safety box* berbasis IoT yang mengintegrasikan kamera digital, algoritma YOLOv5 untuk autentikasi wajah *real-time*, dan mikrokontroler ESP32 sebagai pengendali aktuator pengunci elektronik. Sistem ini dirancang untuk mengenali wajah secara lokal tanpa ketergantungan pada layanan *cloud* guna meningkatkan efisiensi, privasi, dan kecepatan respons. Evaluasi dilakukan melalui pengujian fungsional dan analisis metrik performa, termasuk *precision*, *recall*, *confusion matrix*, dan *mean Average Precision* (mAP). Hasil pengujian menunjukkan bahwa sistem mampu mengidentifikasi wajah terdaftar dan menolak wajah yang tidak terdaftar secara akurat, dengan nilai mAP sebesar 66,3% pada *threshold* IoU 0,5. Sistem juga menunjukkan ketahanan terhadap variasi pencahayaan, sudut pandang, dan ekspresi wajah. Temuan ini menunjukkan bahwa kombinasi YOLOv5 dan ESP32 dapat diterapkan secara efektif dalam sistem autentikasi wajah *real-time* untuk aplikasi keamanan berbasis IoT berskala kecil hingga menengah.

Kata kunci: *Safety Box*, Sistem Keamanan, Autentikasi Wajah, *Internet of Things*, YOLOv5, ESP32

ABSTRACT

Abstract - Improving physical access security has become a crucial issue in the development of *Internet of Things* (IoT)-based systems, particularly in biometric authentication applications. This research aimed to develop a security system for a *safety box* based on IoT by integrating a digital camera, the YOLOv5 algorithm for *real-time* facial authentication, and an ESP32 microcontroller to control the electronic locking actuator. The system had been designed to recognize faces locally without relying on *cloud* services in order to enhance efficiency, privacy, and response speed. The evaluation was carried out through functional testing and performance metrics analysis, including *precision*, *recall*, *confusion matrix*, and *mean average precision* (mAP). The test results showed that the system was capable of accurately identifying registered faces and rejecting unregistered ones, with an mAP score of 66.3% at an IoU threshold of 0.5. The system had also demonstrated robustness against variations in lighting, viewing angles, and facial expressions. These findings indicated that the integration of YOLOv5 and ESP32 could be effectively applied in *real-time* facial authentication systems for small-to medium-scale IoT-based security applications.

Keywords: *safety box*, security system, facial authentication, *Internet of Things*, YOLOv5, ESP32

Copyright © 2025 Jurnal Teknik Elektro dan Komputasi (ELKOM)

1. PENDAHULUAN

Keamanan terhadap aset-aset berharga seperti uang tunai, dokumen penting, dan barang bernilai lainnya menjadi isu yang semakin krusial di era digital saat ini. Meskipun brankas atau *safety box* masih banyak digunakan sebagai media penyimpanan yang dianggap aman, sebagian besar sistem konvensional tersebut masih mengandalkan mekanisme kunci fisik atau kombinasi angka statis yang rentan terhadap teknik pembobolan secara manual maupun *bypass* elektronik[1]. Selain itu, sistem keamanan tradisional umumnya tidak memiliki kemampuan pemantauan secara waktu nyata (*real-time monitoring*), sehingga pengguna tidak mendapatkan notifikasi langsung apabila terjadi akses ilegal[2]. Seiring berkembangnya teknologi, pendekatan berbasis *Internet of Things* (IoT) mulai diterapkan untuk meningkatkan keamanan, seperti melalui integrasi kamera, mikrokontroler ESP32, dan aktuator pengunci seperti *solenoid*, sehingga sistem

dapat mengidentifikasi pengguna serta mengendalikan akses secara otomatis[3]. Dalam hal deteksi wajah, algoritma *You Only Look Once* versi 5 (YOLOv5) telah terbukti memberikan performa deteksi waktu nyata yang efisien dan akurat, termasuk pada perangkat edge yang memiliki sumber daya terbatas[4][5].

Berbagai penelitian sebelumnya telah menunjukkan efektivitas integrasi antara IoT dan metode *deep learning* untuk meningkatkan sistem keamanan, misalnya pada penerapan *smart lock* berbasis Raspberry Pi[6], serta sistem pemantauan keamanan menggunakan kombinasi YOLOv5 dan IoT[7]. Namun, penelitian masih terbatas pada pengenalan objek umum tanpa mengintegrasikan autentikasi wajah dengan kendali akses otomatis berbasis *Internet of Things* secara menyeluruh. Selain itu, banyak sistem masih mengandalkan layanan *cloud*, yang memiliki tantangan tersendiri dalam hal privasi dan latensi transmisi. Di sisi lain, evaluasi performa deteksi seperti *precision*, *recall*, *F1-score*, dan *mean Average Precision* (mAP) umumnya belum dilakukan secara menyeluruh di kondisi nyata seperti pencahayaan rendah atau sudut wajah yang beragam[8].

