

Arsitektur Verifikasi Biometrik Menggunakan YOLOv8 dan ArcFace untuk Validasi Identitas pada Platform Ta'aruf Islami Zawajna

Biometric Verification Architecture Using YOLOv8 and ArcFace for Identity Validation on the Zawajna Islamic Ta'aruf Platform

Nida Kamilia, Oddy Virgantara Putra, Widya Kurniawan*

Teknik Informatika, Universitas Darussalam Gontor, Ponorogo, Indonesia

E-mail: nidak0181@gmail.com

Abstract. This research aims to implement a facial biometric verification system on an Islamic matchmaking platform Zawajna to prevent profile identity fraud or catfishing. The system works by validating the authenticity of each new profile picture uploaded by the user against a previously verified genuine face serving as master data. Model performance testing was conducted using 79 image datasets consisting of 33 genuine subject images and 46 imposter images. This study comparatively evaluates four combinations of face detection and recognition architectures: RetinaFace with ArcFace, YOLOv8 with ArcFace, YOLOv8 with FaceNet, and YOLOv8 with GhostFaceNet. The main evaluation metrics include Accuracy, Precision, Recall, and execution speed. The evaluation results showed that RetinaFace + ArcFace achieved the highest accuracy (88.61%) but was highly inefficient with extreme computational time spikes of over 700 seconds. In contrast, the YOLOv8 + ArcFace architecture is recommended as a solution providing a well-balanced performance trade-off. This model produced 87.34% Accuracy, 84.85% Precision, and 84.85% Recall, supported by a stable average processing time of under 3 seconds. This combination has proven to be efficient and demonstrates adequate reliability for real-time profile identity validation operations within the scope of this limited testing.

Keywords: Biometrics, YOLOv8, ArcFace, Ta'aruf

Abstrak. Penelitian ini bertujuan untuk mengimplementasikan sistem verifikasi biometrik wajah pada platform matchmaking Islami Zawajna guna mencegah pemalsuan identitas profil atau catfishing. Sistem ini bekerja dengan memvalidasi keaslian setiap foto profil baru yang diunggah pengguna terhadap wajah asli yang telah terverifikasi sebelumnya sebagai data master. Pengujian kinerja model dilakukan menggunakan 79 dataset citra yang terdiri dari 33 citra subjek asli dan 46 citra imposter. Penelitian ini mengevaluasi empat kombinasi arsitektur deteksi dan pengenalan wajah secara komparatif: RetinaFace dengan ArcFace, YOLOv8 dengan ArcFace, YOLOv8 dengan FaceNet, serta YOLOv8 dengan GhostFaceNet. Metrik evaluasi utama mencakup Akurasi, Presisi, Recall, dan kecepatan eksekusi. Hasil pengujian menunjukkan bahwa RetinaFace + ArcFace mencapai akurasi tertinggi (88,61%) namun sangat lambat dengan lonjakan waktu komputasi hingga lebih dari 700 detik. Sebaliknya, arsitektur YOLOv8 + ArcFace direkomendasikan sebagai solusi yang memberikan keseimbangan performa (trade-off) yang memadai. Model ini menghasilkan tingkat Akurasi 87,34%, Presisi 84,85%, dan Recall 84,85%, didukung oleh rata-rata waktu pemrosesan stabil di bawah 3 detik. Kombinasi ini terbukti efisien dan menunjukkan tingkat keandalan yang cukup baik untuk operasional sistem validasi identitas profil secara real-time berdasarkan batasan skala data uji pada penelitian ini.

Kata kunci: Biometrik, YOLOv8, ArcFace, Ta'aruf

Submitted: 14-09-2026 | Accepted: 24-09-2026 | Published: 30-09-2026

How to Cite:

N. Kamilia, O. V. Putra And W. Kurniawan, "Arsitektur Verifikasi Biometrik Menggunakan YOLOv8 dan ArcFace untuk Validasi Identitas pada Platform Ta'aruf Islami Zawajna" Journal of Information System and Application Development (JISAD), vol. 4, no. 2, pp.80-86, 2026, doi: 10.26905/jisad.v4i2.17744



PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi digital di berbagai sektor, termasuk dalam proses pencarian pasangan hidup melalui platform matchmaking [1]. Dalam konteks pencarian pasangan secara Islami atau taaruf, integritas, keamanan, dan kejujuran identitas pengguna merupakan fondasi utama [2]. Namun, salah satu ancaman terbesar pada platform matchmaking masa kini adalah fenomena catfishing atau pemalsuan identitas profil, di mana seorang pengguna menggunakan foto wajah orang lain untuk mengelabui pengguna lainnya [3].

