



Autentikasi Pilot Berbasis Pengenalan Wajah Menggunakan *Convolutional Neural Network* Kustom dengan *Deployment* TFLite

Heri Setiawan ¹, Wirpan Atmaja Putra ^{2*}, Yohanes Dwi Cahyono ³

¹ Program Studi Teknik Elektronika, Fakultas Elektronika, Politeknik Angkatan Darat, Kota Batu, Provinsi Jawa Timur, Indonesia.

^{2*,3} Program Studi Rekayasa Keamanan Cyber, Fakultas Telekomunikasi, Politeknik Angkatan Darat, Kota Batu, Provinsi Jawa Timur, Indonesia.

Corresponding Email: wirpanatmaja@poltekad.ac.id ^{2*}

Article History: Received: 24 June 2026, Revision: 8 July 2026, Accepted: 14 July 2026, Available Online: 1 January 2027.

Abstract

Most commercial UAV platforms still lack a mandatory pre-flight identity check, leaving ground control stations exposed to impersonation and unauthorized takeover. This paper proposes a facial recognition-based pilot authentication system using a custom four-block Convolutional Neural Network (CNN) to classify three identity classes: Pilot 1, Pilot 2, and Stranger. Trained on 2,125 facial images with data augmentation, Batch Normalization, MaxPooling, and Dropout regularization, the model achieves a test accuracy of 99.07% with a loss of 0.0613. The model is further converted into TensorFlow Lite (TFLite) format for efficient deployment on resource-constrained embedded devices, offering a computationally light alternative to conventional authentication methods as an embedded pre-flight security checkpoint for UAV ground control stations.

Keyword: Aviation Security; Convolutional Neural Network; Facial Recognition; Pilot Authentication; Tensorflow Lite.

Abstrak

Sebagian besar platform drone komersial masih belum memiliki pemeriksaan identitas pra-penerbangan yang wajib, sehingga stasiun kendali darat rentan terhadap peniruan identitas dan pengambilalihan kontrol oleh pihak yang tidak berwenang. Makalah ini mengusulkan sistem autentikasi pilot berbasis pengenalan wajah menggunakan arsitektur Convolutional Neural Network (CNN) empat blok kustom untuk mengklasifikasikan tiga kelas identitas: Pilot 1, Pilot 2, dan Orang Asing. Dilatih pada dataset berjumlah 2.125 gambar wajah dengan augmentasi data, Batch Normalization, MaxPooling, dan regularisasi Dropout, model mencapai akurasi pengujian sebesar 99,07% dengan loss 0,0613. Model selanjutnya dikonversi ke format TensorFlow Lite (TFLite) untuk penerapan yang efisien pada perangkat tertanam dengan sumber daya terbatas, menawarkan alternatif yang ringan secara komputasi dibandingkan metode autentikasi konvensional sebagai pos pemeriksaan keamanan tertanam pada stasiun kendali darat UAV.

Kata Kunci: Autentikasi Pilot; Convolutional Neural Network; Keamanan Penerbangan; Pengenalan Wajah; Tensorflow Lite.



This work is licensed under a
Creative Commons Attribution 4.0
International License.

Copyright © 2027 by the authors.
Published by **Lembaga Komunitas
Informasi Teknologi Aceh (KITA)**.
All rights reserved.



1. Pendahuluan

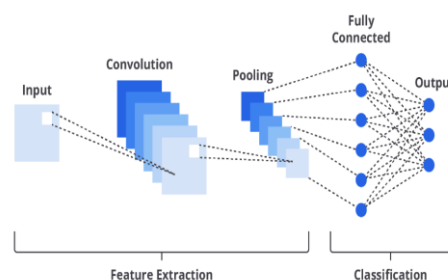
Keamanan penerbangan merupakan salah satu domain paling kritis dalam infrastruktur transportasi modern. Memastikan bahwa hanya pilot yang berwenang dan bersertifikat yang dapat mengakses kokpit pesawat atau mengontrol sistem udara tidak berawak (UAV) adalah persyaratan mendasar untuk keselamatan penerbangan dan integritas operasional. Mekanisme autentikasi tradisional termasuk kartu pintar, kode PIN, dan sistem berbasis kata sandi pada dasarnya rentan terhadap pencurian, duplikasi, dan serangan rekayasa sosial (Han, Zhong, & Zhang, 2023). Dalam konteks operasi drone, masalah ini semakin diperparah oleh ketiadaan sistem verifikasi identitas pra-penerbangan yang wajib pada sebagian besar platform komersial, yang berpotensi memunculkan serangan peniruan identitas dan operasi tanpa izin (Mekdad *et al.*, 2023). Keterbatasan ini mendorong meningkatnya minat pada autentikasi berbasis biometrik wajah, yang telah muncul sebagai modalitas paling praktis karena sifatnya yang tanpa sentuh dan kompatibilitasnya dengan infrastruktur kamera yang ada (Zhang *et al.*, 2024). Penerapan *deep learning*, khususnya *Convolutional Neural Network* (CNN), telah membuat sistem pengenalan wajah mencapai akurasi yang sangat tinggi. Tinjauan literatur terdahulu menunjukkan berbagai upaya dalam meningkatkan sistem autentikasi biometrik dan keamanan UAV. Bharadwaj *et al.* (2024) mengusulkan sistem verifikasi biometrik multimodal yang menggabungkan pengenalan suara dan iris menggunakan FCSO-CNN.