Penelitian ini bertujuan mengembangkan sistem keamanan *safety box* berbasis IoT dengan mengintegrasikan kamera, model YOLOv5 untuk autentikasi wajah waktu nyata, serta modul ESP32 sebagai pengendali aktuator kunci elektronik. Sistem ini juga dirancang agar dapat menampilkan hasil deteksi melalui antarmuka web lokal tanpa ketergantungan terhadap layanan *cloud*. Inovasi utama dari penelitian ini terletak pada penggunaan algoritma YOLOv5 untuk proses autentikasi wajah *real-time*, pengendalian perangkat keras secara otomatis melalui komunikasi IoT, serta evaluasi performa sistem secara kuantitatif dengan metrik yang komprehensif. Dengan pendekatan ini, penelitian tidak hanya memberikan solusi praktis terhadap kebutuhan keamanan aset, tetapi juga memberikan kontribusi ilmiah dengan menyediakan sistem yang dapat diuji, direproduksi, dan diadaptasi untuk aplikasi serupa di masa depan.

2. KAJIAN PUSTAKA

Bagian ini membahas teori dan teknologi yang digunakan dalam pengembangan sistem keamanan berbasis pengenalan wajah, termasuk *Internet of Things* (IoT), perangkat ESP32, dan algoritma YOLOv5. Kajian juga mencakup beberapa penelitian terdahulu yang relevan untuk memberikan dasar dan perbandingan terhadap pengembangan sistem yang dilakukan dalam penelitian ini.

2.1. Sistem Keamanan Berbasis IoT

Sistem keamanan modern merupakan integrasi perangkat lunak dan perangkat keras yang dirancang untuk mencegah akses tidak sah terhadap aset penting. Salah satu media yang masih sering digunakan adalah brankas atau *safety box*. Namun, sistem konvensional dengan kunci fisik atau kombinasi angka mulai dianggap kurang aman karena rawan terhadap manipulasi dan pembobolan[9]. Untuk menjawab tantangan tersebut, kini dikembangkan *smart safety box* yang secara otomatis mengontrol akses dengan menggunakan teknologi biometrik dan *Internet of Things* (IoT)[10]. Penelitian dalam [11] mengembangkan sistem pengamanan pintu menggunakan RFID dan ESP8266 berbasis IoT, di mana pengguna dapat membuka kunci secara otomatis melalui otentikasi identitas. Sementara itu, [12] merancang *smart locker* berbasis fingerprint dan NodeMCU ESP8266, yang mampu mengontrol pintu loker secara otomatis dan terhubung ke jaringan lokal. Penelitian lain dalam [13] mengembangkan sistem pengamanan kendaraan dengan otentikasi wajah berbasis Raspberry Pi dan kamera, yang menunjukkan efektivitas biometrik dalam mencegah akses ilegal.

2.2. *Internet of Things* (IoT) dalam Sistem Keamanan

Internet of Things (IoT) memungkinkan berbagai perangkat fisik saling terhubung melalui jaringan untuk bertukar data dan mengontrol tindakan secara otomatis. Dalam sistem keamanan, IoT digunakan untuk mengintegrasikan sensor, kamera, dan aktuator seperti *solenoid door lock* untuk mendeteksi dan mengontrol akses secara *real-time*[14]. Salah satu perangkat IoT yang sering digunakan adalah ESP32, karena ukurannya kecil dan telah mendukung Wi-Fi serta Bluetooth, sehingga cocok untuk sistem keamanan berbasis lokal tanpa tergantung *cloud*[15]. ESP32 juga dinilai lebih efisien dari sisi konsumsi daya dan pemrosesan jika dibandingkan dengan mikrokontroler sebelumnya seperti Arduino Uno atau NodeMCU ESP8266. Dengan kemampuan *dual-core* dan kompatibilitas terhadap *MicroPython* maupun Arduino IDE, ESP32 menjadi solusi ideal untuk pengembangan sistem keamanan mandiri dan terhubung.

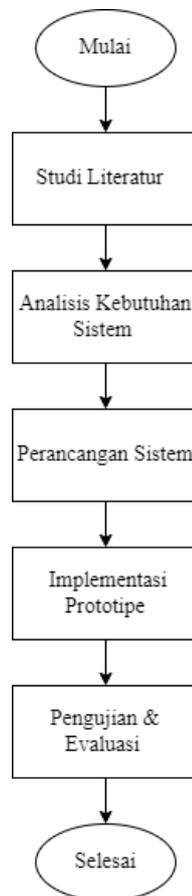
2.3. Deteksi Wajah dan YOLOv5

Teknologi *face recognition* digunakan untuk mengidentifikasi individu berdasarkan karakteristik wajah. Salah satu model populer yang digunakan dalam sistem *real-time* adalah *You Only Look Once* versi 5 (YOLOv5), yang mampu mendeteksi wajah secara cepat dan akurat dalam satu proses deteksi[16]. Model ini dibangun dengan arsitektur *Convolutional Neural Network* (CNN) yang ringan dan dapat berjalan pada perangkat seperti Raspberry Pi atau ESP32-CAM. YOLOv5 juga efektif digunakan dalam kondisi pencahayaan yang rendah maupun sudut wajah yang bervariasi[17].

Penelitian dalam [18] mengimplementasikan YOLOv5 untuk sistem monitoring keamanan rumah berbasis IoT, yang mampu mendeteksi keberadaan manusia secara *real-time* dan mengirim notifikasi melalui aplikasi Telegram. Selain itu, studi dalam [19] menunjukkan bahwa penggunaan YOLOv5 untuk otentikasi wajah memberikan hasil akurasi yang baik meskipun dijalankan pada perangkat *edge* dengan keterbatasan daya komputasi. Penggunaan YOLOv5 pada sistem berbasis ESP32-CAM juga telah diuji dalam [20], dengan hasil menunjukkan bahwa model dapat dioptimalkan untuk deteksi wajah lokal tanpa koneksi *cloud*, meskipun dengan keterbatasan jumlah wajah yang dapat dikenali secara simultan.

