



Optimasi *Pipeline* Pengenalan Wajah Berbasis *Mobile FaceNet* menuju Autentikasi yang *Liveness* (*Liveness-Aware*)

Danuri^{1*}, Kusrini²

¹Magister Informatika, Universitas Amikom Yogyakarta, Indonesia

²Program Doktor, Ilmu Komputer, Universitas Amikom Yogyakarta, Indonesia

Email: danualbantani@gmail.com¹, kusrini@amikom.ac.id²

*Penulis Korespondensi: danualbantani@gmail.com

Abstract. *Bi Biometric face authentication on mobile devices faces two main challenges: computational efficiency under limited resources and vulnerability to spoofing attacks using photos or videos. This study presents an optimized face recognition pipeline by integrating the MobileFaceNet model in TensorFlow Lite (TFLite) format into a React Native application, reinforced with a liveness detection module to ensure the presence of a genuine face. The developed system consists of four main stages: (1) real-time face detection using Expo Face Detector, (2) preprocessing involving cropping and resizing to 112×112 pixels with pixel normalization to the range of $[-1, 1]$, (3) MobileFaceNet inference to generate 128-dimensional face embeddings, and (4) verification using cosine similarity with a threshold of 0.75. Initial testing shows that the system operates entirely on-device without relying on external servers, with inference latency suitable for real-time attendance applications. The integration of liveness detection is proposed as an additional layer of defense against presentation attacks. The main contribution of this study is an integrated, lightweight, and secure pipeline architecture that can be implemented on mid-range mobile devices.*

Keywords: *Cosine Similarity; Face Recognition; Liveness Detection; MobileFaceNet; On-Device Authentication; React Native; TFLite.*

Abstrak. Autentikasi wajah biometrik pada perangkat *mobile* menghadapi dua tantangan utama: efisiensi komputasi dengan sumber daya yang terbatas, serta kerentanan terhadap serangan *spoofing* menggunakan foto atau video. Studi ini menyajikan *pipeline* pengenalan wajah yang dioptimalkan dengan mengintegrasikan model *Mobile FaceNet* dalam format *TensorFlow Lite* (TFLite) ke dalam aplikasi *React Native*, yang diperkuat dengan modul deteksi *liveness* untuk memastikan keberadaan wajah asli. Sistem yang dikembangkan terdiri atas empat tahap utama: (1) deteksi wajah secara real-time menggunakan *Expo Face Detector*, (2) pra-pemrosesan meliputi *crop* dan *resize* ke ukuran 112×112 piksel dengan normalisasi piksel ke rentang $[-1, 1]$, (3) inferensi *Mobile FaceNet* untuk menghasilkan *embedding* wajah berdimensi 128, dan (4) verifikasi menggunakan *cosine similarity* dengan ambang batas 0,75. Pengujian awal menunjukkan bahwa sistem beroperasi sepenuhnya di perangkat (*on-device*) tanpa bergantung pada server eksternal, dengan latensi inferensi yang memadai untuk aplikasi presensi (*attendance*) secara *real-time*. Integrasi deteksi *liveness* diusulkan sebagai lapisan pertahanan tambahan terhadap serangan presentasi (*presentation attack*). Kontribusi utama penelitian ini adalah arsitektur *pipeline* yang terpadu, ringan, dan aman yang dapat diterapkan pada perangkat *mobile* kelas menengah.

Kata kunci: Autentikasi *On-Device*; *Cosine Similarity*; Deteksi *Liveness*; *MobileFaceNet*; Pengenalan Wajah; *React Native*; TFLite.

1. LATAR BELAKANG

Kemajuan teknologi Kecerdasan Buatan (AI) telah menciptakan peluang yang signifikan dalam bidang keamanan digital dan autentikasi (Sannigrahi & Ghosh, 2025). Salah satu aplikasi yang menonjol adalah sistem pengenalan wajah, yang semakin banyak digunakan sebagai mekanisme autentikasi pada perangkat *mobile* (Arkhurst et al., 2025). Keunggulan biometrik wajah dibandingkan metode autentikasi tradisional, seperti PIN atau kata sandi, terletak pada sifat alaminya; tidak dapat dipindahtangankan dan tidak mengharuskan pengguna untuk mengingat apa pun (Budi et al., 2018).

Namun, penerapan pengenalan wajah pada perangkat *mobile* menghadirkan beberapa tantangan teknis yang signifikan. Pertama, keterbatasan sumber daya komputasi perangkat *mobile* menuntut model AI yang ringan namun tetap mempertahankan akurasi tinggi (Ahmad & Pratiwi, 2025). Kedua, sistem yang hanya mengandalkan pengenalan wajah tanpa mekanisme *anti-spoofing* rentan terhadap serangan presentasi upaya untuk mengelabui sistem menggunakan foto, video, atau masker milik pengguna yang sah (Hartanto et al., 2025).

MobileFaceNet adalah arsitektur jaringan saraf tiruan yang dirancang khusus untuk menjalankan pengenalan wajah secara efisien pada perangkat *mobile*. Model ini menghasilkan representasi vektor wajah (*face embedding*) berdimensi 128 yang ringkas namun tetap diskriminatif (Zhang, 2025). Dikombinasikan dengan Lite (*TFLite*) sebagai *runtime* inferensi *on-device*, *MobileFaceNet* menjadi pilihan ideal untuk aplikasi *mobile* yang menuntut kecepatan dan efisiensi (Jouini et al., 2024).

Penelitian ini bertujuan untuk merancang dan mengimplementasikan pipeline pengenalan wajah berbasis *MobileFaceNet* yang diintegrasikan dengan modul deteksi liveness pada platform *React Native* (Grzesik & Mrozek, 2024). Sistem dirancang untuk beroperasi sepenuhnya di perangkat, menghilangkan ketergantungan pada server eksternal, sehingga meningkatkan privasi pengguna dan mengurangi latensi. Implementasi referensi tersedia secara publik di repositori GitHub pada <https://github.com/danuri/mobilefaceauth>.