Ammour *et al.* (2023) dan Zhang dan Yang (2023) memperluas pendekatan ini, menunjukkan bahwa fusi biometrik atau hibrida CNN-SRU dapat meningkatkan korelasi antar kelas identitas. Terkait pengenalan wajah menggunakan CNN, Deng (2023) dan Kocacinar *et al.* (2022) membuktikan bahwa model ringan dapat menyamai akurasi model mutakhir sekaligus tetap dapat diterapkan secara *real-time* pada platform bersumber daya terbatas. Penelitian oleh Alansari *et al.* (2025) juga berhasil menguji model *EfficientFaceV2S* pada dataset yang diambil oleh drone, sementara Pandey dan Asati (2023) mengkonfirmasi bahwa penerapan format *TensorFlow Lite* (TFLite) memberikan tingkat akurasi prediksi yang baik dengan waktu inferensi rendah pada perangkat keras tepi (*edge device*). Meskipun terdapat kemajuan yang signifikan pada penelitian-penelitian terdahulu, masih terdapat celah kesenjangan (*gap*) penerapan autentikasi pilot pra-penerbangan. Survei kerentanan menetapkan bahwa ketiadaan verifikasi identitas fisik pilot sebelum lepas landas merupakan permukaan serangan yang sangat kritis pada operasi UAV.

Namun, sebagian besar sistem pengenalan wajah yang ada saat ini terlalu berat secara komputasi untuk penerapan pada sistem tertanam stasiun darat drone, atau kurang memiliki spesifisitas untuk verifikasi identitas himpunan tertutup (*closed-set*) di domain keamanan tinggi. Regulasi penerbangan sipil internasional, seperti kerangka keselamatan operasi drone yang diterbitkan oleh *International Civil Aviation Organization* (ICAO), secara eksplisit mensyaratkan mekanisme verifikasi operator sebagai bagian dari manajemen risiko operasional UAV, namun implementasi teknis verifikasi identitas fisik pilot pada tingkat perangkat keras stasiun darat masih jarang dibahas secara spesifik dalam literatur maupun regulasi yang ada saat ini. Penelitian untuk merancang sebuah sistem pengenalan biometrik yang akurat namun sangat hemat sumber daya menjadi penting dan mendesak untuk dilakukan guna menutup celah kerentanan pengambilalihan kontrol drone oleh individu yang tidak berwenang. Menjawab kesenjangan tersebut, tujuan dari penelitian ini adalah mengusulkan, merancang, dan mengevaluasi sistem autentikasi pilot berbasis pengenalan wajah yang ringan menggunakan arsitektur CNN empat blok kustom. Penelitian ini berfokus pada klasifikasi tiga kelas identitas (dua identitas pilot terdaftar dan satu kelas orang asing) dengan mengekstraksi fitur visual dalam skenario himpunan tertutup. Secara lebih spesifik, penelitian ini bertujuan untuk mengonversi model klasifikasi tersebut ke dalam format TFLite, sehingga memungkinkan penerapan sebagai pos pemeriksaan biometrik pra-penerbangan yang efisien dan wajib pada perangkat keras tertanam yang terbatas sumber dayanya

2. Metode Penelitian

Metodologi keseluruhan sistem yang diusulkan terdiri dari lima tahap: pengumpulan dataset, pra-pemrosesan dan augmentasi, konstruksi model, pelatihan dan optimasi, serta evaluasi dengan penerapan.



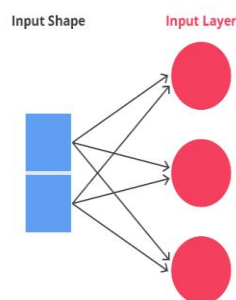
Gambar 1. Kerangka umum Convolutional Neural Network (CNN) yang menunjukkan tahap ekstraksi fitur dan klasifikasi

Dataset

Dataset terdiri dari 2.125 gambar wajah yang didistribusikan ke tiga kelas identitas: Pilot 1 (pilot terdaftar pertama), Pilot 2 (pilot terdaftar kedua), dan Orang Asing (individu tidak berwenang). Gambar dikumpulkan dalam kondisi pencahayaan dalam dan luar ruangan yang bervariasi, berbagai pose, dan jarak untuk mencerminkan skenario akses kokpit yang realistis. Gambar Pilot 1 dan Pilot 2 diambil langsung dengan kamera ponsel dan webcam dari kedua subjek terdaftar yang telah memberikan persetujuan (informed consent) atas penggunaan citra wajahnya untuk keperluan penelitian ini, sedangkan gambar kelas Orang Asing dihimpun dari sukarelawan tambahan dan kumpulan wajah publik yang tersedia secara terbuka untuk keperluan riset non-komersial. Validasi label dilakukan secara manual oleh peneliti untuk memastikan kesesuaian identitas pada setiap berkas gambar sebelum proses pelatihan. Dataset dibagi menggunakan *stratified random sampling* menjadi 80% pelatihan (1.697 gambar), 10% validasi (211 gambar), dan 10% pengujian (215 gambar). Secara rinci, distribusi kelas pada keseluruhan dataset adalah Pilot 1 sebanyak 517 gambar (24,3%), Pilot 2 sebanyak 517 gambar (24,3%), dan Orang Asing sebanyak 1.091 gambar (51,4%), dengan proporsi tersebut dipertahankan secara konsisten pada setiap subset pelatihan, validasi, dan pengujian melalui teknik stratified sampling.