3. METODE PENELITIAN

Metode penelitian ini menggunakan teknik rekayasa prototipe untuk membangun dan menerapkan sistem keamanan yang menggunakan pengenalan wajah dan terhubung ke *Internet of Things* (IoT). Sistem dirancang untuk dapat mengidentifikasi pengguna melalui citra wajah secara *real-time*, mengendalikan aktuator pengunci menggunakan mikrokontroler ESP32, serta memberikan umpan balik berupa perekaman video dan tampilan web antarmuka lokal. Tahapan penelitian ini digambarkan dalam diagram alir berikut:



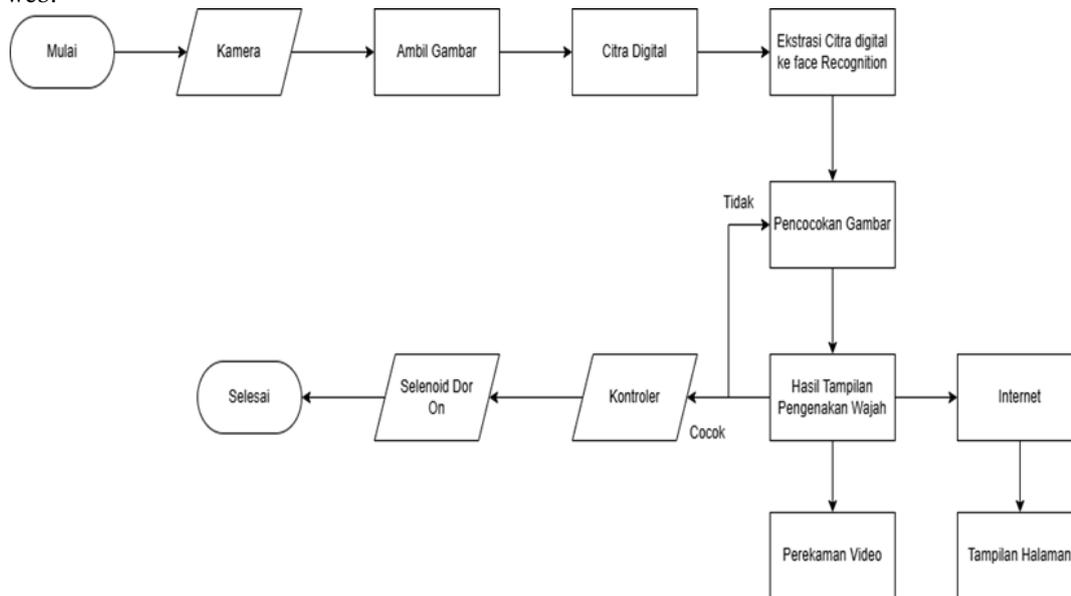
Gambar 1. Diagram Alir Tahapan Penelitian

Berdasarkan gambar 1 diatas, metode penelitian ini diawali dengan studi literatur untuk memperoleh dasar teori dan teknologi terkait. Selanjutnya dilakukan analisis kebutuhan sistem, perancangan perangkat keras dan lunak, serta pengembangan prototipe sistem keamanan berbasis pengenalan wajah dan IoT. Setelah implementasi selesai, sistem diuji dan dievaluasi guna menilai fungsionalitas dan keandalannya.

3.1 Diagram Alir Sistem

Diagram alir sistem memberikan gambaran proses kerja utama mulai dari inialisasi sistem hingga aktivasi aktuator. Sistem dimulai dengan pengambilan gambar oleh kamera, kemudian citra dikonversi menjadi data digital untuk diproses menggunakan algoritma deteksi wajah. Jika wajah yang dikenali sesuai dengan data yang tersimpan, maka sistem akan mengaktifkan *solenoid* untuk membuka kunci.

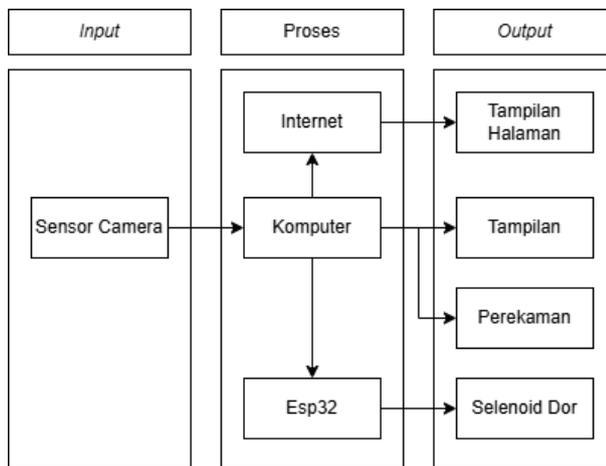
Selain itu, sistem juga melakukan perekaman video dan menampilkan hasilnya melalui antarmuka web.