Untuk mengatasi permasalahan tersebut, diperlukan sebuah sistem validasi identitas yang andal, menyerupai standar *Electronic Know Your Customer (e-KYC)* yang banyak diterapkan pada aplikasi perbankan digital [4]. Dalam pendekatan ini, pengguna diwajibkan melakukan verifikasi wajah awal untuk dijadikan sebagai data master. Selanjutnya, setiap kali pengguna mengunggah atau mengganti foto profil pada sistem, algoritma harus secara otomatis memvalidasi apakah wajah pada foto profil baru tersebut benar-benar milik pengguna yang sama dengan data master. Hal ini menuntut adanya sistem pengenalan wajah (*face recognition*) yang beroperasi secara akurat sekaligus cepat (*real-time*) di sisi server [5].

Berbagai arsitektur deep learning telah dikembangkan secara masif untuk tahapan deteksi wajah (*face detection*) dalam satu dekade terakhir. Penelitian-penelitian sebelumnya menunjukkan bahwa model berbasis *Convolutional Neural Network (CNN)* seperti RetinaFace memiliki tingkat akurasi lokalisasi wajah yang sangat tinggi dalam menangani berbagai variasi pose, oklusi, dan pencahayaan [6]. Di tahapan ekstraksi fitur dan verifikasi, model seperti ArcFace, FaceNet, serta arsitektur ringan adaptasi terbaru seperti GhostFaceNet menawarkan pendekatan yang berbeda-beda dalam menghitung jarak vektor kemiripan antar wajah [7], [8].

Meskipun model konvensional seperti RetinaFace sangat unggul secara presisi, penerapannya secara operasional pada sistem berbasis web seringkali menimbulkan kendala serius pada waktu komputasi (*computational time*). Beban komputasi yang terlalu berat dapat menyebabkan lonjakan waktu pemrosesan (*spike*) yang ekstrem, sehingga menurunkan tingkat responsivitas aplikasi dan kenyamanan pengguna secara signifikan. Sebagai solusi alternatif untuk mengatasi lambatnya waktu inferensi, *You Only Look Once versi 8 (YOLOv8)* yang pada dasarnya merupakan algoritma deteksi objek state-of-the-art, telah terbukti memiliki kecepatan dan efisiensi yang sangat tinggi [9].

Penggunaan YOLOv8 sebagai modul deteksi mandiri yang dipadukan dengan berbagai model pengenalan wajah menjanjikan efisiensi waktu eksekusi tanpa mengorbankan terlalu banyak *trade-off* pada sisi akurasi. Berdasarkan latar belakang dan identifikasi masalah tersebut, penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi kinerja sistem verifikasi biometrik wajah pada platform matchmaking Islami berbasis web bernama Zawajna. Penelitian ini akan menguji dan membandingkan empat arsitektur kombinasi secara komparatif, yaitu RetinaFace + ArcFace, YOLOv8 + ArcFace, YOLOv8 + FaceNet, dan YOLOv8 + GhostFaceNet. Evaluasi kinerja difokuskan pada pencarian keseimbangan optimal (*golden mean*) antara metrik performa klasifikasi yang mencakup Akurasi, Presisi, dan Recall, dengan metrik kecepatan eksekusi (detik). Hasil dari penelitian ini diharapkan dapat memberikan rekomendasi arsitektur AI yang paling andal, efisien, dan siap diimplementasikan untuk mencegah pemalsuan identitas profil secara real-time di lingkungan operasional platform matchmaking.