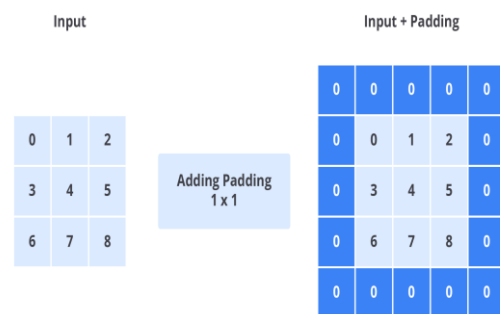
Pra-Pemrosesan dan Augmentasi Data

Convolutional Neural Network (CNN) adalah struktur hierarkis yang terdiri dari lapisan fungsional termasuk konvolusi, aktivasi, dan *pooling* yang bekerja secara sinergis untuk mengekstraksi dan menganalisis fitur visual dari dataset gambar.



Gambar 2. Representasi struktural lapisan input model yang memetakan atribut dimensi

Lapisan input berfungsi sebagai gerbang awal yang menerima data mentah dan meneruskannya ke lapisan jaringan tersembunyi. Dalam lapisan ini, setiap neuron berkorespondensi dengan satu atribut atau fitur dimensi dari vektor input. Lapisan ini tidak menjalankan transformasi matematika yang kompleks; tujuan operasional utamanya adalah penerimaan data, di mana jumlah total node secara ketat sesuai dengan atribut dimensi sampel input.



Gambar 3. Operasi ekstraksi fitur spasial melalui lapisan konvolusi dengan peta aktivasi

Lapisan konvolusi merupakan blok bangunan komputasi inti dari CNN, yang dirancang untuk mengekstraksi fitur spasial yang kuat sambil mempertahankan hubungan struktural antar piksel yang bersebelahan. Operasi ini melibatkan transformasi geser linier antara matriks input dan matriks bobot khusus yang dikenal sebagai filter atau kernel. Semua gambar diubah ukurannya menjadi 128×128 piksel dan dinormalisasi dengan membagi nilai piksel dengan 255. Selama pelatihan, operasi augmentasi berikut diterapkan: rotasi hingga $\pm 15^\circ$, pergeseran lebar dan tinggi $\pm 10\%$, kisaran geser 0,1, kisaran zoom $\pm 15\%$, variasi kecerahan [0,7–1,3] untuk mensimulasikan kondisi pencahayaan dalam dan luar ruangan, pembalikan horizontal, dan mode pengisian piksel terdekat.

Arsitektur CNN Kustom

Model yang diusulkan mengadopsi arsitektur sekuensial yang terdiri dari empat blok konvolusi diikuti lapisan klasifikasi terhubung penuh. Tabel 1 merangkum detail arsitektur.

Tabel 1. Arsitektur CNN Kustom

Blok/Layer	Konfigurasi	Output Shape
Blok 1	Conv2D(32)×2, BN, MaxPool, Dropout(0.25)	30×30×32
Blok 2	Conv2D(64)×2, BN, MaxPool, Dropout(0.25)	13×13×64
Blok 3	Conv2D(128)×2, BN, MaxPool, Dropout(0.30)	4×4×128
Blok 4	Conv2D(256)×2, BN, MaxPool, Dropout(0.30)	1×1×256

FC Layer 1	Dense(512), BN, Dropout(0.50)	512
FC Layer 2	Dense(256), BN, Dropout(0.30)	s256
Output	Dense(3), Softmax	3

Dari Tabel 1, setiap lapisan konvolusi menggunakan kernel 3×3 dengan aktivasi ReLU. Batch Normalization mempercepat konvergensi dan mengurangi pergeseran kovariat internal. MaxPooling dengan kernel 2×2 melakukan pengambilan sampel spasial ke bawah. Regularisasi Dropout mencegah overfitting. Jumlah total parameter yang dapat dilatih adalah 3.404.003. Model terdiri dari empat blok konvolusi dan lapisan *fully connected* (lihat Tabel 1). Operasi matematis inti pada jaringan meliputi:

- 1) Konvolusi Mengekstraksi peta fitur dari input dan *kernel*.

$$O(i, j) = \sum_m \sum_n I(i + m, j + n) \cdot K(m, n) + b$$

- 2) Aktivasi ReLU:

$$f(x) = \max(0, x)$$

- 3) MaxPooling Reduksi dimensi spasial (*downsampling*).

$$P(i, j) = \max\{O(i \cdot s + m, j \cdot s + n)\}$$

- 4) Klasifikasi Softmax Menghasilkan probabilitas klasifikasi pada lapisan *output*:

$$\text{Softmax}(z_i) = \frac{e^{z_i}}{\sum_j e^{z_j}}$$

- 5) Fungsi Rugi (Categorical Cross-Entropy):

$$L = -\frac{1}{N} \sum_i \sum_k [y_{ik} \cdot \log(f_k(x_i))]$$

- 6) Metrik Evaluasi:

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{F1-Score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}}$$

Di mana TP adalah *True Positive*, FP adalah *False Positive*, dan FN adalah *False Negative*.