Gambar 2. Diagram Alir Sistem Keamanan Berbasis Pengenalan Wajah

3.2 Diagram Blok Sistem

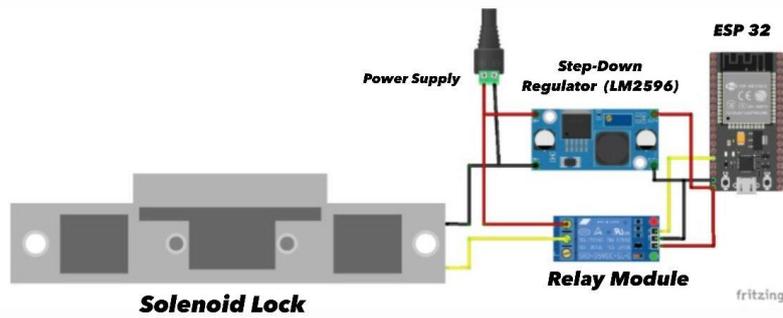
Diagram blok sistem secara umum menggambarkan hubungan antara perangkat input, proses, dan output yang bekerja secara terintegrasi untuk mendukung fungsi keamanan brankas berbasis IoT. Kamera berfungsi sebagai sensor input untuk menangkap citra wajah pengguna. Proses utama dilakukan oleh komputer dan mikrokontroler ESP32 yang saling terhubung untuk menjalankan deteksi wajah, pengendalian aktuator, dan pengiriman data ke internet. Hasil dari proses ditampilkan melalui berbagai media *output* seperti halaman web, rekaman video, dan kontrol *solenoid*, seperti ditunjukkan pada Gambar 3.



Gambar 3. Diagram Blok Sistem Keamanan *Safety box*

3.3 Rancangan Elektrikal Sistem

Perancangan elektrikal sistem melibatkan koneksi antar perangkat keras seperti kamera, modul relay, ESP32, dan *solenoid*. Kamera digunakan untuk menangkap citra wajah, ESP32 menerima perintah melalui komunikasi nirkabel, dan relay berfungsi untuk mengaktifkan *solenoid* sebagai aktuator pengunci pintu brankas. Skema koneksi antar komponen tersebut ditunjukkan pada Gambar 4.

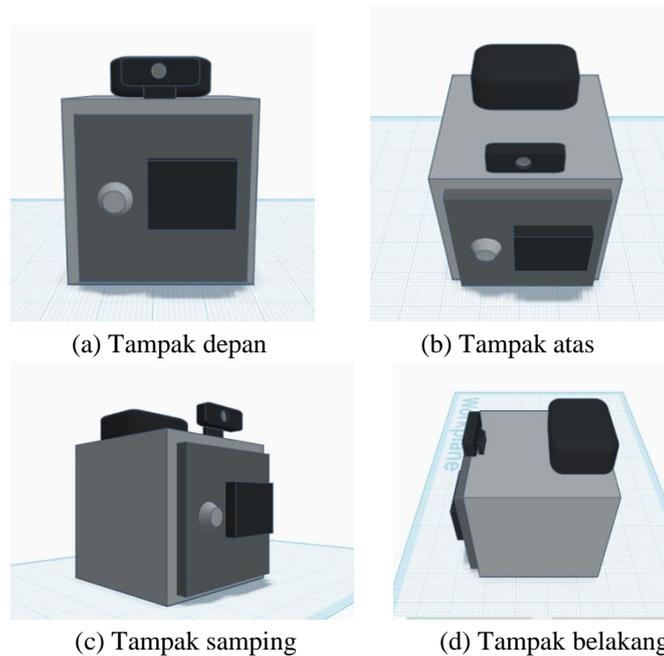


Gambar 4. Rangkaian Elektrikal Sistem

Gambar 4 menunjukkan rancangan elektrikal sistem yang terdiri dari ESP32, modul relay, modul step-down LM2596, dan *solenoid lock*. Daya disuplai dari adaptor melalui terminal konektor, kemudian diturunkan tegangannya oleh modul *step-down* sebelum dialirkan ke ESP32 dan komponen lainnya. ESP32 berfungsi sebagai pusat kendali dan mengaktifkan relay melalui sinyal GPIO. Relay kemudian mengalirkan arus ke solenoid untuk membuka kunci pintu secara otomatis. Ketika tidak aktif, relay memutus arus, dan mekanisme penguncian kembali ke posisi semula.

3.4 Desain 3D Sistem

Untuk menggambarkan implementasi fisik dari sistem yang dikembangkan, dilakukan pemodelan desain 3D menggunakan perangkat lunak berbasis CAD. Desain ini menampilkan komponen utama seperti kamera, bodi brankas, tombol fisik, dan ruang *solenoid lock*.



Gambar 5. Desain 3D *Safety box* Berbasis Kamera dan IoT

Keterangan:

- (a) Tampak depan memperlihatkan kamera di bagian atas, tombol fisik di sisi kiri panel depan, serta pintu brankas di sebelah kanan.
- (b) Tampak atas menampilkan posisi kamera, tombol, dan pintu dilihat dari sudut atas.
- (c) Tampak samping menunjukkan dimensi samping brankas serta posisi kamera, tombol, dan pintu yang menonjol.
- (d) Tampak belakang memperlihatkan lokasi solenoid lock dan bagian belakang dari modul kamera.