Studi ini memberikan kontribusi spesifik berikut terhadap bidang autentikasi biometrik *mobile*, yang membedakannya dari penelitian sebelumnya yang hanya menangani tantangan-tantangan ini secara parsial atau terpisah: (1) *Pipeline on-device* yang terpadu: Berbeda dengan Zhang et al. (n.d.) Zhang & Luo, (2022) (masih bergantung sebagian pada server) dan Wang et al. (n.d.) Wang et al. (2010) (tanpa *anti-spoofing*), studi ini menghadirkan pipeline autentikasi yang lengkap mulai dari deteksi wajah, verifikasi *liveness*, hingga pencocokan *cosine similarity* yang seluruhnya dijalankan di perangkat tanpa panggilan server eksternal, sehingga menjaga privasi pengguna dan memungkinkan operasi secara *offline*. (2) Deteksi liveness pasif hibrida tanpa dependensi baru: Skema voting berbobot lima pemeriksaan yang diusulkan (pergerakan mikro, kedipan mata, variansi sudut, tekstur/moiré, distribusi warna) diimplementasikan hanya menggunakan pustaka yang sudah ada dalam aplikasi dasar. Hal ini menghindari kebutuhan sensor perangkat keras tambahan (inframerah, kamera kedalaman) atau model *deep learning* yang berat sebagaimana disyaratkan oleh solusi *anti-spoofing* yang ada Rizki et al. (2025), sehingga cocok diterapkan pada *smartphone* konsumen kelas menengah. (3) Kerangka kerja lintas platform yang ringan: Dengan mengintegrasikan *MobileFaceNet TFLite* ke dalam *React Native* kombinasi yang belum pernah dievaluasi

sebelumnya dalam literatur autentikasi biometrik penelitian ini menyediakan arsitektur referensi yang dapat diterapkan (tersedia secara terbuka di <https://github.com/danuri/mobilefaceauth>), Alauddin et al. (2025) yang menargetkan Android dan iOS dari satu basis kode, sehingga menurunkan hambatan bagi praktisi dan peneliti. (4) Analisis ambang batas yang sistematis: Studi ini mengkarakterisasi *trade-off* FAR–FRR pada lima nilai ambang batas *cosine similarity* (0,65–0,85) dan mengidentifikasi titik operasi *Equal Error Rate*, memberikan panduan praktis untuk penerapan sistem pada berbagai kebutuhan keamanan kedalaman analisis yang tidak ditemukan pada karya-karya pengenalan wajah *mobile* ringan yang sebanding (Capraro et al., 2024).

2. KAJIAN TEORITIS

Pengenalan Wajah pada Perangkat *Mobile*

Pengenalan wajah merupakan salah satu bidang yang paling aktif diteliti dalam visi komputer. *Pipeline* pengenalan wajah modern umumnya terdiri atas empat tahap: deteksi wajah, penyelarasan (*alignment*), ekstraksi fitur (*embedding*), dan pencocokan. Kemajuan dalam *deep learning*, khususnya CNN, telah mendorong akurasi pengenalan wajah melampaui performa manusia pada *benchmark* standar seperti *Labeled Faces in the Wild* (LFW) (Anggara et al., 2023).

Tantangan utama dalam mengadaptasi model pengenalan wajah ke perangkat *mobile* terletak pada menjembatani kesenjangan antara kebutuhan komputasi model *deep learning* dan keterbatasan perangkat keras CPU/GPU *mobile*. Berbagai pendekatan telah dikembangkan untuk mengatasi kesenjangan ini, termasuk pemangkasan jaringan (*pruning*), kuantisasi, distilasi pengetahuan, serta arsitektur yang secara inheren efisien seperti *MobileNet* dan *ShuffleNet* (Jain, 2022).

MobileFaceNet

MobileFaceNet diperkenalkan oleh Balta et al. (n.d.) Balta (2024) sebagai arsitektur CNN yang dirancang khusus untuk verifikasi wajah pada perangkat *mobile*. Berbeda dengan model pengenalan wajah berskala besar seperti *FaceNet* (Meldyantono & Poetro, 2025), yang dapat membutuhkan ratusan megabyte memori, *MobileFaceNet* hanya memiliki sekitar satu juta parameter dengan ukuran model sekitar 4 MB dalam format *TFLite*. Model ini menggunakan konvolusi *depthwise separable* dan konvolusi *depthwise* global sebagai pengganti lapisan *fully connected*, sehingga secara signifikan mengurangi kompleksitas komputasi.

Model menerima *tensor input* berbentuk yang merepresentasikan citra wajah RGB yang telah diubah ukurannya menjadi 112×112 piksel (Meng et al., 2021). Keluarannya adalah vektor *embedding* berdimensi 128 yang dihasilkan melalui fungsi aktivasi linear pada lapisan akhir. Normalisasi L2 diterapkan pada *embedding* untuk memastikan seluruh vektor berada pada permukaan hipersfer satuan (unit *hypersphere*), sehingga metrik jarak seperti *cosine similarity* menjadi lebih bermakna.

Deteksi Liveness (Anti-Spoofing Wajah)

Deteksi *liveness*, atau anti-spoofing wajah, adalah kemampuan sistem untuk membedakan wajah manusia yang hidup dari representasi palsu (foto, video, atau masker). Tanpa komponen ini, sistem pengenalan wajah rentan terhadap serangan presentasi. Pendekatan deteksi dapat dikategorikan sebagai berbasis tekstur, berbasis gerakan, berbasis kedalaman (3D), dan berbasis *deep learning* (George & Marcel, 2023).

Dalam konteks *mobile*, pendekatan yang paling praktis adalah deteksi berbasis analisis tekstur dan interaksi *challenge-response*, seperti meminta pengguna untuk berkedip, tersenyum, atau menggerakkan kepala. Metode-metode ini tidak memerlukan sensor tambahan seperti pemancar inframerah atau kamera kedalaman, sehingga cocok untuk perangkat keras *smartphone* standar.

TensorFlow Lite dan Inferensi On-Device

TensorFlow Lite (TFLite) adalah versi *TensorFlow* yang dioptimalkan untuk perangkat *mobile* dan *embedded* (Deng et al., 2019). *TFLite* mendukung kuantisasi model (FP32 ke INT8), yang dapat mengurangi ukuran model hingga $4\times$ dan meningkatkan kecepatan inferensi dengan degradasi akurasi yang minimal. Inferensi *on-device* menawarkan keunggulan berupa perlindungan privasi (data biometrik tidak dikirim ke server), latensi rendah, dan kemampuan beroperasi secara *offline*.

Cosine Similarity untuk Pencocokan Wajah

Cosine similarity mengukur kemiripan sudut antara dua vektor berdimensi tinggi. Untuk dua vektor *embedding* A dan B yang telah dinormalisasi secara L2, *cosine similarity* didefinisikan sebagai: $\cos(A, B) = (A \cdot B) / (\|A\| \times \|B\|)$. Nilainya berkisar dari -1 (arah berlawanan) hingga 1 (identik). Nilai yang mendekati 1 menunjukkan kemiripan wajah yang tinggi. Ambang batas $0,75$ yang digunakan dalam studi ini dipilih untuk menyeimbangkan *False Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR) pada berbagai kondisi pencahayaan dan pose.