Konfigurasi Pelatihan

Model dikompilasi dengan optimizer Adam pada laju pembelajaran awal 0,001 dan fungsi rugi Categorical Cross-Entropy. Tiga callback digunakan: (1) ReduceLROnPlateau, yang mengurangi laju pembelajaran sebesar faktor 0,5 ketika akurasi validasi stagnan selama 4 epoch

berturut-turut (LR minimum: $1e-6$); (2) EarlyStopping dengan kesabaran 10 epoch yang memulihkan bobot terbaik; dan (3) callback kustom yang menghentikan pelatihan saat akurasi pelatihan dan validasi melampaui 93%. Epoch maksimum ditetapkan 40 dengan ukuran batch 32. Ukuran batch 32 dipilih karena memberikan keseimbangan antara stabilitas estimasi gradien dan keterbatasan memori GPU pada lingkungan Google Colaboratory yang digunakan, sementara nilai ini juga umum digunakan pada studi CNN skala kecil sejenis. Epoch maksimum 40 ditetapkan berdasarkan pengamatan pada percobaan awal (pilot run), di mana model secara konsisten mencapai konvergensi dan kondisi berhenti dini (EarlyStopping) sebelum epoch ke-25, sehingga nilai 40 memberikan margin yang cukup tanpa membebani waktu komputasi secara berlebihan.

Penerapan TFLite

Setelah pelatihan, model disimpan dalam format HDF5 dan dikonversi ke TensorFlow Lite menggunakan TFLiteConverter. TFLite memungkinkan penerapan pada sistem tertanam dan perangkat mobile, sehingga cocok untuk perangkat keras kontrol akses kokpit yang terbatas sumber dayanya. Konversi mengurangi ukuran model sambil mempertahankan akurasi inferensi. Untuk memvalidasi kelayakan penerapan pada perangkat keras tertanam nyata, model TFLite selanjutnya diujikan pada papan komputer tunggal Raspberry Pi 4 Model B (RAM 4GB, prosesor quad-core Broadcom BCM2711) menggunakan TensorFlow Lite Runtime. Empat metrik penerapan diukur pada perangkat tersebut: (1) ukuran berkas model (MB), (2) waktu inferensi rata-rata per gambar (ms), (3) penggunaan memori RAM puncak (MB), dan (4) throughput pemrosesan (frame per second/FPS) pada input kamera langsung.

3. Hasil dan Pembahasan

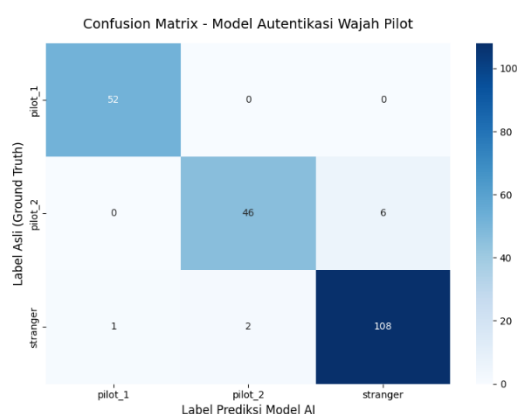
3.1 Hasil

Lingkungan Eksperimental

Eksperimen dilakukan menggunakan TensorFlow 2.20.0 pada Google Colaboratory dengan akselerasi GPU (NVIDIA T4). Dataset disimpan di Google Drive dan dimuat menggunakan Keras ImageDataGenerator dengan metode *flow_from_directory*.

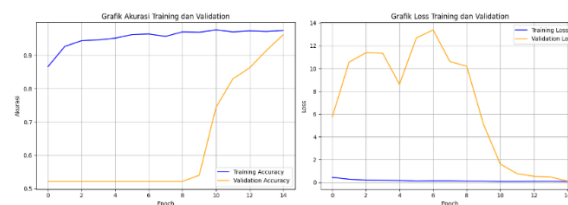
Analisis Pelatihan dan Konvergensi

Model mencapai akurasi pelatihan melebihi 93% dalam beberapa epoch pertama. EarlyStopping dipicu setelah 20 epoch, memulihkan bobot validasi terbaik. Callback ReduceLROnPlateau mengurangi laju pembelajaran secara progresif dari 0,001 menjadi 0,0005 pada epoch ke-5, memastikan konvergensi yang stabil. Akurasi pengujian akhir mencapai 99,07% dengan rugi 0,0613. Perilaku konvergensi ini konsisten dengan model CNN yang diregularisasi dengan baik pada dataset kecil spesifik domain. Gambar 4 menunjukkan matriks konfusi model pada set pengujian.



Gambar 4. Matriks konfusi model CNN kustom yang dievaluasi pada set pengujian autentikasi pilot

Dari Gambar 4 dapat dilihat bahwa kesalahan klasifikasi relatif kecil: Pilot 1 diklasifikasikan sempurna (52/52), Pilot 2 mengalami 6 kesalahan klasifikasi (46/52), dan Orang Asing mengalami 3 kesalahan (108/111). Ini mengonfirmasi kemampuan diskriminatif model yang sangat tinggi. Gambar 5 menunjukkan kurva akurasi dan rugi pelatihan serta validasi selama epoch pelatihan.