3.5 Pengujian dan Evaluasi Sistem

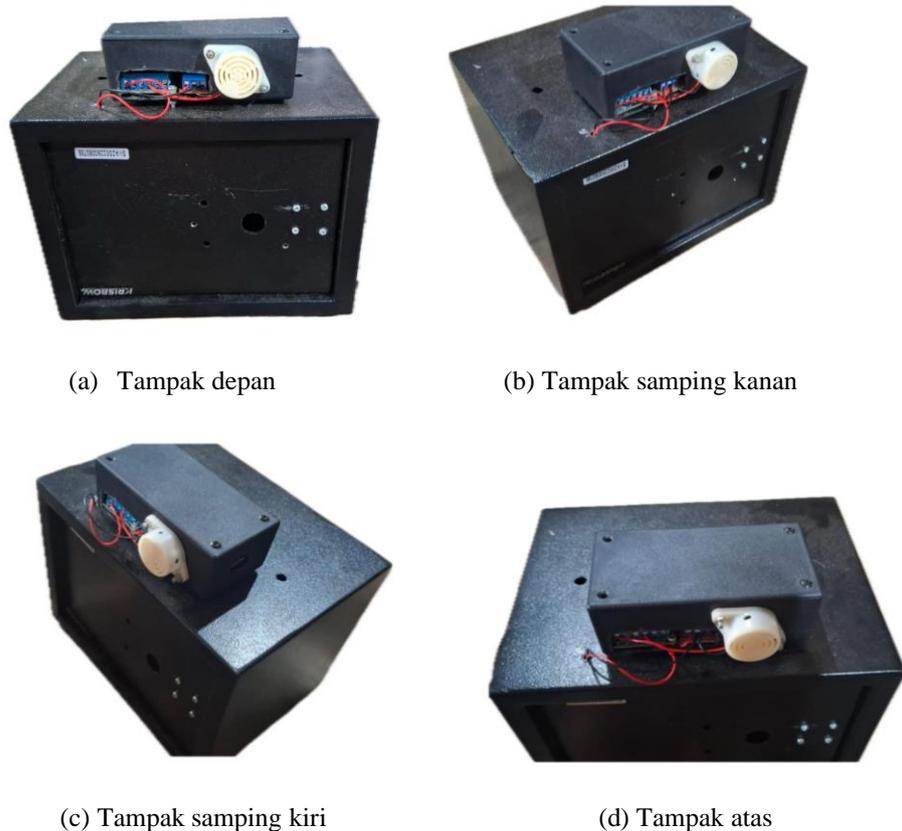
Pengujian sistem dilakukan untuk menilai performa model deteksi wajah serta keandalan mekanisme autentikasi dalam kondisi operasional yang menyerupai situasi nyata. Pengujian dilaksanakan dalam dua skenario utama, yaitu ketika wajah pengguna terdaftar (dikenali) dan ketika wajah tidak terdaftar (tidak dikenali). Dataset pengujian divariasikan berdasarkan aspek pencahayaan, sudut pengambilan gambar, serta ekspresi wajah, guna mensimulasikan beragam kemungkinan yang terjadi dalam penggunaan aktual. Evaluasi performa dilakukan dengan menerapkan sejumlah metrik yang relevan terhadap model deteksi berbasis YOLOv5, meliputi *confusion matrix*, *precision*, *recall*, dan *mean Average Precision (mAP)*. Selain evaluasi kuantitatif, pengamatan visual terhadap hasil deteksi juga dilakukan melalui tampilan kamera secara langsung. Seluruh proses pengujian telah terintegrasi dengan perangkat keras sistem, seperti kamera digital dan mikrokontroler ESP32, untuk memastikan bahwa hasil evaluasi merepresentasikan kinerja sistem secara menyeluruh dan autentik.

4. HASIL DAN PEMBAHASAN

Bagian ini memaparkan hasil implementasi sistem keamanan *safety box* berbasis IoT dengan autentikasi wajah menggunakan algoritma YOLOv5, serta evaluasi performa model deteksi melalui berbagai metrik pengukuran. Pembahasan dilakukan secara terpisah antara aspek implementasi perangkat keras dan perangkat lunak, serta aspek evaluasi algoritmik yang mendasari keandalan sistem.

4.1 Implementasi Sistem Keamanan *Safety Box* Berbasis IoT

Sistem yang dikembangkan mengintegrasikan kamera digital, model deteksi wajah YOLOv5, dan mikrokontroler ESP32 untuk mengontrol aktuator kunci elektronik (*solenoid*). Proses autentikasi dilakukan secara lokal melalui citra wajah yang ditangkap oleh kamera, kemudian diklasifikasikan oleh model *deep learning* sebelum diteruskan ke ESP32 untuk eksekusi perintah penguncian atau pembukaan brankas. Gambar fisik sistem ditunjukkan pada Gambar 6.



Gambar 6. Prototipe Sistem *Safety Box* dengan Integrasi Kamera dan ESP32

Keterangan:

- (a) Tampak depan menampilkan modul kamera yang terpasang pada bagian atas brankas, *solenoid lock* sebagai aktuator pengunci elektronik, serta permukaan pintu brankas yang berfungsi sebagai akses utama sistem.

