

Peningkatan Validasi Identitas pada Sistem Presensi berbasis *Flutter*

Improving Identity Validation in a Flutter-based Attendance System

¹Carlita Masaccio Mauren*, ²Abdussalam

^{1,2}Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Semarang

^{1,2}Jl. Imam Bonjol No.207, Pendrikan Kidul, Kec. Semarang Tengah, Kota Semarang, Jawa Tengah

*e-mail: 111202214768@mhs.dinus.ac.id

(received: 27 April 2026, revised: 18 May 2026, accepted: 21 May 2026)

Abstrak

Penelitian ini bertujuan meningkatkan validasi identitas pada sistem presensi berbasis *Flutter* yang masih rentan terhadap manipulasi kehadiran, seperti *buddy punching* dan penggunaan *fake GPS*. Permasalahan utama pada sistem sebelumnya adalah mekanisme validasi berbasis lokasi belum mampu memastikan bahwa proses presensi benar-benar dilakukan oleh pengguna yang sah. Sebagai penelitian implementasi sistem dan rekayasa perangkat lunak, penelitian ini menerapkan pendekatan multi-feature similarity berbasis face embedding, dengan appearance similarity sebagai komponen utama yang dihitung menggunakan cosine similarity, serta fitur pendukung berupa geometry similarity, quality score, color similarity, dan texture similarity. Pengembangan sistem dilakukan menggunakan metode FAST dengan implementasi *Flutter*, *Google ML Kit* untuk deteksi wajah dan landmark, serta *MobileFaceNet* untuk ekstraksi *face embedding*. Pengujian dilakukan melalui uji coba langsung, *API testing*, dan *black-box testing* terhadap 655 karyawan dengan *threshold similarity* 0,80. Hasil pengujian pada 14 skenario menunjukkan seluruh keluaran sistem sesuai dengan hasil yang diharapkan, sehingga akurasi skenario mencapai 100%. Dibandingkan sistem presensi berbasis *GPS* sebelumnya, indikasi manipulasi kehadiran menurun dari 70 kasus atau 10,7% menjadi 1 kasus atau 0,15%. Selain itu, *False Acceptance Rate* menurun dari 12,8% menjadi 0,2%, dengan waktu verifikasi rata-rata 1200 ms. Hasil ini menunjukkan bahwa pendekatan *multi-feature similarity* berbasis *face embedding* mampu meningkatkan validitas dan integritas data kehadiran secara *real-time* pada perangkat *mobile*.

Kata kunci: sistem presensi, face embedding, face recognition, flutter, multi-feature similarity

Abstract

This study aims to improve identity validation in a Flutter-based attendance system that remains vulnerable to attendance manipulation, such as *buddy punching* and *fake GPS* usage. The primary issue in the previous system was that location-based validation mechanisms were unable to ensure that attendance activities were genuinely performed by authorized users. As a system implementation and software engineering study, this research applies a multi-feature similarity approach based on face embeddings, where appearance similarity serves as the primary component calculated using cosine similarity. Supporting features include geometry similarity, quality score, color similarity, and texture similarity. The system was developed using the FAST methodology, with implementation based on Flutter, Google ML Kit for face and landmark detection, and MobileFaceNet for face embedding extraction. Testing was conducted through direct implementation trials, API testing, and black-box testing involving 655 employees using a similarity threshold of 0.80. The results from 14 testing scenarios showed that all system outputs matched the expected outcomes, resulting in 100% scenario accuracy. Compared to the previous GPS-based attendance system, indications of attendance manipulation decreased from 70 cases (10.7%) to only 1 case (0.15%). In addition, the False Acceptance Rate decreased from 12.8% to 0.2%, with an average verification time of 1200 ms. These findings demonstrate that the multi-feature similarity approach based on face embeddings is capable of improving the validity and integrity of real-time attendance data on mobile devices.