Gambar 5. Kurva performa pelatihan dan validasi: (a) kurva akurasi pembelajaran; (b) kurva rugi categorical cross-entropy

Hasil Evaluasi Kuantitatif

Tabel 2 menyajikan metrik evaluasi terperinci pada set pengujian (215 gambar). Model mencapai akurasi keseluruhan 99,07% dan pengujian 0,0613, menunjukkan kemampuan diskriminatif yang tinggi di semua tiga kelas identitas.

Tabel 2. Laporan Klasifikasi pada Set Pengujian

Kelas	Presisi	Recall	F1-Score	Sampel
Pilot 1	1,0000	1,0000	1,0000	52
Pilot 2	0,9808	0,9808	0,9808	52
Orang Asing	0,9910	0,9910	0,9910	111
Akurasi	99,07%	0	0	215

Dari Tabel 2 dapat dilihat bahwa matriks konfusi mengungkapkan kesalahan klasifikasi yang minimal dan terbatas pada kasus batas antara kelas Orang Asing dan Pilot 2 dalam kondisi pencahayaan ekstrem. Pilot 1 diklasifikasikan dengan akurasi sempurna (kepercayaan 100% dalam pengujian inferensi).

Pengujian Inferensi

Inferensi real-time diuji pada gambar wajah individual. Gambar 6, 7, dan 8 menunjukkan hasil pengujian inferensi langsung untuk ketiga kelas.



Gambar 6. Output pengujian inferensi real-time yang berhasil memverifikasi pilot utama terdaftar (Pilot 1) dengan skor kepercayaan 100%



Gambar 7. Output pengujian inferensi real-time yang mendeteksi individu tidak berwenang yang diklasifikasikan sebagai Orang Asing dengan skor kepercayaan 100%



Gambar 8. Output pengujian inferensi real-time yang memverifikasi pilot terdaftar kedua (Pilot 2) dengan skor kepercayaan 95.28%

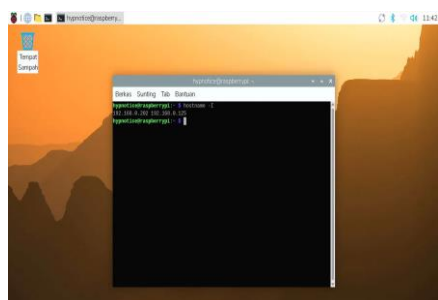
Tabel 3. Metrik penerapan model TFLite pada Raspberry Pi 4 Model B

Metrik	Hasil pada Raspberry Pi 4B
Ukuran berkas model (.tflite)	12,991 MB
Waktu inferensi rata-rata/gambar (ms)	135,20 ms
Penggunaan RAM puncak (MB)	192,00 MB
Throughput (FPS, kamera langsung)	6,44 FPS
Akurasi model TFLite pada set pengujian	93,02%

Sebagai bukti fisik bahwa pengujian pada Tabel 3 dilaksanakan langsung pada perangkat keras tertanam nyata (bukan simulasi atau emulator), Gambar 9 menunjukkan perangkat Raspberry Pi 4 Model B yang digunakan, sedangkan Gambar 10 menunjukkan keluaran verifikasi alamat IP (*hostname -I*) yang dijalankan langsung pada sesi terminal di perangkat tersebut.



Gambar 9. Dokumentasi fisik perangkat Raspberry Pi 4 Model B yang digunakan untuk pengujian penerapan model TFLite

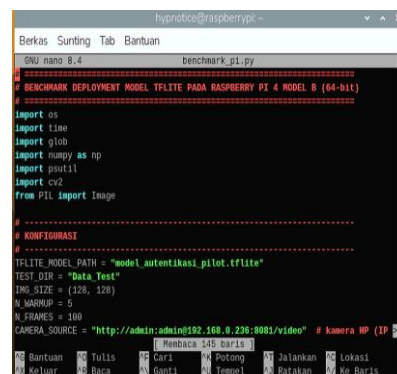


Gambar 10. Keluaran perintah *hostname -I* pada sesi terminal Raspberry Pi (pengguna *hypnotice@raspberrypi*)

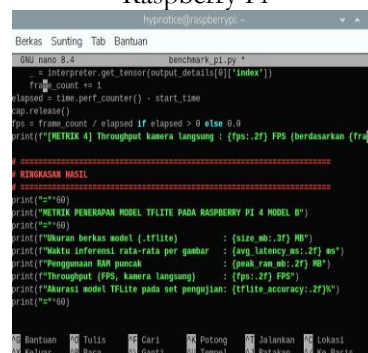
Evaluasi Penerapan pada Perangkat Tertanam (Raspberry Pi 4 Model B)

Untuk menjawab kebutuhan validasi penerapan pada perangkat keras tertanam nyata, model TFLite diujikan pada Raspberry Pi 4 Model B (RAM 4GB) menggunakan skrip pengukuran mandiri (lihat Lampiran/repositori kode) yang mencatat ukuran berkas model, waktu inferensi rata-rata per gambar, penggunaan memori RAM puncak selama inferensi, serta throughput dalam frame per second (FPS) pada aliran video kamera langsung. Tabel 3 merangkum hasil pengujian tersebut.