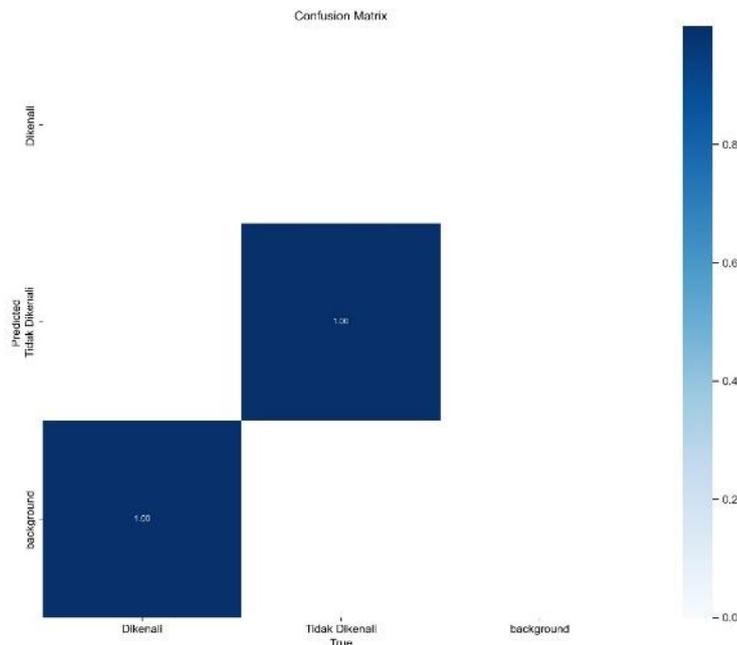
- (b) Tampak samping kanan memperlihatkan posisi menonjol dari *solenoid lock* dan dudukan kamera, serta jalur kabel yang menghubungkan modul kamera dan *solenoid* ke mikrokontroler ESP32.
- (c) Tampak samping kiri menunjukkan sisi kiri brankas yang mencakup bagian samping dari dudukan kamera, serta memperlihatkan struktur *casing* sistem secara keseluruhan.
- (d) Tampak atas menggambarkan konfigurasi keseluruhan komponen di bagian atas brankas, termasuk modul kamera, ESP32, rangkaian kabel jumper, dan posisi pemasangan perangkat pada dudukan khusus.

4.2 Evaluasi Kinerja Model YOLOv5 dalam Deteksi Wajah

Evaluasi dilakukan untuk mengukur keandalan model YOLOv5 dalam mengenali wajah pengguna pada sistem keamanan berbasis IoT. Pengujian dilakukan menggunakan dataset yang telah divariasikan dari sisi pencahayaan, sudut wajah, dan ekspresi, guna mensimulasikan kondisi operasional nyata. Tiga aspek evaluasi utama yang dianalisis adalah *confusion matrix*, *precision-recall curve* (PR curve), dan visualisasi hasil deteksi langsung.

4.2.1 Confusion Matrix

Evaluasi awal performa model dilakukan menggunakan *confusion matrix*, yang merepresentasikan jumlah prediksi benar dan salah dari dua kategori utama, yaitu wajah dikenali dan tidak dikenali oleh sistem. Hasil *confusion matrix* ditunjukkan pada Gambar 7.



Gambar 7. *Confusion Matrix* Deteksi Wajah oleh Model YOLOv5

Sebagai pelengkap visualisasi, Tabel 1 menyajikan bentuk numerik dari *confusion matrix* tersebut.

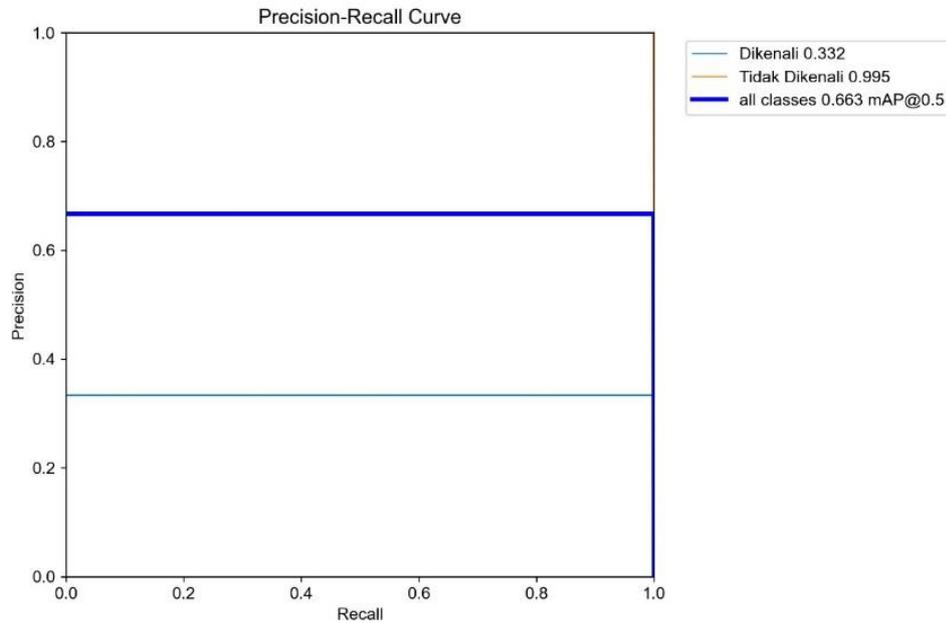
Tabel 1. *Confusion Matrix* Deteksi Wajah oleh Model YOLOv5

	Prediksi: Dikenali	Prediksi: Tidak Dikenali
Aktual: Dikenali	1.00	0.00
Aktual: Tidak Dikenali	0.00	1.00

Berdasarkan Gambar 6 dan Tabel 1, sistem menunjukkan hasil klasifikasi yang optimal, di mana seluruh data uji berhasil diprediksi dengan benar. Seluruh nilai diagonal utama pada *confusion matrix* mencapai 1.00, yang mengindikasikan akurasi sempurna untuk kategori wajah dikenali maupun tidak dikenali. Tidak ditemukan kesalahan klasifikasi berupa *false positive* maupun *false negative*, sehingga model YOLOv5 terbukti mampu membedakan wajah pengguna dan non-pengguna secara presisi dalam sistem autentikasi.