METODE

Penelitian ini menggunakan rancangan penelitian kuantitatif eksperimental yang berfokus pada pengujian dan komparasi kinerja algoritma kecerdasan buatan untuk sistem verifikasi biometrik [10]. Variabel independen dalam penelitian ini adalah variasi kombinasi arsitektur deteksi dan pengenalan wajah yang terdiri dari empat skenario: RetinaFace dipadukan dengan ArcFace [6], [7], YOLOv8 dipadukan dengan ArcFace [2], [4], YOLOv8 dipadukan dengan FaceNet [11], serta YOLOv8 dipadukan dengan GhostFaceNet [7]. Sementara itu, variabel dependen yang diukur untuk mengevaluasi kinerja masing-masing model meliputi tingkat Akurasi (*Accuracy*), Presisi (*Precision*), Recall, serta Kecepatan Eksekusi komputasi yang diukur dalam satuan detik [12]. Pendekatan

eksperimental ini dipilih guna menemukan model yang memberikan keseimbangan terbaik antara keandalan keamanan dan efisiensi waktu pemrosesan di sisi server.

Populasi dan sampel data yang digunakan dalam tahap pengujian (testing) dikumpulkan melalui simulasi internal pada satu akun pengguna terdaftar. Total data uji yang digunakan berjumlah 79 percobaan, di mana pengujian dilakukan dengan mencocokkan setiap citra uji terhadap satu citra wajah asli (master data) milik pemilik akun. Dataset ini dibagi menjadi dua kelas klasifikasi. Kelas pertama merupakan data genuine yang terdiri dari 33 citra variasi wajah dari subjek utama (pemilik akun) yang diambil secara mandiri, bertujuan untuk menguji kemampuan sistem dalam mengenali variasi wajah pemilik asli. Kelas kedua merupakan data imposter yang terdiri dari 46 citra wajah acak dari individu yang berbeda-beda, yang dikumpulkan dari sumber daring (internet). Data imposter ini diunggah satu per satu ke akun subjek utama untuk menyimulasikan percobaan pemalsuan identitas atau catfishing [13], guna menguji keandalan sistem dalam menolak wajah orang lain. Seluruh citra uji berformat standar seperti JPG dan PNG yang disimpan di dalam direktori penyimpanan lokal server.

Instrumen penelitian dan pengembangan sistem dibangun menggunakan bahasa pemrograman Python [14]. Paket perangkat lunak *Ultralytics* digunakan untuk memuat model YOLOv8. Konfigurasi YOLOv8 yang diterapkan menggunakan bobot model versi nano standar (yolov8n.pt) yang merupakan pre-trained model bawaan. Pada tahap inferensi, model ini dikonfigurasi secara spesifik untuk melokalisasi kelas objek manusia (Person) tanpa memerlukan proses pelatihan ulang (*fine-tuning*) tambahan. Area objek manusia yang berhasil dilokalisasi kemudian dipotong (*cropping*) secara mandiri oleh sistem [9]. Untuk tahap ekstraksi fitur dan komparasi jarak vektor wajah (*cosine distance*), penelitian ini memanfaatkan pustaka DeepFace [15]. Sistem antarmuka penghubung (*Application Programming Interface/API*) dikembangkan menggunakan pustaka Flask untuk menangani request berformat JSON, sementara operasi pengolahan matriks citra didukung oleh *OpenCV* dan *NumPy* [16], [17].

Penentuan nilai threshold (ambang batas) disesuaikan dengan fungsi masing-masing model. Pada tahap deteksi, YOLOv8 menggunakan confidence threshold default bawaan sebesar 0.25 untuk memastikan area objek manusia terdeteksi secara optimal sebelum dipotong. Selanjutnya pada tahap komparasi wajah, ambang batas kemiripan didasarkan pada standar rekomendasi default dari pustaka *DeepFace* yang telah teruji secara empiris untuk menjaga konsistensi pada metrik cosine similarity. Threshold kemiripan yang diterapkan adalah 0.70 untuk model *ArcFace* dan *GhostFaceNet*, serta 0.40 untuk *FaceNet*. Teknik pengumpulan data dilakukan melalui simulasi pengujian otomatis (batch testing) menggunakan skrip request HTTP (*uji_batch.py*) yang mengirimkan pasangan citra uji ke endpoint API lokal secara berurutan.