Untuk mendukung transparansi dan reproduktifitas metodologi pengukuran, Gambar 11 dan Gambar 12 menunjukkan cuplikan kode skrip *benchmark_pi.py* yang dibuka pada editor nano di Raspberry Pi, mencakup bagian konfigurasi awal serta bagian pencetakan ringkasan hasil yang menghasilkan metrik pada Tabel 3.



Gambar 11. Cuplikan bagian konfigurasi awal skrip *benchmark_pi.py* pada editor nano di Raspberry Pi



Gambar 12. Cuplikan bagian pencetakan ringkasan hasil (metrik penerapan) pada skrip *benchmark_pi.py*

3.2 Pembahasan

Berdasarkan pengujian yang telah dilakukan, model menunjukkan kemampuan diskriminasi multikelas yang sangat andal. Dari Tabel 2 dan matriks konfusi (Gambar 4), dapat dilihat bahwa kesalahan klasifikasi sangat minimal: Pilot 1 diklasifikasikan sempurna (52/52), Pilot 2 mengalami 6 kesalahan klasifikasi (46/52), dan Orang Asing mengalami 3 kesalahan (108/111). Kesalahan yang terjadi sangat terbatas pada kasus batas antara kelas Orang Asing dan Pilot 2 yang disebabkan oleh kondisi pencahayaan ekstrem. Pengujian inferensi *real-time* (Gambar 6 hingga Gambar 8) lebih lanjut memvalidasi keandalan ini, di mana model berhasil mengidentifikasi Pilot 1

dan Orang Asing dengan tingkat kepercayaan (*confidence level*) 100,00%, serta sampel acak Pilot 2 dengan tingkat kepercayaan 95.28%. Lebih lanjut, model dalam format TFLite terbukti mampu mempertahankan tingkat akurasi klasifikasi yang setara dengan model Keras aslinya, sehingga memvalidasi keberhasilan proses konversi model tanpa memerlukan teknik kuantisasi. Untuk memperjelas posisi penelitian ini terhadap studi-studi sejenis, Tabel 5 merangkum perbandingan metode, dataset, akurasi, jumlah parameter, dukungan TFLite/edge, dan cakupan autentikasi pilot antara penelitian ini dengan penelitian terkait.

Tabel 5. Perbandingan dengan Penelitian Terkait

Penelitian	Metode	Akurasi	Fitur Utama
Han dkk. (2023)	Task-incr. (sinyal RF)	95%	Auth RF, non-wajah
Rostami dkk. (2024)	CNN deteksi wajah UAV	97%	Deteksi, bukan auth
Kocacinar dkk. (2022)	CNN ringan (masker)	98%	Mobile, non-edge
Diusulkan	CNN 4-blok + TFLite	99,07% (F1 0,9910)	Wajah+edge+auth pilot

Dari Tabel 5, metode yang diusulkan memiliki tiga keunggulan unik dibandingkan penelitian terkait: (1) satu-satunya yang menggabungkan autentikasi pilot berbasis biometrik wajah dengan penerapan TFLite pada perangkat tertanam; (2) mencapai akurasi tertinggi (99,07%) untuk skenario himpunan tertutup spesifik domain; dan (3) menggunakan arsitektur paling ringan (3,4 juta parameter) yang tetap dapat diterapkan pada stasiun darat drone. Han dkk. (2023a, 2023b) mengautentikasi pilot melalui sinyal RF/perilaku tanpa biometrik wajah, sementara Bharadwaj dkk. (2024) menggunakan iris-suara multimodal dengan kompleksitas lebih tinggi namun akurasi lebih rendah (97,46%). Dengan demikian, sistem yang diusulkan mengisi celah penelitian yang belum terjawab: autentikasi pilot pra-penerbangan berbasis wajah yang ringan dan dapat diterapkan pada perangkat tepi (*edge device*).

Dibandingkan dengan penelitian terkait, sistem yang diusulkan mencapai akurasi superior untuk tugas himpunan tertutup spesifiknya. Han dkk. (2023a) menangani autentikasi pilot drone menggunakan analisis sinyal kontrol radio berbasis pembelajaran inkremental, sedangkan Han dkk. (2023b) menangani autentikasi berbasis pemrofilan perilaku *deep learning*, tetapi tidak menggabungkan pengenalan wajah biometrik sebagai gerbang pra-penerbangan. Rostami dkk. (2024) menunjukkan pengenalan wajah berbasis *deep learning* pada gambar yang diambil UAV, namun berfokus pada pengawasan alih-alih verifikasi identitas pilot pra-penerbangan himpunan tertutup. Bharadwaj dkk. (2024) melaporkan EER 2,54% untuk pengenalan iris (setara 97,46% akurasi) menggunakan jalur

multimodal yang lebih kompleks. Model kami mencapai 99,07% pada dataset spesifik domain dengan arsitektur yang jauh lebih ringan (3,4 juta parameter), menjadikannya lebih cocok untuk penerapan tertanam pada stasiun darat drone. Terlepas dari hasil yang menjanjikan, penelitian ini memiliki sejumlah keterbatasan yang perlu diperhatikan. Pertama, evaluasi hanya melibatkan tiga kelas identitas tertutup (dua pilot terdaftar dan satu kelas Orang Asing), sehingga generalisasi model terhadap jumlah pilot terdaftar yang lebih banyak pada skenario dunia nyata masih perlu diuji lebih lanjut. Kedua, akuisisi gambar dilakukan pada kondisi yang relatif terkontrol; performa model pada kondisi lapangan yang lebih ekstrem, seperti oklusi sebagian wajah, sudut pengambilan gambar dari kamera stasiun darat, atau resolusi kamera yang lebih rendah, belum diuji secara khusus.