4.2.2 Precision-Recall Curve dan mAP

Evaluasi selanjutnya dilakukan menggunakan *precision-recall curve* untuk mengukur performa model dalam mendeteksi wajah terdaftar dan membedakannya dari latar belakang. Nilai *mean Average Precision* (mAP) dihitung pada *threshold* IoU 0.5 sebagai indikator akurasi keseluruhan. Hasil evaluasi tersebut ditunjukkan pada Gambar 8.



Gambar 8. Precision-Recall Curve dan Nilai mAP Model YOLOv5

Tabel 2 berikut menyajikan nilai precision dan recall masing-masing kelas berdasarkan evaluasi PR Curve, serta nilai mAP keseluruhan pada *threshold* IoU 0.5.

Tabel 2. Rekapitulasi Precision dan mAP per Kelas

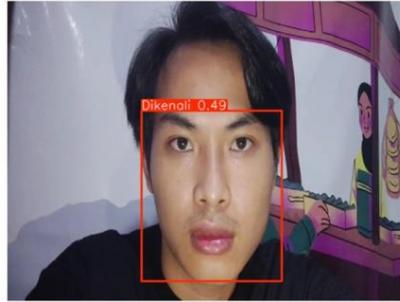
Kelas	Precision	Recall	mAP@0.5
Dikenali	0.332	1.000	–
Tidak Dikenali	0.995	1.000	–
Rata-rata (mAP)	–	–	0.663

Hasil evaluasi menunjukkan bahwa kelas "Tidak Dikenali" memiliki nilai presisi yang sangat tinggi, menunjukkan kemampuan model dalam menghindari kesalahan dalam mengklasifikasikan wajah yang tidak terdaftar. Sebaliknya, kelas "Dikenali" memiliki nilai precision sebesar 0,332, mengindikasikan bahwa model lebih selektif dan cenderung berhati-hati dalam mengenali wajah pengguna yang terdaftar. Secara keseluruhan, nilai *mean Average Precision* (mAP) sebesar 66,3% pada *threshold* IoU 0.5 menunjukkan bahwa model memiliki tingkat akurasi yang cukup baik dalam mendeteksi objek dengan syarat tumpang tindih area prediksi minimal 50% terhadap area sebenarnya (*ground truth*). Nilai ini menunjukkan bahwa sistem dapat diandalkan untuk deteksi wajah dalam konteks autentikasi, meskipun performa untuk kelas pengguna spesifik masih dapat ditingkatkan.

4.2.3 Visualisasi Hasil Deteksi Akhir

Untuk mengevaluasi performa sistem secara visual, dilakukan pengamatan terhadap hasil deteksi wajah pada skenario nyata melalui *streaming* kamera. Gambar yang ditampilkan menunjukkan respons sistem terhadap wajah pengguna terdaftar dan tidak terdaftar.

Streaming Kamera



Streaming Kamera



Gambar 9. Hasil Deteksi Wajah yang Dikenali oleh Sistem

Berdasarkan visualisasi pada Gambar 9, sistem mampu mengidentifikasi wajah pengguna yang terdaftar dengan *confidence* sebesar 0,49 dan 0,41. Meskipun nilai *confidence* tergolong sedang, model tetap memberikan klasifikasi yang benar sebagai “Dikenali”, yang kemudian memicu aktivasi aktuator pengunci sesuai prosedur autentikasi.

Streaming Kamera



Streaming Kamera



Gambar 10. Hasil Deteksi Wajah yang Tidak Dikenali oleh Sistem

Sebaliknya, Gambar 10 menunjukkan respons sistem terhadap wajah yang tidak terdaftar. *Confidence* yang dihasilkan masing-masing sebesar 0,27 dan 0,44, di mana keduanya diklasifikasikan sebagai “Tidak Dikenali”. *Confidence* yang relatif rendah menunjukkan tingkat ketidakpastian model dalam mencocokkan wajah tersebut dengan data pelatihan, dan hasil ini sesuai dengan kebijakan sistem untuk menolak akses apabila *confidence* berada di bawah ambang batas tertentu. Temuan ini mengindikasikan bahwa sistem tidak hanya mengandalkan deteksi keberadaan wajah, tetapi juga mengintegrasikan *confidence score* sebagai parameter pengambilan keputusan, yang pada akhirnya meningkatkan keakuratan dan keandalan sistem autentikasi wajah secara keseluruhan.

5. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem keamanan *safety box* berbasis IoT yang mengintegrasikan kamera digital, algoritma YOLOv5 untuk autentikasi wajah waktu nyata, dan mikrokontroler ESP32 sebagai pengendali aktuator elektronik. Sistem mampu beroperasi secara mandiri tanpa ketergantungan pada layanan *cloud*, serta menunjukkan performa tinggi dengan akurasi sempurna pada *confusion matrix* dan nilai mAP sebesar 66,3% pada threshold IoU 0.5. Sistem juga terbukti andal terhadap variasi pencahayaan, sudut pandang, dan ekspresi wajah, serta memanfaatkan *confidence score* sebagai dasar pengambilan keputusan autentikasi.