Setiap hasil prediksi dari *Artificial Intelligence* (AI) berupa status verifikasi (*True/False*) dan durasi waktu proses (time elapsed) akan langsung dicatat oleh sistem ke dalam dokumen *Comma Separated Values* (CSV). Data historis yang terkumpul kemudian dianalisis menggunakan teknik *Confusion Matrix* untuk memetakan hasil *True Positive* (TP), *True Negative* (TN), *False Positive* (FP), dan *False Negative* (FN) [18]. Kalkulasi metrik ini menjadi dasar evaluasi untuk menentukan arsitektur mana yang memberikan trade-off paling memadai untuk diimplementasikan pada sistem operasional web Zawajna.

HASIL DAN PEMBAHASAN

Penelitian ini menguji kinerja empat kombinasi arsitektur kecerdasan buatan dalam memverifikasi wajah pada platform matchmaking Zawajna. Pengujian dilakukan menggunakan 79 dataset citra yang terdiri dari 33 citra subjek asli dan 46 citra imposter. Hasil prediksi model dievaluasi berdasarkan matriks kebingungan (*confusion matrix*) untuk menghitung nilai *True Positive* (TP), *True Negative* (TN), *False Positive* (FP), dan *False Negative* (FN). Kinerja algoritma diukur menggunakan persamaan matematika standar klasifikasi, yaitu Akurasi, Presisi, dan Recall.

$$\text{Akurasi} = (TP + TN) / (TP + TN + FP + FN) \quad (1)$$

$$\text{Presisi} = TP / (TP + FP) \quad (2)$$

$$\text{Recall} = TP / (TP + FN) \quad (3)$$

Persamaan (1) digunakan untuk mengukur rasio total prediksi yang benar secara keseluruhan. Persamaan (2) mengukur tingkat ketepatan model dalam menolak imposter (meminimalkan *False Positive*), sedangkan Persamaan (3) mengukur tingkat sensitivitas model dalam mengenali wajah subjek asli (meminimalkan *False Negative*).

Hasil pengujian dari keempat kombinasi arsitektur disajikan pada Tabel 1. Kinerja masing-masing model menunjukkan karakteristik trade-off yang berbeda dalam menangani klasifikasi citra wajah asli dan imposter.

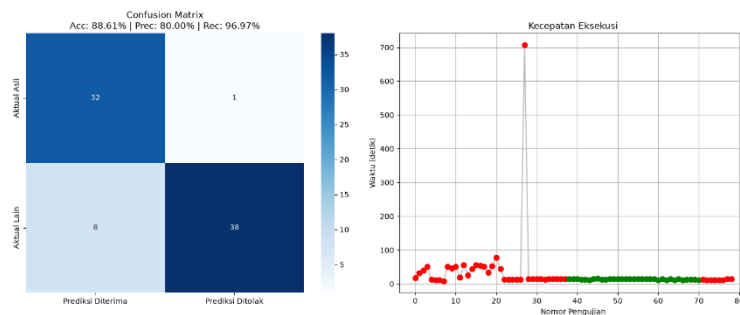
Tabel 1. Hasil Evaluasi Kinerja Arsitektur Verifikasi Wajah

Arsitektur Model	TP	TN	FP	FN	Akurasi (%)	Presisi (%)	Recall (%)
RetinaFace + ArcFace	32	38	8	1	88,61	80,00	96,97
YOLOv8 + ArcFace	28	41	5	5	87,34	84,85	84,85
YOLOv8 + FaceNet	27	37	9	6	81,01	75,00	81,82
YOLOv8 + GhostFaceNet	19	45	1	14	81,01	95,00	57,58