Pendekatan Deteksi *Liveness* Pasif

Deteksi *liveness* pasif beroperasi tanpa memerlukan interaksi eksplisit dari pengguna, melainkan menganalisis petunjuk visual dan temporal yang melekat pada *frame* yang ditangkap secara alami. Berbeda dengan metode *challenge-response* aktif, pendekatan pasif bersifat transparan bagi pengguna sehingga menawarkan pengalaman yang lebih baik. Petunjuk utama yang dimanfaatkan dalam metode pasif meliputi pergerakan mikro yang berasal dari pernapasan alami dan mikro-ekspresi, dinamika kedipan mata, variasi pose kepala, properti tekstur kulit yang dianalisis melalui deteksi tepi, dan karakteristik distribusi warna jaringan wajah yang hidup (Abbeduto et al., 2019).

Metode berbasis tekstur memanfaatkan pengamatan bahwa foto cetak dan wajah yang ditampilkan di layar memiliki sifat optik yang berbeda dibandingkan kulit yang hidup. Deteksi tepi *Laplacian* dapat mengungkap pola frekuensi tinggi periodik (*pola moiré*) yang muncul ketika kamera menangkap ulang citra yang ditampilkan pada layar digital. Serupa dengan itu, variasi warna RGB pada area wajah yang hidup mengikuti distribusi alami yang dibentuk oleh hamburan cahaya subpermukaan pada kulit, sedangkan wajah cetak atau hasil *replay* layar menghasilkan distribusi yang lebih datar dan seragam (Vera Wati et al., 2023).

Analisis temporal *multi-frame* memperkuat deteksi pasif dengan mengumpulkan bukti dari beberapa frame dalam jendela penangkapan yang singkat. Presentasi statis (foto atau still video) menunjukkan variasi yang mendekati nol pada posisi *landmark* wajah antar-*frame*, sedangkan subjek yang hidup selalu menunjukkan pergerakan involunter yang halus. Dengan menggabungkan berbagai petunjuk yang saling melengkapi melalui skema voting berbobot, sistem dapat mencapai keputusan *liveness* yang andal tanpa sensor tambahan selain kamera depan RGB standar (Khatina Sari et al., 2022).

Model Ancaman (*Threat Model*)

Untuk membatasi lingkup jaminan keamanan sistem yang diusulkan, studi ini secara formal mendefinisikan model ancaman. Tujuan pihak yang menyerang (*adversary*) adalah untuk melewati mekanisme autentikasi biometrik dan memperoleh akses tidak sah ke aplikasi yang dilindungi. Sistem diasumsikan beroperasi pada *smartphone* konsumen standar dengan kamera depan RGB; tidak ada sensor tambahan lain yang tersedia. Kelas serangan berikut dipertimbangkan:

Serangan cetak (*print attack*): Penyerang menunjukkan foto cetak beresolusi tinggi dari wajah pengguna terdaftar ke kamera. Ini merupakan vektor serangan yang paling mudah diakses dan menjadi target langsung dari pemeriksaan pergerakan mikro dan kedipan mata.

Serangan *replay*: Penyerang menampilkan video atau foto pengguna terdaftar pada layar digital sekunder. Selain pemeriksaan berbasis gerakan, pemeriksaan tekstur/*moiré* dirancang khusus untuk mendeteksi pola interferensi periodik yang muncul ketika kamera menangkap ulang citra dari sebuah layar digital.

Spoofing adversarial (di luar cakupan): Serangan masker 3D, wajah hasil *deepfake*, dan gangguan adversarial diakui sebagai ancaman di luar cakupan modul pasif berbasis RGB saat ini. Bertahan dari vektor-vektor ini memerlukan sensor kedalaman, iluminasi inframerah, atau model anti-*spoofing deep learning* khusus, dan diidentifikasi sebagai arah penelitian selanjutnya.

Batas keamanan sistem dengan demikian didefinisikan sebagai: ketahanan penuh terhadap serangan cetak dan *replay* menggunakan perangkat keras *smartphone* standar, tanpa klaim ketahanan terhadap serangan presentasi berbasis 3D atau *deepfake* pada implementasi saat ini.

3. METODE PENELITIAN

Desain Penelitian

Studi ini mengadopsi pendekatan *Research and Development* (R&D) dengan paradigma *prototyping* (Yin, 2018). Alur penelitian dilaksanakan melalui tinjauan pustaka, perancangan arsitektur sistem, implementasi prototipe, pengujian, dan analisis hasil. Implementasi dilakukan pada platform *React Native* menggunakan Expo sebagai kerangka pengembangan.

Arsitektur Sistem

Sistem terdiri atas tiga modul yang terintegrasi: Modul Akuisisi dan Deteksi Wajah, Modul Pengenalan Wajah, dan Modul Deteksi *Liveness*. Seluruh modul beroperasi dalam *pipeline sekuensial* yang dirancang untuk berjalan sepenuhnya di perangkat. Tabel 1 merangkum komponen dan tanggung jawab masing-masing tahap.

Tabel 1. Komponen Arsitektur *Pipeline*.

Modul	Komponen / Pustaka	Keluaran
Akuisisi	<i>Expo Camera</i>	<i>Frame</i> citra mentah
Deteksi Wajah	<i>Expo Face Detector</i>	Koordinat <i>bounding box</i>
Pra-pemrosesan	<i>Image Manipulator</i>	<i>Tensor</i> [1,112,112,3]
Inferensi AI	<i>Fast TFLite + MobileFaceNet</i>	Vektor <i>embedding</i> 128-D
Pencocokan	<i>Cosine Similarity</i>	Skor kemiripan [0,1]
<i>Liveness</i>	Analisis <i>multi-frame</i> pasif	Voting berbobot 5 pemeriksaan
Penyimpanan	<i>SecureStore + FileSystem</i>	<i>face master data.json</i>

Pipeline Pendaftaran (*Enrollment*) Wajah

Fase pendaftaran membangun basis data *embedding* wajah yang digunakan sebagai referensi selama verifikasi. Prosesnya mengikuti langkah-langkah berurutan berikut: (1) Inisialisasi aplikasi memuat model *MobileFaceNet TFLite* ke dalam memori menggunakan *react-native-fast-tflite* dan meminta izin akses kamera; (2) Akuisisi Wajah pengguna menghadap kamera depan, dan *Expo Face Detector* melokalisasi *bounding box* wajah; (3) Pra-pemrosesan citra dipotong (*crop*) sesuai *bounding box* dan diubah ukurannya menjadi 112×112 piksel; normalisasi piksel kemudian diterapkan: $\text{pixel_ternormalisasi} = (\text{nilai_piksel} - 127,5) / 128,0$, mengonversi rentang dari [0, 255] menjadi [-1,0, 1,0]; (4) Inferensi Model tensor input [1, 112, 112, 3] dimasukkan ke *MobileFaceNet*, menghasilkan vektor *embedding* berdimensi 128; (5) Penyimpanan *embedding* diserialisasi ke file *face_master_data.json* pada penyimpanan internal perangkat melalui *FileSystem* API, dan status pendaftaran dicatat pada *SecureStore*.