Keywords: attendance system, face embedding, face recognition, flutter, multi-feature similarity

<http://sistemasi.ftik.unisi.ac.id>

1 Pendahuluan

Era digital mendorong perubahan signifikan dalam pengelolaan sumber daya manusia, khususnya pada sistem presensi. Perusahaan dituntut mengadopsi pendekatan inovatif melalui integrasi teknologi, seperti Sistem Informasi Manajemen SDM, yang terbukti meningkatkan efisiensi operasional, akurasi data, dan kualitas pengambilan keputusan [1][2]. Efektivitas sistem informasi juga dipengaruhi oleh optimalisasi pemanfaatan teknologi yang berkontribusi terhadap kinerja sistem di lingkungan kerja [3]. Dalam konteks ini, aplikasi presensi berbasis mobile menjadi solusi populer karena mampu mengatasi keterbatasan metode konvensional yang tidak efisien dan rentan manipulasi [4].

Namun demikian, sistem presensi digital masih menghadapi tantangan serius terkait keabsahan dan integritas data kehadiran. Mekanisme berbasis geolokasi diketahui memiliki celah keamanan, seperti praktik *buddy-punching* serta penyalahgunaan kredensial pengguna [5][6]. Selain itu, penggunaan *Global Positioning System (GPS)* belum sepenuhnya efektif karena rentan terhadap manipulasi lokasi melalui teknik *location spoofing* menggunakan aplikasi pihak ketiga. Fenomena ini menunjukkan bahwa pendekatan berbasis lokasi saja belum mampu menjamin validitas data kehadiran dan berpotensi menimbulkan kerugian serta menurunkan objektivitas evaluasi kinerja [7].

Sebagai solusi, teknologi biometrik menawarkan mekanisme autentikasi yang lebih personal dan sulit dipalsukan. Pengenalan wajah (*face recognition*) menjadi alternatif yang sesuai untuk perangkat mobile karena bersifat *contactless*, higienis, serta memanfaatkan kamera *smartphone*. Penelitian sebelumnya menunjukkan bahwa sistem berbasis pengenalan wajah mampu meningkatkan akurasi dan efisiensi presensi, dengan tingkat akurasi yang cukup tinggi, termasuk metode PCA yang mencapai rata-rata 88% [8][9][10], dan pada penelitian lainnya menyebutkan hasil yang di dapatkan rata-rata 85% [11]. Selain itu, adopsi teknologi biometrik juga dipengaruhi oleh faktor persepsi kegunaan dan kemudahan penggunaan [12].

Meskipun memiliki berbagai keunggulan, implementasi teknologi pengenalan wajah pada platform mobile seperti *Flutter* masih menghadapi tantangan, terutama dalam efisiensi pemrosesan citra pada perangkat dengan keterbatasan sumber daya. Pendekatan *face embedding* berbasis *deep learning* dapat digunakan sebagai representasi utama wajah karena mampu menghasilkan fitur matematis yang ringkas dan diskriminatif. Representasi ini juga berperan penting dalam meningkatkan keamanan sistem serta mengurangi risiko pemalsuan data *biometrik* [13]. Akan tetapi, proses verifikasi wajah pada perangkat *mobile* tetap dipengaruhi oleh variasi kondisi input, seperti pencahayaan, pose wajah, jarak kamera, kualitas citra, warna, tekstur, dan oklusi sebagian wajah. Jika sistem hanya mengandalkan satu jenis fitur kemiripan, hasil verifikasi berpotensi kurang stabil pada kondisi pengambilan gambar yang tidak ideal. Oleh karena itu, penelitian ini mengombinasikan *face embedding* dengan fitur pendukung dalam pendekatan *multi-feature similarity* untuk meningkatkan ketahanan proses validasi identitas.

Ditinjau dari ruang lingkup penelitian, artikel ini diposisikan sebagai penelitian implementasi sistem dan rekayasa perangkat lunak pada aplikasi presensi mobile, bukan sebagai penelitian yang mengembangkan model *computer vision* baru. Fokus utama penelitian adalah merancang, mengimplementasikan, dan mengevaluasi fitur validasi identitas berbasis *face recognition* pada aplikasi *Flutter*. Evaluasi yang dilakukan mencakup aspek fungsional sistem, performa verifikasi, serta keamanan biometrik melalui pengukuran nilai *similarity*, *False Acceptance Rate*, waktu *respons*, dan perbandingan indikasi manipulasi kehadiran sebelum dan sesudah penerapan fitur.