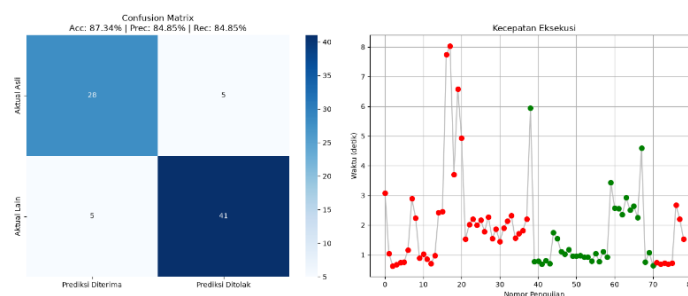
Berdasarkan Tabel 1, model *RetinaFace + ArcFace* unggul dalam metrik *Recall* tertinggi yaitu 96,97% serta Akurasi keseluruhan tertinggi mencapai 88,61%. Hal ini sejalan dengan lokalisasi berbasis CNN padat seperti *RetinaFace* yang sangat sensitif terhadap fitur wajah. Namun, penggunaan YOLOv8 dengan variasi modul pengenalan wajah menghasilkan dinamika yang berbeda. Model YOLOv8 + *GhostFaceNet* menghasilkan tingkat Presisi nyaris sempurna (95,00%) karena hanya mencatat 1 *False Positive* (FP) atau meloloskan 1 citra imposter. Kendati demikian, model ini terlalu protektif sehingga menghasilkan metrik Recall yang buruk (57,58%) karena mencatat 14 *False Negative* (FN) atau salah menolak 14 citra subjek asli. Di sisi lain, model YOLOv8 + *ArcFace* menghasilkan performa yang proporsional, dengan nilai Presisi dan Recall yang seimbang pada angka 84,85% dan tingkat Akurasi yang sangat baik pada 87,34% (dengan 5 FP dan 5 FN).

Selain kemampuan klasifikasi, kecepatan eksekusi merupakan parameter krusial untuk operasional sistem *Electronic Know Your Customer* (e-KYC) waktu nyata (*real-time*). Visualisasi perbandingan kecepatan eksekusi dari keempat model tersebut disajikan pada Gambar 1.

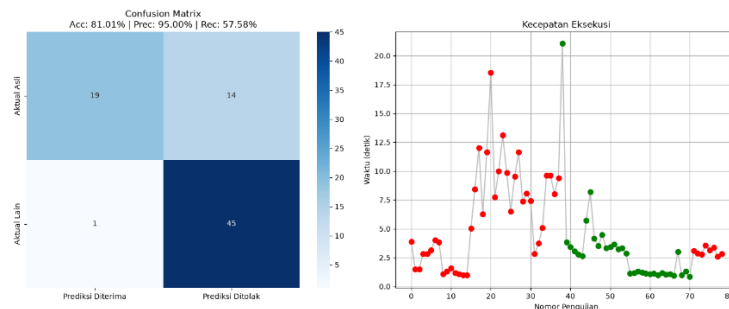
(a) Model RetinaFace + ArcFace



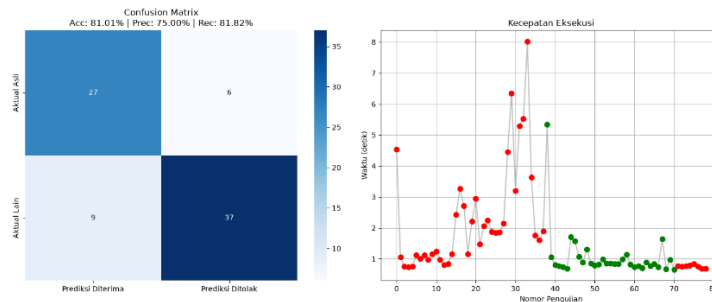
(b) Model YOLOv8 + ArcFace



(c) Model YOLOv8 + GhostFaceNet



(d) Model YOLOv8 + FaceNet



Gambar 1. Grafik Perbandingan Waktu Komputasi Eksekusi Model

Walaupun *RetinaFace* + *ArcFace* memiliki akurasi tertinggi, evaluasi waktu komputasi menunjukkan kelemahan fatal pada arsitektur ini. Waktu komputasi yang dihasilkan sangat lambat dan tidak stabil, di mana terjadi lonjakan waktu pemrosesan (*spike*) yang ekstrem hingga mencapai lebih dari 700 detik untuk memproses satu pengujian citra. Keterlambatan ini dinilai sangat tidak efisien dan akan mengganggu ketersediaan layanan (*availability*) pada operasional aplikasi berbasis *web*. Sebaliknya, integrasi YOLOv8 terbukti secara signifikan menurunkan beban komputasi *server*. Pada arsitektur YOLOv8 + *ArcFace*, waktu eksekusi berjalan sangat cepat, ringan, dan stabil, dengan rata-rata waktu pemrosesan berada di bawah 3 detik per citra.