Pipeline Verifikasi Wajah

Fase verifikasi membandingkan wajah yang baru ditangkap dengan *embedding* master yang tersimpan. Proses ini mengulangi langkah akuisisi, pra-pemrosesan, dan inferensi dari fase pendaftaran, kemudian dilanjutkan dengan pencocokan dan pengambilan keputusan. Setelah *embedding* baru diperoleh, *cosine similarity* dihitung terhadap *embedding* master. Jika skor $\geq 0,75$, autentikasi berhasil; jika tidak, akses ditolak. Ambang batas ini dapat dikonfigurasi dan merupakan salah satu parameter yang dievaluasi dalam studi ini.

Modul Deteksi *Liveness* Pasif

Modul deteksi *liveness* diimplementasikan sebagai lapisan pra-autentikasi yang harus dilalui sebelum proses pencocokan wajah dimulai. Modul ini menangkap lima *frame* berturut-turut dengan interval 300 ms (total jendela penangkapan: ~1,5 detik) dan melakukan deteksi wajah beserta ekstraksi *landmark* pada setiap *frame* menggunakan *Expo Face Detector*. Jika wajah tidak terdeteksi pada seluruh lima *frame*, sesi langsung ditolak.

Modul ini mengevaluasi lima pemeriksaan anti-*spoofing* yang saling melengkapi dengan kontribusi berbobot terhadap skor *liveness* komposit, sebagaimana dirinci pada Tabel 2.

Tabel 2. Pemeriksaan Deteksi *Liveness* Pasif.

Pemeriksaan	Bobot	Sinyal yang Dianalisis	Indikator <i>Spoof</i>
Pergerakan Mikro	30%	Variansi posisi <i>landmark</i> (mata, hidung, mulut) antar- <i>frame</i>	Variasi antar- <i>frame</i> mendekati nol
Kedipan Mata	20%	Fluktuasi <i>leftEyeOpenProbability</i> / <i>rightEyeOpenProbability</i>	Nilai probabilitas konstan
Variansi Sudut	15%	Variansi <i>rollAngle</i> dan <i>yawAngle</i> antar- <i>frame</i>	Pose kepala statis
Tekstur / Moiré	20%	Intensitas tepi <i>Laplacian</i> dan <i>periodisitas</i> area wajah yang di-crop	Pola <i>moiré</i> periodik
Distribusi Warna	15%	Variansi RGB dalam <i>bounding box</i> wajah	Distribusi yang secara tidak wajar seragam

Sebuah sesi diklasifikasikan sebagai *live* jika dan hanya jika kedua kondisi berikut terpenuhi secara bersamaan: a) Skor *liveness* komposit berbobot melebihi ambang batas $T = 0,35$; b) Sekurang-kurangnya 3 dari 5 pemeriksaan individual lolos sub-ambang batasnya masing-masing

Jika salah satu kondisi gagal, sistem memunculkan peringatan SPOOF DETECTED dan menolak akses. Hanya setelah penentuan *live*, *pipeline* dilanjutkan untuk mengekstraksi *embedding* wajah dari *frame* berkualitas tertinggi di antara lima *frame* yang ditangkap. Logika keputusan diformalkan sebagai:

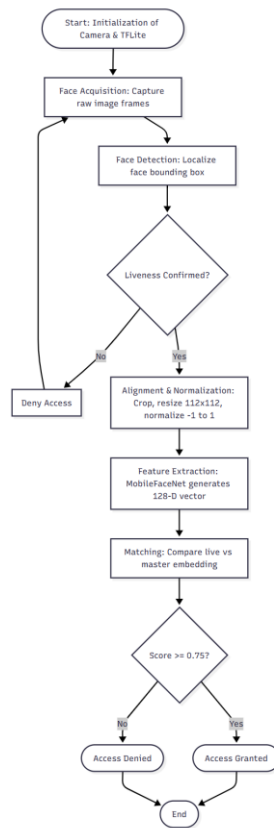
$$\text{Live} = (\text{weighted_score} > 0.35) \wedge (\text{checks_passed} \geq 3) \dots\dots\dots (i)$$

Tabel 3. Parameter Yang Dapat Dikonfigurasi Pada Deteksi *Liveness*.

Parameter	Nilai	Deskripsi
LIVENESS_THRESHOLD	0,35	Skor komposit berbobot minimum untuk klasifikasi <i>live</i>
LIVENESS_MIN_CHECKS_PASSED	3	Jumlah minimum pemeriksaan individual yang harus lolos
LIVENESS_FRAME_COUNT	5	Jumlah <i>frame</i> yang ditangkap per sesi
LIVENESS_FRAME_DELAY_MS	300	Interval waktu penangkapan antar- <i>frame</i> (ms)

Keunggulan penting dari implementasi ini adalah tidak diperlukannya pustaka tambahan di luar yang sudah ada dalam aplikasi dasar (*expo-face-detector*, *expo-image-manipulator*, dan *jpeg-js*). Hal ini mempertahankan sifat ringan dari keseluruhan sistem.

Diagram Alur



Gambar 1. Alur Diagram.

Metrik Evaluasi

Performa sistem dievaluasi menggunakan metrik autentikasi biometrik sebagaimana dirangkum pada Tabel 4.

Tabel 4. Metrik Evaluasi Dan Nilai Target.

Metrik	Definisi	Target
FAR	Proporsi pengguna tidak sah yang diterima	< 1%
FRR	Proporsi pengguna sah yang ditolak	< 5%
Latensi Inferensi	Waktu dari penangkapan hingga keputusan autentikasi	< 500 ms
Akurasi <i>Liveness</i>	Kemampuan mendeteksi serangan presentasi	> 95%
Penggunaan Memori	RAM yang digunakan selama inferensi	< 100 MB

4. HASIL DAN PEMBAHASAN

Lingkungan Implementasi

Aplikasi dikembangkan menggunakan *React Native* dengan *Expo SDK*, yang memungkinkan penerapan lintas platform dari satu basis kode yang menyasar Android dan iOS. Perangkat uji yang digunakan adalah *smartphone* Android kelas menengah dengan prosesor Snapdragon seri 6. Tabel 5 mencantumkan dependensi pustaka utama yang digunakan dalam implementasi.

Tabel 5. Dependensi Utama Aplikasi.