Dengan ruang lingkup tersebut, penelitian ini bertujuan mengembangkan dan mengevaluasi sistem presensi berbasis *Flutter* dengan mekanisme validasi identitas menggunakan *face recognition*. Pendekatan yang digunakan adalah *multi-feature similarity* berbasis *face embedding*, dengan *appearance similarity* sebagai komponen utama yang dihitung menggunakan *cosine similarity*. Fitur pendukung berupa *geometry*, *quality*, *color*, dan *texture similarity* digunakan untuk meningkatkan ketahanan sistem terhadap variasi kondisi input pada perangkat *mobile*. Sistem ini diharapkan mampu meningkatkan validitas data kehadiran, mengurangi potensi *buddy punching*, serta meminimalkan manipulasi presensi berbasis *GPS*.

2 Tinjauan Literatur

Sistem presensi berbasis teknologi digital telah berkembang pesat seiring meningkatnya kebutuhan efisiensi dan akurasi dalam pengelolaan kehadiran. Penelitian sebelumnya menunjukkan bahwa integrasi sistem presensi online berbasis *face recognition* dan *GPS* mampu meningkatkan efisiensi operasional secara signifikan [1]. Namun demikian, efektivitas sistem informasi tetap bergantung pada optimalisasi pemanfaatan teknologi informasi di lingkungan kerja [3]. Selain itu, inovasi manajemen juga berperan penting dalam mendorong transformasi digital yang efisien dan produktif [4].

Di sisi keamanan, mekanisme berbasis *GPS* masih memiliki kelemahan mendasar karena rentan terhadap serangan *location spoofing*. Studi menunjukkan bahwa teknik *GPS spoofing* dapat memberikan dampak signifikan terhadap keakuratan lokasi pada perangkat mobile [15]. Penelitian lain mengklasifikasikan penggunaan *GPS* palsu menggunakan metode regresi logistik dan menunjukkan bahwa manipulasi lokasi cukup sulit dideteksi secara konvensional [7]. Implementasi *geolocator* untuk mendeteksi manipulasi lokasi pada sistem presensi juga belum sepenuhnya efektif dalam menjamin keabsahan data kehadiran [16]. Selain itu, pendekatan berbasis *QR code* dan geolokasi memang dapat mengurangi kecurangan, tetapi masih memiliki keterbatasan karena tetap bergantung pada validitas lokasi [5].

Sebagai alternatif, teknologi biometrik, khususnya pengenalan wajah, menawarkan solusi autentikasi yang lebih personal dan sulit dipalsukan. Beberapa penelitian telah mengembangkan sistem presensi berbasis *face recognition* menggunakan pendekatan *machine learning* dan integrasi lokasi pada perangkat *mobile* [8][9]. Metode lain seperti *Principal Component Analysis (PCA)* dan *OpenCV* juga telah digunakan untuk pengenalan wajah dengan tingkat akurasi masing-masing sekitar 88% dan 85% [10][11]. Selain itu, integrasi kecerdasan buatan dalam sistem presensi biometrik menunjukkan peningkatan efektivitas dalam pengelolaan kehadiran [6]. Dari sisi pengguna, faktor persepsi kegunaan dan kemudahan penggunaan juga berpengaruh terhadap tingkat adopsi teknologi biometrik [12].

Pada aspek teknis, pengembangan sistem pengenalan wajah perlu memperhatikan keamanan data biometrik, khususnya dalam bentuk *face embedding* pada perangkat *mobile* [13]. *Face embedding* berbasis *deep learning* dapat digunakan untuk merepresentasikan karakteristik utama wajah dalam bentuk vektor numerik, yang kemudian dapat dibandingkan menggunakan *cosine similarity*. Namun, performa sistem pengenalan wajah pada perangkat *mobile* juga dipengaruhi oleh kondisi lingkungan dan kualitas input, seperti penggunaan masker, pencahayaan, pose wajah, jarak kamera, blur, dan oklusi sebagian wajah [17]. Studi lain menunjukkan bahwa pendekatan *autentikasi biometrik multimodal* dapat meningkatkan keandalan sistem verifikasi identitas secara berkelanjutan [18].