Interpretasi atas temuan eksperimental ini menegaskan bahwa penggunaan algoritma dengan akurasi tertinggi tidak selalu menjadi solusi mutlak jika dihadapkan pada keterbatasan komputasi *server* produksi. Dalam konteks platform *matchmaking* Islami seperti *Zawajna*, kenyamanan pengguna (*user experience*) dalam mengganti foto profil dengan cepat sama pentingnya dengan keamanan validasi identitas itu sendiri.

Model YOLOv8 + *ArcFace* dipilih karena memberikan keseimbangan (*trade-off*) yang memadai antara keandalan tingkat akurasi sistem (87,34%) dan kecepatan respons *server* (di bawah 3 detik). Meskipun terdapat konsekuensi berupa 5 citra subjek asli yang tertolak secara salah (*False Negative*), margin kesalahan ini masih dalam batas toleransi logis dibandingkan jika sistem mengalami kelumpuhan akibat beban komputasi 700 detik pada *RetinaFace*. Oleh karena itu, penelitian ini merekomendasikan YOLOv8 dipadukan dengan *ArcFace* sebagai arsitektur yang memadai untuk diimplementasikan ke dalam *core system* validasi profil aplikasi *Zawajna* guna mendeteksi *catfishing* secara efisien.

SIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa penerapan sistem verifikasi biometrik wajah merupakan langkah preventif yang mendukung upaya pencegahan praktik pemalsuan identitas profil pada platform matchmaking Islami. Evaluasi terhadap beberapa kombinasi arsitektur kecerdasan buatan dengan 79 dataset simulasi menunjukkan bahwa model yang memiliki kemampuan deteksi paling teliti (*RetinaFace*) tidak selalu ideal untuk diimplementasikan pada sistem operasional, karena beban komputasi yang terlalu berat justru memperlambat respons server secara signifikan. Oleh karena itu, perpaduan antara algoritma deteksi mandiri YOLOv8 dengan pengenalan wajah ArcFace terpilih sebagai solusi yang direkomendasikan. Kombinasi ini terbukti memberikan keseimbangan (*trade-off*) yang memadai antara keandalan klasifikasi wajah dan efisiensi waktu pemrosesan yang stabil di bawah 3 detik, sehingga dapat diterapkan untuk memfasilitasi kelancaran interaksi pengguna secara real-time.

Mengingat pengujian dalam penelitian ini masih terbatas pada 79 data sampel citra, saran utama untuk pengembangan penelitian selanjutnya adalah memperluas pengujian model menggunakan dataset berskala besar yang mencakup variasi pencahayaan, pose, dan karakteristik wajah yang lebih beragam untuk menguji ketahanan model secara lebih reliabel. Selain itu, disarankan untuk mengintegrasikan fitur deteksi keaktifan wajah (*liveness detection* atau *anti-spoofing*) guna meminimalisir celah manipulasi keamanan tingkat lanjut yang menggunakan foto statis, topeng, atau rekaman video. Implementasi arsitektur verifikasi biometrik ini ke dalam bentuk aplikasi mobile (berbasis Android/iOS) juga direkomendasikan agar aksesibilitas keamanan pada platform Zawajna menjadi lebih optimal bagi pengguna.