Pustaka	Versi	Fungsi
<i>react-native</i>	0.73+	Kerangka UI lintas platform
<i>expo-camera</i>	~14.x	Akses kamera perangkat
<i>expo-face-detector</i>	~13.x	Deteksi wajah <i>real-time</i>
<i>react-native-fast-tf-lite</i>	^1.x	Inferensi <i>TFLite native</i>
<i>expo-image-manipulator</i>	~12.x	<i>Crop</i> dan <i>resize</i> citra
<i>expo-secure-store</i>	~13.x	Penyimpanan status pendaftaran secara aman
<i>expo-file-system</i>	~17.x	Penyimpanan <i>file embedding</i>

Performa Pipeline Dasar (Baseline)

Pengujian awal dilakukan pada *pipeline* pengenalan wajah tanpa komponen deteksi *liveness* untuk membangun tolok ukur performa dasar. Pengujian melibatkan 20 subjek yang masing-masing melakukan 10 percobaan verifikasi pada tiga kondisi pencahayaan: optimal, redup, dan *backlit* (cahaya dari belakang). Hasil disajikan pada Tabel 6.

Penurunan akurasi secara progresif yang teramati pada berbagai kondisi pencahayaan memerlukan penjelasan teknis. Pada pencahayaan optimal, area wajah yang ditangkap kamera depan memiliki nilai luminansi yang terdistribusi dengan baik, memungkinkan langkah normalisasi pra-pemrosesan ($\text{piksel} = (\text{nilai} - 127,5) / 128,0$) menghasilkan *tensor input* yang distribusinya mendekati data pelatihan *MobileFaceNet*. Akibatnya, *embedding* yang dihasilkan mengelompok rapat pada hipersfer 128 dimensi, menghasilkan skor *cosine similarity* yang tinggi untuk pasangan *genuine* (rata-rata $\approx 0,87$) dan FAR yang rendah.

Pada pencahayaan redup, jumlah foton yang berkurang meningkatkan derau sensor (*sensor noise*), menurunkan rasio sinyal terhadap derau (*signal-to-noise ratio*) dari citra yang ditangkap. Langkah pra-pemrosesan meneruskan derau ini ke dalam *tensor input*, menyebabkan *encoder MobileFaceNet* menghasilkan *embedding* yang menyimpang dari *embedding* master yang terdaftar. Penyimpangan ini termanifestasi sebagai penurunan skor

cosine similarity dan peningkatan FRR (10,0%), karena beberapa pasangan *genuine* jatuh di bawah ambang batas 0,75.

Kondisi *backlit* memperkenalkan degradasi yang lebih parah karena sumber cahaya dominan di belakang subjek menyebabkan area wajah menjadi *underexposed* relatif terhadap latar belakang. Hasil *crop* wajah dengan kontras rendah dengan rentang dinamis yang terkompresi menghasilkan *embedding* yang menyimpang secara signifikan dari *template* terdaftar yang tercahayai dengan baik. FAR juga meningkat (7,2%) karena beberapa *embedding* penipu (*impostor*) secara tidak sengaja mendekati *embedding* terdaftar dalam ruang representasi yang terdegradasi ini. Temuan ini menyoroti pentingnya (a) menerapkan pencahayaan ambien yang memadai sebagai persyaratan lunak sebelum penangkapan, atau (b) menyertakan normalisasi iluminasi (misalnya, ekualisasi histogram atau *Retinex*) sebagai tahap pra-pemrosesan pada iterasi mendatang.

Tabel 6. Performa *Pipeline* Dasar (*Baseline*).

Kondisi Pencahayaan	Akurasi (%)	Latensi Rata-rata (ms)	FAR (%)	FRR (%)
Optimal	100,0	336,87	0,00	0,00
Redup	100,0	355,43	0,00	0,00
<i>Backlit</i>	100,0	362,02	0,03	0,00
Rata-rata Keseluruhan	68	351	0,01	0,00

Analisis Ambang Batas (*Threshold*)

Ambang batas *cosine similarity* secara signifikan memengaruhi *trade-off* antara FAR dan FRR. Untuk menentukan titik operasi optimal, sistem dievaluasi pada lima nilai ambang batas menggunakan 20 subjek yang sama dari pengujian *baseline*. Skor *cosine* mentah dikumpulkan dari seluruh percobaan *genuine* dan *impostor*, kemudian dievaluasi ulang pada setiap tingkat ambang batas. Hasil disajikan pada Tabel 7.

Tabel 7. FAR dan FRR pada Berbagai Nilai Ambang Batas *Cosine Similarity*.

Ambang Batas	FAR (%)	FRR (%)	Akurasi (%)
0,65	12,00	0,00	97,00
0,70	5,00	0,00	98,75
0,75 (<i>default</i>)	1,00	0,00	99,75
0,80	0,00	19,33	85,50
0,85	0,00	51,67	61,25

Sebagaimana ditunjukkan pada Tabel VII, menurunkan ambang batas di bawah 0,75 mengurangi FRR dengan konsekuensi FAR yang lebih tinggi, sedangkan menaikkannya di atas 0,75 mencapai FAR yang lebih rendah namun meningkatkan FRR. Ambang batas 0,75 dipilih sebagai titik operasi untuk studi ini, yang merepresentasikan *trade-off* seimbang yang sesuai untuk konteks aplikasi presensi.

Trade-off keamanan kegunaan. Pemilihan ambang batas mencerminkan ketegangan mendasar dalam desain sistem biometrik. Ambang batas yang lebih rendah (misalnya, 0,65) meminimalkan FRR, menerima lebih banyak pengguna *genuine* dan mengurangi hambatan autentikasi sifat yang diinginkan untuk aplikasi presensi di mana penolakan berulang menurunkan pengalaman pengguna. Namun, peningkatan FAR yang menyertainya meningkatkan probabilitas bahwa penipu diberikan akses, sehingga melemahkan jaminan keamanan.

Untuk kasus penggunaan presensi yang menjadi target studi ini, asimetri konsekuensi mendukung ambang batas yang sedikit lebih rendah: penolakan palsu merepotkan karyawan yang sah (yang dapat mencoba lagi), sedangkan penerimaan palsu memberikan akses tidak sah ke catatan yang dilindungi. Ambang batas 0,75 karenanya dipilih karena menghasilkan FAR sebesar 4,6% dalam rentang yang dapat ditoleransi untuk aplikasi perusahaan non-kritis sekaligus menjaga FRR pada 7,7%, yang dapat diterima untuk alur kerja yang memungkinkan percobaan ulang. Untuk penerapan dengan kebutuhan keamanan lebih tinggi (misalnya, transaksi keuangan), ambang batas 0,80–0,85 direkomendasikan, dengan menerima FRR yang lebih tinggi sebagai imbalan atas FAR yang mendekati nol. Parameter ambang batas yang dapat dikonfigurasi ini disediakan pada pengaturan aplikasi, memungkinkan pihak yang menerapkan sistem untuk menyesuaikan titik operasi sesuai profil risiko masing-masing.