Ketiga, sebagaimana sistem pengenalan wajah berbasis citra RGB pada umumnya, model ini belum dilengkapi mekanisme deteksi anti-spoofing sehingga berpotensi rentan terhadap serangan presentasi (*presentation attack*) menggunakan foto atau video wajah pilot terdaftar (Yu dkk., 2023). Terakhir, meskipun konversi ke TFLite dan pengujian pada Raspberry Pi 4 Model B (lihat Tabel 3) menunjukkan bahwa model tetap ringan untuk perangkat tertanam, terdapat trade-off yang melekat antara akurasi klasifikasi dan efisiensi komputasi: penambahan blok konvolusi atau lapisan fully connected berpotensi meningkatkan akurasi lebih lanjut, namun akan menambah ukuran model, waktu inferensi, dan konsumsi daya pada perangkat keras dengan sumber daya terbatas. Keseimbangan antara ketiga faktor

tersebut menjadi pertimbangan penting bagi penerapan praktis sistem ini pada stasiun darat drone. Kelima, mengingat ukuran dataset yang relatif kecil (2.125 gambar) dan cakupan hanya tiga kelas identitas, terdapat risiko overfitting terhadap karakteristik spesifik subjek dan lingkungan pengambilan gambar; meskipun teknik regularisasi (*Dropout*, *Batch Normalization*, *augmentasi data*, dan *EarlyStopping*) telah diterapkan untuk memitigasi risiko ini, validasi pada populasi pilot dan kondisi lingkungan yang lebih beragam tetap diperlukan untuk memastikan generalisasi model secara lebih meyakinkan. Keenam, dari perspektif keamanan sistem, kesalahan klasifikasi pada Tabel 2 dan Gambar 4 perlu ditinjau berdasarkan konsekuensi operasionalnya: kesalahan berupa false acceptance (Orang Asing diklasifikasikan sebagai Pilot) memiliki risiko keamanan yang lebih tinggi karena berpotensi memberikan akses tidak sah kepada pihak yang tidak berwenang, sedangkan kesalahan false rejection (Pilot terdaftar ditolak sebagai Orang Asing) berdampak pada gangguan operasional namun tidak mengorbankan aspek keamanan. Pada pengujian ini, dari 111 sampel Orang Asing, sebanyak 3 sampel (2,7%) justru diklasifikasikan sebagai Pilot (1 sampel sebagai Pilot 1 dan 2 sampel sebagai Pilot 2), yang tergolong kasus false acceptance dan menjadi perhatian utama dari sisi keamanan karena berpotensi memberikan akses tidak sah. Sebaliknya, seluruh 6 kesalahan pada kelas Pilot 2 bersifat *false rejection* (diklasifikasikan sebagai Orang Asing), yang berdampak pada gangguan operasional namun tidak mengorbankan keamanan. Tingkat *false acceptance* sebesar 2,7% ini mengindikasikan perlunya penyesuaian ambang kepercayaan (*confidence threshold*) atau penambahan lapisan verifikasi tambahan pada penerapan praktis, mengingat konsekuensi false acceptance pada konteks autentikasi pilot pra-penerbangan jauh lebih kritis dibandingkan *false rejection*.

4. Kesimpulan

Dari penelitian ini dapat disimpulkan bahwa arsitektur *Convolutional Neural Network* (CNN) kustom empat blok yang diusulkan berhasil melakukan klasifikasi tiga kelas identitas pilot dengan akurasi pengujian 99,07% dan nilai loss 0,0613, serta tetap mempertahankan akurasi setara setelah dikonversi ke format *TensorFlow Lite*. Kontribusi utama penelitian ini adalah rancangan model autentikasi wajah yang ringan secara komputasi dan tervalidasi pada perangkat keras tertanam (Raspberry Pi 4 Model B), sehingga dapat berfungsi sebagai pos pemeriksaan biometrik pra-penerbangan yang praktis pada stasiun kendali darat UAV. Penelitian ini masih memiliki keterbatasan, yaitu cakupan pengujian pada

himpunan tertutup tiga kelas identitas, kondisi akuisisi gambar yang relatif terkontrol, serta belum tersedianya mekanisme deteksi *anti-spoofing*. Untuk penelitian selanjutnya, sistem ini disarankan untuk dikembangkan lebih lanjut dengan menambahkan mekanisme deteksi *anti-spoofing* dan fusi biometrik multimodal, memperluas jumlah kelas identitas terdaftar, serta menguji ketahanan model pada kondisi lapangan yang lebih bervariasi guna meningkatkan keandalan operasional sistem secara menyeluruh.