Dalam konteks verifikasi wajah pada perangkat *mobile*, penggunaan *face embedding* sebagai satu-satunya dasar perhitungan *similarity* belum selalu cukup untuk menangani variasi kondisi *input* yang kompleks. Nilai *similarity* berbasis *embedding* dapat berubah ketika citra wajah dipengaruhi pencahayaan rendah, posisi wajah miring, kualitas citra buruk, atau adanya bagian wajah yang tertutup. Oleh karena itu, diperlukan pendekatan yang tidak hanya mengandalkan satu fitur kemiripan, tetapi juga mengombinasikan beberapa fitur pendukung agar proses verifikasi identitas lebih stabil dan *lebih andal*.

Dari perspektif pengembangan sistem, metode *FAST (Framework for the Application of System Thinking)* telah banyak digunakan dalam berbagai implementasi sistem informasi, seperti sistem keuangan sekolah [14], sistem simpan pinjam koperasi [19], dan sistem kasir apotek [20]. Pendekatan ini memungkinkan proses pengembangan dilakukan secara terstruktur dan sistematis sehingga mampu menghasilkan sistem yang sesuai dengan kebutuhan pengguna. Dalam penelitian ini, *FAST* digunakan sebagai metode pengembangan sistem, sedangkan validasi identitas wajah dilakukan menggunakan pendekatan *multi-feature similarity*.

Berdasarkan kajian literatur tersebut, dapat diidentifikasi bahwa penelitian yang mengintegrasikan *face recognition* berbasis *multi-feature similarity* dalam ekosistem *Flutter* untuk sistem presensi mobile masih terbatas. Penelitian ini menempatkan *face embedding* berbasis *deep learning* sebagai komponen utama *appearance similarity* yang dihitung menggunakan *cosine similarity*. Untuk meningkatkan ketahanan sistem terhadap variasi kondisi input, penelitian ini

menambahkan fitur pendukung berupa *geometry similarity*, *quality score*, *color similarity*, dan *texture similarity*. Dengan demikian, pendekatan *multi-feature similarity* digunakan sebagai metode verifikasi identitas secara *real-time* pada sistem presensi berbasis *Flutter*.

3 Metode Penelitian

Metode FAST (*Framework for the Application of System Thinking*) merupakan pendekatan pengembangan sistem yang berorientasi pada analisis kebutuhan serta pemecahan masalah secara terstruktur melalui proses yang sistematis dan iteratif [19][20]. Metode ini membantu pengembang dalam memahami kebutuhan pengguna, merancang solusi yang sesuai, serta mengimplementasikan sistem secara bertahap dan terarah.

Penelitian ini dilaksanakan pada periode Maret–Agustus 2024 di lingkungan perusahaan mitra. Populasi pengujian terdiri dari 655 karyawan yang tersebar di kantor pusat dan cabang regional, dengan variasi usia, jenis kelamin, serta kondisi pencahayaan lingkungan. Dataset wajah yang digunakan mencakup citra dengan pose normal, ekspresi yang bervariasi, serta penggunaan aksesoris seperti kacamata dan masker.

Uji coba langsung dilakukan pada lingkungan operasional perusahaan mitra dengan melibatkan karyawan sebagai pengguna sistem presensi. Pengujian ini dilakukan untuk mengevaluasi kemampuan sistem dalam memvalidasi identitas pengguna pada kondisi penggunaan nyata, termasuk variasi pencahayaan, jarak pengambilan citra, ekspresi wajah, dan kondisi wajah tertutup sebagian. Selain uji coba langsung, API testing digunakan untuk memastikan komunikasi antara aplikasi dan layanan *backend* berjalan sesuai kebutuhan, sedangkan *black-box* testing digunakan untuk mengevaluasi keluaran sistem berdasarkan skenario input yang telah ditentukan.

Pengembangan sistem dilakukan menggunakan *framework Flutter 3.41.4* dan *Dart 3.11.1*, dengan memanfaatkan *library google_mlkit_face_detection* untuk proses deteksi wajah serta model *CNN* ringan *MobileFaceNet* yang telah dioptimalkan untuk perangkat mobile. *Flutter* dipilih karena mendukung pengembangan aplikasi mobile lintas perangkat dengan satu basis kode, sehingga memudahkan integrasi fitur presensi, akses kamera, komunikasi API, dan antarmuka pengguna secara konsisten. Dalam penelitian ini, *Flutter* berperan sebagai lapisan aplikasi yang menghubungkan proses pengambilan citra wajah, pengiriman data ke sistem, penerimaan hasil verifikasi, serta penyajian umpan balik kepada pengguna secara *real-time*. Dengan demikian, *Flutter* tidak hanya digunakan sebagai platform antarmuka, tetapi juga sebagai lingkungan implementasi fitur validasi identitas pada perangkat *mobile*. Pengujian kinerja sistem dilakukan pada perangkat Android dengan metrik evaluasi meliputi akurasi skenario pengujian, *False Acceptance Rate (FAR)*, waktu respons, serta perbandingan indikasi manipulasi kehadiran sebelum dan sesudah penerapan sistem.