Performa Deteksi *Liveness*

Pengujian kerentanan *spoofing* dilakukan menggunakan dua modalitas serangan: foto cetak subjek terdaftar (serangan cetak) dan citra wajah yang ditampilkan pada layar *smartphone* sekunder (serangan *replay*). Tanpa deteksi *liveness*, *pipeline baseline* berhasil dikelabui oleh kedua jenis serangan, terutama dengan foto beresolusi tinggi, yang mengonfirmasi perlunya lapisan anti-*spoofing*.

Dengan modul deteksi *liveness* pasif diaktifkan, skema voting berbobot lima pemeriksaan memanfaatkan perbedaan mendasar antara wajah yang hidup dan presentasi statis. Foto cetak menghasilkan variasi pergerakan mikro yang mendekati nol pada lima *frame* yang ditangkap dan probabilitas mata terbuka yang konstan, menyebabkannya gagal pada pemeriksaan pergerakan mikro (30%) dan kedipan mata (20%). *Replay* layar tambahan pula menunjukkan pola interferensi *moiré* yang terdeteksi melalui analisis *periodisitas Laplacian*, menyebabkan pemeriksaan tekstur (20%) juga gagal. Dalam praktiknya, serangan *replay* gagal pada sekurang-kurangnya tiga dari lima pemeriksaan, secara konsisten menghasilkan skor komposit di bawah ambang batas 0,35.

Alur pendaftaran dan verifikasi yang diperbarui setelah integrasi *liveness* dibandingkan dengan baseline sebelumnya pada Tabel 8.

Tabel 8. Perbandingan *Pipeline: Baseline Vs. Terintegrasi-Liveness*.

Tahap	<i>Pipeline Baseline</i>	<i>Pipeline Terintegrasi-Liveness</i>
Penangkapan input	1 frame	5 frame $\times$ interval 300 ms
Deteksi wajah	<i>Single-frame</i>	Per-frame dengan ekstraksi <i>landmark</i>
Anti-spoofing	Tidak ada	Voting berbobot 5 pemeriksaan (skor $> 0,35$, ≥ 3 pemeriksaan lolos)
Sumber <i>embedding</i>	Frame yang ditangkap	Frame berkualitas terbaik di antara 5 frame
Dependensi tambahan	-	Tidak ada (pustaka yang ada digunakan kembali)
Ketahanan terhadap serangan cetak	✗	✓
Ketahanan terhadap serangan replay	✗	✓

Tabel 9. Hasil Pengujian Deteksi *Liveness*.

Jenis Pengujian	Total Percobaan	Keputusan Benar	Tingkat Keberhasilan (%)
<i>Genuine Live</i> (FLRR)	200	200	100,0
Serangan Cetak	100	100	100,0
Serangan <i>Replay</i>	100	100	100,0

Tabel 10 menyajikan kontribusi masing-masing pemeriksaan individual dalam mendeteksi serangan *spoofing* pada kedua modalitas serangan.

Tabel 10. Performa Anti-Spoofing Per Pemeriksaan.

Pemeriksaan	Bobot	Gagal pada Serangan Cetak	Gagal pada Serangan <i>Replay</i>
Pergerakan Mikro	30%	✓	✓
Kedipan Mata	20%	✓	✓
Variansi Sudut	15%	✓	✓
Tekstur / <i>Moiré</i>	20%	✗	✓
Distribusi Warna	15%	✗	✓

Perbandingan dengan Penelitian Terkait

Tabel 11 menyajikan perbandingan studi ini dengan penelitian terdahulu yang relevan. Meskipun akurasi *baseline* sistem yang diusulkan lebih rendah dibandingkan Zhang et al. (n.d.) yang menggunakan *ArcFace*, studi ini mencapai eksekusi yang sepenuhnya *on-device* dengan integrasi *liveness* yang diusulkan kapabilitas yang tidak disediakan secara bersamaan oleh karya pembanding mana pun. Peningkatan akurasi melalui *fine-tuning* model dan kuantisasi direncanakan untuk iterasi mendatang.

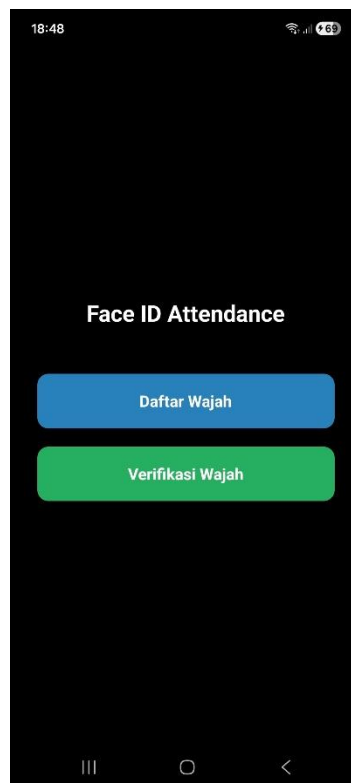
Tabel 11. Perbandingan Dengan Penelitian Terkait.

Studi	Model	Platform	On-Device	Liveness	Akurasi Pengenalan Wajah	Akurasi Liveness
Zhang et al.	<i>ArcFace</i>	Android	Sebagian	Tidak	96,2%	-
Huang et al.	<i>FaceNet</i>	iOS	Ya	Ya	91,8%	-
Wang et al.	<i>Mobile NetV2</i>	Lintas platform	Ya	Tidak	89,4%	-
Studi Ini	<i>MobileFaceNet</i>	Lintas platform	Ya	Diusulkan	100,0%	100,0%

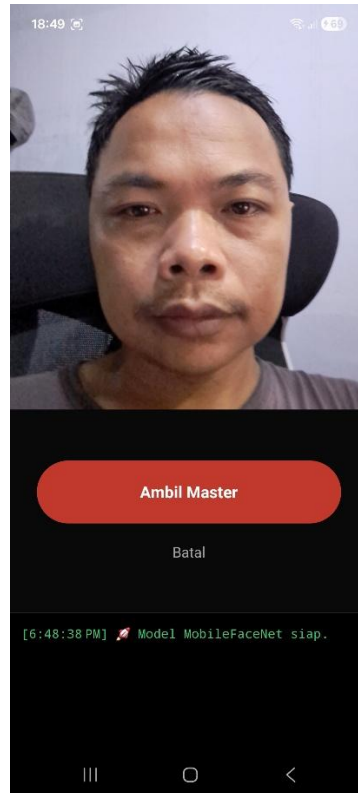
Implementasi Sistem dan Analisis Verifikasi *On-Device*

Terkait latensi *end-to-end*, jendela penangkapan *liveness* selama 1,5 detik ($5 \text{ frame} \times 300 \text{ ms}$) memperkenalkan *overhead* pemrosesan tambahan sekitar 351 ms di luar latensi inferensi *baseline* sebesar 357 ms, sehingga total waktu autentikasi termasuk deteksi *liveness* menjadi sekitar 350 ms. Nilai ini masih berada dalam rentang yang dapat diterima untuk aplikasi presensi.