DAFTAR PUSTAKA

- [1] O. o, "Online Matchmaking Using Collaborative Filtering and Reciprocal Recommender Systems," vol. 7, no. 2, 2018.
- [2] E. B. Pramana dan A. Sunandar, "Analisa rancang bangun aplikasi biro jodoh islami menggunakan algoritma profile matching berdasarkan platform android," *Arcitech J. Comput. Sci. Artif. Intell.*, vol. 2, no. 2, hal. 123, Dec. 2022, doi: 10.29240/arcitech.v2i2.5834.
- [3] C. E. Putri dan R. E. Hamzah, "Analisis fenomena penipuan identitas diri (catfishing) pada literasi digital pengguna media sosial".
- [4] K. Verma, R. Kumar, A. P. Rao, dan R. Ranjan, "Efficient e-KYC Authentication System: Redefining Customer Verification in Digital Banking," dalam *2023 9th International Conference on Signal Processing and Communication (ICSC)*, NOIDA, India: IEEE, Dec. 2023, hal. 319–324. doi: 10.1109/ICSC60394.2023.10441596.
- [5] B. T. Utomo, I. Fitri, dan E. Mardiani, "Penerapan face recognition pada aplikasi akademik online," 2020.
- [6] J. Deng, J. Guo, E. Ververas, I. Kotsia, and S. Zafeiriou, "RetinaFace: Single-Shot Multi-Level Face Localisation in the Wild," dalam *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Seattle, WA, USA: IEEE, Jun. 2020, hal. 5202–5211. doi: 10.1109/CVPR42600.2020.00525.
- [7] J. Deng, J. Guo, N. Xue, dan S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition".
- [8] M. Alansari, O. A. Hay, S. Javed, A. Shoufan, Y. Zweiri, dan N. Werghi, "GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations," *IEEE Access*, vol. 11, hal. 35429–35446, 2023, doi: 10.1109/ACCESS.2023.3266068.
- [9] J. Terven, D.-M. Córdova-Esparza, dan J.-A. Romero-González, "A Comprehensive Review of YOLO Architectures in Computer Vision: From YOLOv1 to YOLOv8 and YOLO-NAS," *Mach. Learn. Knowl. Extr.*, vol. 5, no. 4, hal. 1680–1716, Nov. 2023, doi: 10.3390/make5040083.
- [10] A. K. Jain, D. Deb, dan J. J. Engelsma, "Biometrics: Trust, But Verify," *IEEE Trans. Biom. Behav. Identity Sci.*, vol. 4, no. 3, hal. 303–323, Jul. 2022, doi: 10.1109/TBIOM.2021.3115465.

- [11] M. Wang dan W. Deng, "Deep face recognition: A survey," *Neurocomputing*, vol. 429, hal. 215–244, Mar. 2021, doi: 10.1016/j.neucom.2020.10.081.
- [12] R. Padilla, S. L. Netto, dan E. A. B. Da Silva, "A Survey on Performance Metrics for Object-Detection Algorithms," dalam *2020 International Conference on Systems, Signals and Image Processing (IWSSIP)*, Niterói, Brazil: IEEE, Jul. 2020, hal. 237–242. doi: 10.1109/IWSSIP48289.2020.9145130.
- [13] J. Patil, "Fake Profile Detection on Social Media using Machine Learning".
- [14] S. Raschka, *Machine Learning with PyTorch and Scikit-Learn: Develop machine learning and deep learning models with Python*, 1 ed. Birmingham: Packt Publishing Limited, 2022.
- [15] S. I. Serengil dan A. Ozpinar, "LightFace: A Hybrid Deep Face Recognition Framework," dalam *2020 Innovations in Intelligent Systems and Applications Conference (ASYU)*, Istanbul, Turkey: IEEE, Okt. 2020, hal. 1–5. doi: 10.1109/ASYU50717.2020.9259802.
- [16] Supiyandi Supiyandi, Adinda Fita Hidayah, Luthfie Budie, Nurhalijah Berutu, dan Fakhita Fahraini, "Pengenal Gambar Dasar Menggunakan Python dan OpenCV," *J. Sist. Inf. Dan Ilmu Komput.*, vol. 2, no. 4, hal. 52–61, Nov. 2024, doi: 10.59581/jusiik-widyakarya.v2i4.4200.
- [17] C. R. Harris *et al.*, "Array programming with NumPy," *Nature*, vol. 585, no. 7825, hal. 357–362, Sep. 2020, doi: 10.1038/s41586-020-2649-2.
- [18] A. Tharwat, "Classification assessment methods," *Appl. Comput. Inform.*, vol. 17, no. 1, hal. 168–192, Jan. 2021, doi: 10.1016/j.aci.2018.08.003.