Sebagai alur penelitian, tahapan yang dilakukan mengikuti metode FAST yang mencakup definisi ruang lingkup, analisis permasalahan, analisis kebutuhan, perancangan logis, konstruksi, pengujian, serta implementasi sistem.

3.1 Definisi Ruang Lingkup

Fase definisi ruang lingkup merupakan tahapan awal dalam pengembangan sistem yang bertujuan untuk mengidentifikasi kebutuhan, permasalahan, serta batasan sistem yang akan dibangun. Proses ini dilakukan melalui observasi terhadap mekanisme presensi yang sedang berjalan dan analisis terhadap celah keamanan, seperti *buddy punching* dan manipulasi lokasi. Selain itu, dilakukan juga studi literatur untuk mengkaji penerapan teknologi pengenalan wajah (*face recognition*) yang relevan guna mendukung proses validasi yang lebih akurat dan andal.

3.2 Analisis Permasalahan

Fase analisis masalah dilakukan untuk mengidentifikasi kelemahan pada sistem presensi yang sedang berjalan, di mana berdasarkan hasil observasi, penggunaan *GPS* masih rentan terhadap manipulasi seperti *buddy punching* dan *mock location*, sehingga belum mampu menjamin keabsahan data kehadiran [2]. Oleh karena itu, diperlukan pengembangan sistem dengan mekanisme validasi yang lebih kuat melalui penerapan *face recognition* berbasis *multi-feature similarity*. Dalam pendekatan ini, *face embedding* digunakan sebagai komponen utama *appearance similarity*,

sedangkan *geometry similarity*, *quality score*, *color similarity*, dan *texture similarity* digunakan sebagai fitur pendukung untuk meningkatkan validitas dan integritas data presensi.

3.3 Analisis Kebutuhan

Tahap analisis kebutuhan dilakukan untuk mengidentifikasi kebutuhan sistem dalam pengembangan fitur *face recognition*. Fokus utama meliputi proses pengambilan wajah melalui kamera, deteksi dan validasi wajah, serta penentuan hasil verifikasi berupa wajah berhasil atau gagal dikenali. Selain itu, sistem juga harus mampu memberikan umpan balik secara *real-time* dan menyediakan mekanisme pengulangan jika proses verifikasi tidak berhasil. Analisis ini menjadi dasar dalam merancang sistem yang akurat dan meminimalkan potensi kecurangan.

3.4 Perancangan Logis

Fase perancangan logis bertujuan untuk mentransformasikan kebutuhan sistem yang telah dianalisis ke dalam model sistem baru yang akan dikembangkan. Pada tahap ini, dirancang aspek teknologi meliputi data, proses, dan antarmuka yang mendukung fitur pengenalan wajah, seperti proses pengambilan wajah, verifikasi berhasil, dan verifikasi gagal. Perancangan dilakukan dengan mempertimbangkan aspek usability dan keandalan sistem.

3.5 Analisis Keputusan

Tahap analisis keputusan dilakukan untuk mengevaluasi kelayakan rancangan sistem berdasarkan kebutuhan pengguna, keamanan proses presensi, dan kemampuan sistem dalam memvalidasi identitas. Pada tahap ini, rancangan *face recognition* berbasis *multi-feature similarity* dinilai sebagai solusi yang sesuai karena mampu menggabungkan *face embedding* sebagai komponen utama dengan fitur pendukung berupa *geometry*, *quality*, *color*, dan *texture similarity*.