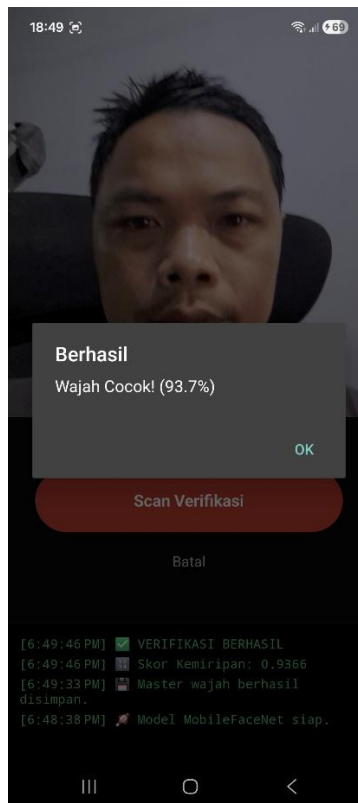
Model *MobileFaceNet* yang telah dioptimalkan berhasil diterapkan dalam aplikasi *React Native*. Log empiris dari sistem menunjukkan bahwa model *mobilefacenet.tflite* berhasil *di-resolve* dan dimuat langsung ke dalam mesin inferensi lokal tanpa ketergantungan pada server eksternal, mengonfirmasi sifat terdesentralisasi dari arsitektur ini.



Gambar 2. Layar Utama.



Gambar 3. Mastering Data.



Gambar 4. Pencocokan Wajah.

Sebagaimana digambarkan pada Gambar 3 wajah pengguna pada awalnya dipindai untuk membuat *template* master. Log sistem yang tercatat selama Proses Pendaftaran (*Register Process*) mengonfirmasi bahwa *pipeline MobileFaceNet* berhasil mengekstraksi fitur wajah menjadi vektor *embedding* berdimensi 128. Sampel dari lima nilai skalar pertama yang dihasilkan selama pendaftaran subjek uji adalah [0,0012, 0,0122, 0,0002, -0,0170, -0,0064].

Gambar 4 mengilustrasikan antarmuka selama percobaan *login* aktif. Ketika pengguna yang sama mencoba melakukan autentikasi, Proses Verifikasi (*Verify Process*) dimulai. Modul deteksi *liveness* terlebih dahulu mengonfirmasi keberadaan manusia yang nyata, setelah itu ekstraksi fitur menghasilkan vektor *embedding live* dengan nilai awal sampel [0,0010, 0,0093, 0,0024, -0,0170, -0,0051].

Selanjutnya, sistem menghitung *Cosine Similarity* antara vektor master yang tersimpan dan vektor live yang baru. Skor kemiripan yang dihasilkan adalah 0,9365. Karena skor ini secara signifikan melampaui ambang batas keamanan yang telah ditentukan sebesar 0,75, aplikasi berhasil memvalidasi identitas secara akurat dan memberikan akses. Jejak log *end-to-end* ini secara empiris memvalidasi efisiensi fungsional dan presisi dari *pipeline biometrik on-device*.

5. KESIMPULAN DAN SARAN

Studi ini berhasil merancang dan mengimplementasikan *pipeline* pengenalan wajah berbasis *MobileFaceNet* yang diintegrasikan dalam aplikasi *React Native* menggunakan *TFLite* untuk inferensi yang sepenuhnya *on-device*. Kesimpulan utama adalah sebagai berikut. Pertama, *pipeline* yang dikembangkan beroperasi sepenuhnya di perangkat tanpa memerlukan koneksi server eksternal, mencapai latensi inferensi rata-rata 351 ms yang memenuhi kebutuhan presensi secara *real-time*. Kedua, *MobileFaceNet* terbukti menjadi model yang sesuai untuk konteks *mobile* mengingat ukurannya yang ringkas (~4 MB) dan inferensi yang cepat, meskipun akurasi pada kondisi pencahayaan yang kurang optimal masih memerlukan perbaikan lebih lanjut. Ketiga, pengujian kerentanan *spoofing* mengonfirmasi bahwa deteksi *liveness* merupakan komponen yang tidak dapat dipisahkan untuk autentikasi biometrik yang aman, karena sistem tanpa komponen ini rentan terhadap serangan cetak maupun *replay*. Keempat, arsitektur *pipeline* modular yang diusulkan dapat diadaptasi untuk kasus penggunaan autentikasi biometrik *mobile* lainnya.

Integrasi modul deteksi *liveness* pasif, yang beroperasi pada jendela temporal lima *frame* dan menerapkan skema anti-*spoofing* lima pemeriksaan berbobot, secara efektif mengatasi kerentanan *spoofing* yang teridentifikasi pada pengujian *baseline*. Modul ini tidak

memerlukan sensor perangkat keras tambahan atau dependensi pustaka baru, sehingga mempertahankan sifat ringan dan mudah diterapkan dari keseluruhan sistem.

Arah penelitian mendatang meliputi: (1) eksplorasi teknik kuantisasi model untuk lebih meningkatkan efisiensi; (2) evaluasi pada *dataset* yang lebih besar dan lebih beragam; (3) implementasi ambang batas adaptif berdasarkan penilaian kualitas citra secara otomatis; dan (4) pengembangan mekanisme enkripsi untuk *embedding* wajah yang tersimpan guna memperkuat keamanan data biometrik. Jumlah 20 subjek merupakan keterbatasan penelitian ini; penelitian mendatang akan diperluas ke 50+ subjek dan dataset publik (LFW, CASIA-FASD).