Meskipun telah diuji langsung dalam kondisi operasional nyata, sistem ini masih memiliki keterbatasan, terutama belum adanya fitur *liveness detection*. Pengembangan selanjutnya dapat difokuskan pada penambahan mekanisme anti-*spoofing*, peningkatan jumlah pengguna, serta uji coba dalam kondisi penggunaan yang lebih kompleks guna meningkatkan keandalan dan skalabilitas sistem secara menyeluruh.

REFERENSI

- [1] H. Zhang, Y. Liu, dan L. Wang, "Security Analysis of Traditional Safe Lock Systems," *IEEE Access*, vol. 9, pp. 110234–110245, 2021.
- [2] H. Sharma dan N. Kanwal, "Smart Surveillance Using IoT: A Review," *Radioelectronic and Computer Systems*, no. 1(109), 2024.
- [3] M. Alshahrani, "Design of IoT Smart Lock for Home Automation," *Int J Comput Appl*, vol. 184, no. 17, pp. 1–6, 2022.
- [4] G. Jocher, A. Stoken, J. Borovec, NanoCode, dan others, "YOLOv5 by Ultralytics," *arXiv preprint arXiv:2011.08036*, 2021.
- [5] F. Wang, M. Zhang, dan C. Liu, "YOLO-Face: Real-Time Face Detection Algorithm," *arXiv preprint arXiv:2203.01047*, 2022.
- [6] V. Bhattacharya, S. Soni, dan A. Verma, "Face Recognition Door Lock System Using Raspberry Pi," *International Journal of Engineering and Technology Innovation*, vol. 10, no. 2, 2022.
- [7] T. Li and W. Wu, "Using IoT and YOLOv5 for Real-Time Security Monitoring," *International Journal of Computer Science and Mobile Computing (IJCSM)*, vol. 13, no. 1, pp. 12–20, 2023.
- [8] J. Lin, H. Sun, dan T. Zhang, "Performance Evaluation Metrics for Face Detection," *Pattern Recognit Lett*, vol. 150, pp. 50–57, 2022.
- [9] I. D. Irawan, A. H. R. Rizal, dan T. A. Kurniawan, "Perancangan Smart Safety Box menggunakan Arduino Uno dan RFID," *Jurnal Teknik ITS*, vol. 9, no. 2, pp. A83–A88, 2020.
- [10] A. T. Santosa, D. R. Prayitno, dan A. Riyanto, "Smart Box berbasis IoT untuk Pengamanan Barang Berharga," *Jurnal Teknologi dan Sistem Komputer*, vol. 9, no. 3, pp. 140–146, 2021.
- [11] A. Ahmad, S. M. Putra, dan R. Andika, "Sistem Pengamanan Pintu Otomatis Menggunakan RFID dan ESP8266 Berbasis IoT," *Jurnal Infra*, vol. 9, no. 1, pp. 85–90, 2021.
- [12] D. Nugroho and E. Prasetyo, "Rancang Bangun Smart Locker Berbasis Fingerprint dan NodeMCU," *Jurnal Informatika dan Sistem Informasi*, vol. 6, no. 1, pp. 23–29, 2020.
- [13] A. Wijaya and others, "Sistem Keamanan Kendaraan Menggunakan Pengenalan Wajah Berbasis Raspberry Pi," *Jurnal Teknologi Informasi*, vol. 13, no. 1, pp. 55–61, 2022.
- [14] A. A. Setiawan, "Implementasi Sistem Keamanan Rumah Berbasis IoT," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 8, no. 4, pp. 765–771, 2021.
- [15] L. Firmansyah, D. R. Saputro, and S. Mulyono, "Perbandingan Mikrokontroler ESP32 dan NodeMCU pada Sistem Monitoring," *Jurnal Teknik Komputer AMIK BSI*, vol. 6, no. 1, pp. 20–25, 2020.
- [16] K. R. Shinde, R. K. Patil, S. B. Waghmare, and R. S. Mulla, "Face Mask Detection Using YOLOv5," in *2021 International Conference on Intelligent Technologies (CONIT)*, 2021, pp. 1–5.
- [17] F. Ulfa, A. A. Rachman, and A. S. Maulana, "Implementasi YOLOv5 untuk Pengenalan Wajah dalam Kondisi Minim Cahaya," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 1, pp. 54–61, 2023.
- [18] R. Sari, M. F. Rahman, and Y. A. Rizky, "Penerapan YOLOv5 pada Sistem Keamanan Rumah dengan Notifikasi Telegram," *Jurnal Sains dan Informatika*, vol. 8, no. 2, pp. 101–108, 2022.
- [19] M. Hidayat and D. Ramadhan, "Implementasi YOLOv5 untuk Otentikasi Wajah di Perangkat Edge," *Jurnal Komputer dan Sistem Cerdas*, vol. 11, no. 1, pp. 19–25, 2023.
- [20] Y. Kurniawan, M. Arifin, and N. Maulana, "Optimasi YOLOv5 untuk ESP32-CAM pada Sistem Keamanan Offline," *Jurnal Teknologi dan Rekayasa*, vol. 14, no. 1, pp. 45–52, 2023.