3.6 Desain Logis

Tahap desain logis dilakukan untuk mentransformasikan kebutuhan sistem presensi berbasis pengenalan wajah ke dalam model yang terstruktur. Proses ini mencakup perancangan alur deteksi wajah, ekstraksi fitur menggunakan model *deep learning*, serta mekanisme pencocokan data wajah dengan data yang sudah tersedia di *database*. Hasil dari desain logis ini kemudian diimplementasikan ke dalam desain fisik menggunakan teknologi *Flutter*, dan penyimpanan lokal atau *online*, sehingga sistem dapat berjalan secara efektif dalam mendeteksi dan memverifikasi identitas pengguna.

3.7 Perhitungan Multi-Feature Similarity

Pada penelitian ini, *Google ML Kit* dan *MobileFaceNet* tidak digunakan sebagai metode yang berdiri sendiri, melainkan sebagai komponen dalam *pipeline multi-feature similarity*. *Google ML Kit* digunakan untuk mendeteksi wajah dan *landmark*, sedangkan *MobileFaceNet* digunakan untuk menghasilkan *face embedding* yang menjadi dasar perhitungan *appearance similarity*. Proses validasi identitas pada penelitian ini dilakukan menggunakan pendekatan *multi-feature similarity* berbasis *face embedding*. *Face embedding* diperoleh melalui model *CNN* ringan *MobileFaceNet* dan digunakan sebagai komponen utama *appearance similarity*. Nilai *appearance similarity* dihitung menggunakan *cosine similarity* untuk membandingkan dua vektor *embedding* wajah. Selain itu, sistem juga menghitung *geometry similarity* berdasarkan *landmark* wajah, *quality score* berdasarkan ukuran wajah, pose, dan ketajaman citra, *color similarity* berdasarkan distribusi warna, serta *texture similarity* berdasarkan pola intensitas citra. Seluruh komponen tersebut digabungkan menggunakan pembobotan, yaitu 0,82 untuk *appearance similarity*, 0,06 untuk *geometry similarity*, 0,05 untuk *quality score*, 0,025 untuk *color similarity*, dan 0,025 untuk *texture similarity*. Nilai *similarity* akhir kemudian dibandingkan dengan threshold 0,80 untuk menentukan apakah wajah pengguna valid atau tidak valid.

3.8 Konstruksi dan Pengujian

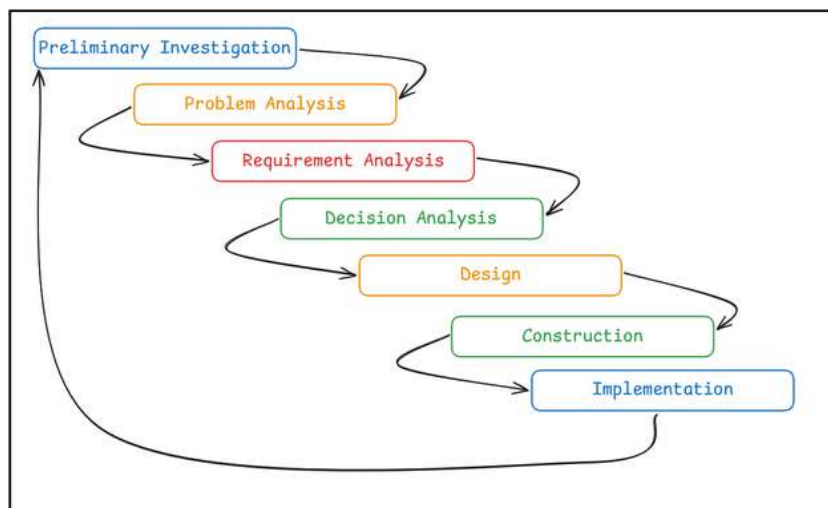
Tahap konstruksi dan pengujian bertujuan untuk mengkonstruksi dan melakukan tahap pengujian pada sistem baru yang telah memenuhi kebutuhan bisnis dan spesifikasi desainnya. Dalam tahap ini

<http://sistemasi.ftik.unisi.ac.id>

harus dilakukan pengujian secara ketat dan mendetail mulai dari program aplikasi dan mengaplikasikan *interface* antara sistem baru dengan sistem yang sudah ada.

3.9 Instalasi dan Pengiriman

Tahap instalasi dan pengiriman merupakan proses distribusi aplikasi kepada pengguna melalui Play Store setelah dilakukan pengujian akhir. Aplikasi yang telah dikembangkan dapat langsung diunduh dan digunakan, disertai panduan singkat agar fitur *face recognition* dapat dioperasikan dengan baik.