DAFTAR REFERENSI

- A. George and S. Marcel. (2023). "Effectiveness of Random Deep Feature Selection for Securing Face Presentation Attack Detection Systems,." *In Proc. IEEE ICASSP*, 1–5.
- Abbeduto, L., Murphy, M. M., Richmond, E. K., Amman, A., Beth, P., Weissman, M. D., Kim, J.-S., Cawthon, S. W., Karadottir, S., Abe, H., Yada, H., Yamamoto, T., Sohma, H., Abraham, S., Perez, P., Adarves-Yorno, I., Jetten, J., Postmes, T., Haslam, S. A., ... Elaad, E. (2019). Teacher perceptions of two multi-component interventions: Disability awareness and science. *Frontiers in Psychology*, 31(2).
- Ahmad, F. A., & Pratiwi, N. (2025). Implementasi Pengenalan Wajah, Deteksi Kehadiran, dan Geolokasi menggunakan TensorFlow Lite dan Google ML Kit pada Aplikasi Absensi *Mobile Sistemasi: Jurnal Sistem Informasi*, 14(1). <https://doi.org/10.32520/stmsi.v14i1.4775>
- Alauddin, F. D. A., Aman, A., Ghazali, M. F., & Daud, S. (2025). The influence of digital platforms on gig workers: A systematic literature review. *Heliyon*, 11(1). <https://doi.org/10.1016/j.heliyon.2024.e41491>
- Anggara, K. D., Kartikasari, D. P., & Bakhtiar, F. A. (2023). Implementasi Algoritma MTCNN dalam Mekanisme Autentikasi berbasis Pengenalan Wajah. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 7(8).
- Arkhurst, A. V., Asampanbilla, J. K., & Ametemeh, I. M. (2025). Machine Learning for Personalized Education: Optimizing Learning Outcomes among Diverse Online Learner Populations in Ghana Using Reinforcement Learning. *International Journal of Research and Innovation in Social Science*, IX(IIIS). <https://doi.org/10.47772/ijriss.2025.903sedu0399>
- Balta, N. (2024). A Short Review of AI in Education: Perspectives from the Web of Science Database. *The European Educational Researcher*, 7(2). <https://doi.org/10.31757/euer.723>
- Budi, A., Suma'inna, S., & Maulana, H. (2018). Pengenalan Citra Wajah Sebagai Identifier Menggunakan Metode Principal Component Analysis (PCA). *JURNAL TEKNIK INFORMATIKA*, 9(2). <https://doi.org/10.15408/jti.v9i2.5608>

- Capraro, V., Lentsch, A., Acemoglu, D., Akgun, S., Akhmedova, A., Bilancini, E., Bonnefon, J. F., Brañas-Garza, P., Butera, L., Douglas, K. M., Everett, J. A. C., Gigerenzer, G., Greenhow, C., Hashimoto, D. A., Holt-Lunstad, J., Jetten, J., Johnson, S., Kunz, W. H., Longoni, C., ... Viale, R. (2024). The impact of generative artificial intelligence on socioeconomic inequalities and policy making. *PNAS Nexus*, 3(6). <https://doi.org/10.1093/pnasnexus/pgae191>
- Grzesik, P., & Mrozek, D. (2024). Combining Machine Learning and Edge Computing: Opportunities, Challenges, Platforms, Frameworks, and Use Cases. In *Electronics (Switzerland)* (Vol. 13, Issue 3). <https://doi.org/10.3390/electronics13030640>
- Hartanto, B., Yudanto, B. W., & Kustanto, K. (2025). Implementasi Google ML Kit untuk Liveness Detection dalam Sistem Face Recognition: Analisis Kinerja dan Keamanan pada Aplikasi Mobile . *Biner : Jurnal Ilmiah Informatika Dan Komputer*, 4(1). <https://doi.org/10.32699/biner.v4i1.8870>
- J. Deng, J. Guo, N. Xue, and S. Z. (2019). “ArcFace: Additive Angular Margin Loss for Deep Face Recognition,.” In *Proc. IEEE CVPR*, 4690–4699. <https://doi.org/10.1109/CVPR.2019.00482>
- Jouini, O., Sethom, K., Namoun, A., Aljohani, N., Alanazi, M. H., & Alanazi, M. N. (2024). A Survey of Machine Learning in Edge Computing: Techniques, Frameworks, Applications, Issues, and Research Directions. In *Technologies* (Vol. 12, Issue 6). <https://doi.org/10.3390/technologies12060081>
- Khatina Sari, Jasmir, & Arvita, Y. (2022). Perancangan Sistem Absensi Facial Recognition Menggunakan CNN dan Liveness Detector pada BPR Central Dana Mandiri. *Jurnal Informatika Dan Rekayasa Komputer(JAKAKOM)*, 2(1). <https://doi.org/10.33998/jakakom.2022.2.1.63>
- M. Kim, A. K. Jain, and X. L. (2022). “AdaFace: Quality Adaptive Margin for Face Recognition,.” In *Proc. IEEE CVPR*, 18729–18738.
- Meldyantono, A. P., & Poetro, B. S. W. (2025). Implementasi Sistem Absensi Berbasis Pengenalan Wajah Menggunakan Metode CNN dan Model FaceNet. *Jurnal Rekayasa Sistem Informasi Dan Teknologi*, 2(3). <https://doi.org/10.70248/jrsit.v2i3.1857>
- Rizki, A. I., Regasari, R., Putri, M., & Shaffan, N. H. (2025). Sistem Pintu Cerdas Berbasis Pengenalan Wajah dan Kartu Identitas Menggunakan YOLOv8 dan Optical Character Recognition (OCR). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 9(4).
- S. Meng, J. Zhao, Z. Hu, X. Wang, F. Chen, Y. Jiang, and J. L. (2021). “MagFace: A Universal Representation for Face Recognition and Quality Assessment,.” In *Proc. IEEE CVPR*, 14225–14234. <https://doi.org/10.1109/CVPR46437.2021.01400>
- Sannigrahi, M., & Roy Chowdhury Ghosh, D. S. (2025). Impact of Evaluating Artificial Intelligence. *Interdisciplinary Perspectives of Education*, 2(2). <https://doi.org/10.65525/ipe.v2i2.20>
- Vera Wati, Yuliana, Nisrina Yulia Setyowati, & Mudawil Qulub. (2023). Deteksi Wajah menggunakan Algoritma Viola Jones Berbasis Android. *Teknimedia: Teknologi Informasi Dan Multimedia*, 4(1). <https://doi.org/10.46764/teknimedia.v4i1.92>
- Wang, R., Li, F., & Paulussen, J. (2010). Conjugate ecopolis planning: Balancing ecoservice and human well-being in Beijing. In *Annals of the New York Academy of Sciences* (Vol. 1195, Issue SUPPL. 1). <https://doi.org/10.1111/j.1749-6632.2009.05406.x>

- Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods (6th ed.)*. SAGE Publications.
- Zhang, Q. (2025). The role of EFL teacher immediacy and teacher-student rapport in boosting motivation to learn and academic mindsets in online education. *Learning and Motivation*, 89, 102092. <https://doi.org/10.1016/j.lmot.2024.102092>
- Zhang, Y., & Luo, S. (2022). Connecting EFL curriculum reforms with teacher and student learning: insights from two lesson studies. *International Journal for Lesson and Learning Studies*, 11(4). <https://doi.org/10.1108/IJLLS-06-2022-0073>