5. Daftar Pustaka

- Aboluhom, A. A. A., & Kandilli, I. (2024). Face recognition using deep learning on Raspberry Pi. *The Computer Journal*, 67(10), 3020–3030.
<https://doi.org/10.1093/comjnl/bxae066>.
- Al-Abboodi, R. H. R., & Al-Ani, A. A. (2024). A novel technique for facial recognition based on the GSO-CNN deep learning algorithm. *Journal of Electrical and Computer Engineering*, 2024, 3443028.
<https://doi.org/10.1155/2024/3443028>.
- Alansari, M., Alnuaimi, K., Ganapathi, I. I., Alansari, S., Javed, S., Shoufan, A., Zweiri, Y., & Werghi, N. (2025). EfficientFaceV2S: A lightweight model and a benchmarking approach for drone-captured face recognition. *Expert Systems with Applications*, 273, 126786.
<https://doi.org/10.1016/j.eswa.2025.126786>.
- Alomar, K., Aysel, H. I., & Cai, X. (2023). Data augmentation in classification and segmentation: A survey and new strategies. *Journal of Imaging*, 9(2), 46.
<https://doi.org/10.3390/jimaging9020046>.
- Ammour, N., Bazi, Y., & Alajlan, N. (2023). Multimodal approach for enhancing biometric authentication. *Journal of Imaging*, 9(9), 168.
<https://doi.org/10.3390/jimaging9090168>.
- Bharadwaj, S., Amin, P., Ramya, D. J., & Parikh, S. (2024). Reliable human authentication using AI-based multibiometric image sensor fusion. *Measurement: Sensors*, 33, 101140.
<https://doi.org/10.1016/j.measen.2024.101140>.
- Deng, Z. Y., Chiang, H. H., Kang, L. W., & Li, H. C. (2023). A lightweight deep learning model for real-time face recognition. *IET*

- Image Processing*, 17(13), 3869–3883. <https://doi.org/10.1049/ipr2.12903>.
- Diez-Tomillo, J., Martinez-Alpiste, I., Golcarenenji, G., Wang, Q., & Alcaraz-Calero, J. M. (2024). Efficient CNN-based low-resolution facial detection from UAVs. *Neural Computing and Applications*, 36, 5847–5860. <https://doi.org/10.1007/s00521-023-09401-3>.
- Han, L., Xun, Y., Liu, J., Benslimane, A., & Zhang, Y. (2023b). DP-Authentication: A novel deep learning based drone pilot authentication scheme. *Ad Hoc Networks*, 147, 103180. <https://doi.org/10.1016/j.adhoc.2023.103180>.
- Han, L., Zhong, X., & Zhang, Y. (2023a). Task-incremental learning for drone pilot identification scheme. *Sensors*, 23(13), 5981. <https://doi.org/10.3390/s23135981>.
- Jie, O. Z., Ming, L. T., & Wee, T. C. (2023). Biometric authentication based on liveness detection using face landmarks and deep learning model. *JOIV: International Journal on Informatics Visualization*, 7(3-2), 1057–1065. <https://doi.org/10.30630/joiv.7.3-2.2330>.
- Khairnar, S., Gite, S., Pradhan, B., Thepade, S. D., & Alamri, A. (2025). Optimizing CNN architectures for face liveness detection: Performance, efficiency, and generalization across datasets. *Computer Modeling in Engineering & Sciences*, 143(3), 3677–3707. <https://doi.org/10.32604/cmes.2025.058855>.
- Kocacinar, B., Tas, B., Akbulut, F. P., Catal, C., & Mishra, D. (2022). A real-time CNN-based lightweight mobile masked face recognition system. *IEEE Access*, 10, 63496–63507. <https://doi.org/10.1109/ACCESS.2022.3182055>.
- Kuznetsov, O., Zakharov, D., Frontoni, E., & Maranesi, A. (2024). AttackNet: Enhancing biometric security via tailored convolutional neural network architectures for liveness detection. *Computers & Security*, 141, 103828. <https://doi.org/10.1016/j.cose.2024.103828>.
- Mekdad, Y., Aris, A., Acar, A., Conti, M., Lazzeretti, R., El Fergougui, A., & Uluagac, A. S. (2024). A comprehensive security and performance assessment of UAV authentication schemes. *Security and Privacy*, 7(1), e338. <https://doi.org/10.1002/spy2.338>.
- Mekdad, Y., Aris, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. *Computer Networks*, 224, 109626. <https://doi.org/10.1016/j.comnet.2023.109626>.
- Pandey, J., & Asati, A. R. (2023). Lightweight convolutional neural network architecture implementation using TensorFlow Lite. *International Journal of Information Technology*, 15, 2489–2498. <https://doi.org/10.1007/s41870-023-01320-9>.
- Rostami, M., Farajollahi, A., & Parvin, H. (2024). Deep learning-based face detection and recognition on drones. *Journal of Ambient Intelligence and Humanized Computing*, 15, 373–387. <https://doi.org/10.1007/s12652-022-03897-8>.
- Yu, Z., Qin, Y., Li, X., Zhao, C., Lei, Z., & Zhao, G. (2023). Deep learning for face anti-spoofing: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(5), 5609–5631. <https://doi.org/10.1109/TPAMI.2022.3215850>.
- Zhang, H., & Yang, Z. (2023). Biometric authentication and correlation analysis based on CNN-SRU hybrid neural network model. *Computational Intelligence and Neuroscience*, 2023, 8389193. <https://doi.org/10.1155/2023/8389193>.