Gambar 1 Alur metode FAST

4 Hasil dan Pembahasan

Penerapan metode *FAST* pada Gambar 1, menghasilkan beberapa *output* pada setiap tahapan yang dilalui.

4.1 Definisi Ruang Lingkup

Tahap definisi dan ruang lingkup pada bab hasil dan pembahasan berfokus pada penentuan batasan implementasi fitur *face recognition* dalam aplikasi presensi berbasis *Flutter*. Ruang lingkup penelitian ini mencakup proses pengambilan citra wajah melalui kamera, deteksi wajah, ekstraksi *face embedding* sebagai komponen utama *appearance similarity*, serta perhitungan *multi-feature similarity* untuk menentukan keberhasilan atau kegagalan *otentikasi*. Pendekatan *multi-feature similarity* yang digunakan mengombinasikan *appearance similarity*, *geometry similarity*, *quality score*, *color similarity*, dan *texture similarity* agar sistem mampu melakukan validasi identitas secara lebih stabil pada berbagai kondisi input. Selain itu, pembahasan juga dibatasi pada evaluasi kinerja sistem dalam meningkatkan validitas data presensi dan meminimalkan potensi kecurangan seperti *buddy punching*.

4.2 Analisis Permasalahan

Berdasarkan hasil analisis, ditemukan beberapa permasalahan, di antaranya sistem presensi yang masih menggunakan *GPS* rentan terhadap manipulasi seperti *buddy punching* dan penggunaan *fake GPS*. Selain itu, sistem belum mampu memverifikasi identitas pengguna secara valid karena mekanisme presensi belum dilengkapi dengan *otentikasi* biometrik yang kuat. Oleh karena itu, diperlukan pengembangan fitur *face recognition* dengan pendekatan *multi-feature similarity* berbasis *face embedding* agar proses autentikasi lebih akurat, meningkatkan keabsahan data kehadiran, serta meminimalkan potensi kecurangan dalam presensi.

4.3 Analisis Kebutuhan

Aplikasi presensi berbasis *face recognition* yang dikembangkan merupakan sistem yang digunakan untuk mencatat kehadiran karyawan secara digital dengan memanfaatkan validasi biometrik. Proses analisis kebutuhan dilakukan melalui observasi terhadap sistem presensi yang

sedang berjalan serta studi literatur terkait teknologi presensi digital dan pengenalan wajah. Berdasarkan hasil analisis, sistem presensi yang ada sebelumnya masih memiliki keterbatasan menjamin keabsahan identitas pengguna, sehingga diperlukan pengembangan sistem dengan mekanisme validasi yang lebih aman dan akurat.

Sistem yang dikembangkan memiliki beberapa komponen utama, yaitu data pengguna, proses presensi, dan pengolahan data. Selain itu, proses analisis kebutuhan juga mempertimbangkan kebutuhan pengguna sistem, antara lain: pengguna dapat melakukan presensi secara *real-time* menggunakan perangkat *mobile*; sistem dapat melakukan verifikasi identitas pengguna melalui kamera secara otomatis; sistem mampu membandingkan wajah pengguna dengan data yang tersimpan untuk mencegah *buddy punching*; sistem dapat menyimpan data kehadiran secara akurat dan terintegrasi; admin dapat memantau dan mengelola data kehadiran karyawan; dan sistem mampu meminimalkan manipulasi autentikasi wajah.

4.4 Perencanaan Logis

Pada tahap perancangan logis, kebutuhan sistem diterjemahkan ke dalam bentuk desain antarmuka (*user interface*) yang berfokus pada implementasi fitur pengenalan wajah (*face recognition*) dengan bantuan tools seperti Figma. Tahapan ini bertujuan untuk memvisualisasikan alur interaksi pengguna dalam proses autentikasi wajah sebelum masuk ke tahap pengembangan sistem. Perancangan difokuskan pada alur utama dari fitur *face recognition*, yang mencakup: antarmuka pengambilan citra wajah melalui kamera secara *real-time*; proses deteksi serta validasi wajah pengguna; tampilan notifikasi ketika verifikasi wajah berhasil; tampilan notifikasi ketika wajah gagal dikenali; dan mekanisme pengulangan pengambilan wajah apabila proses verifikasi tidak berhasil.

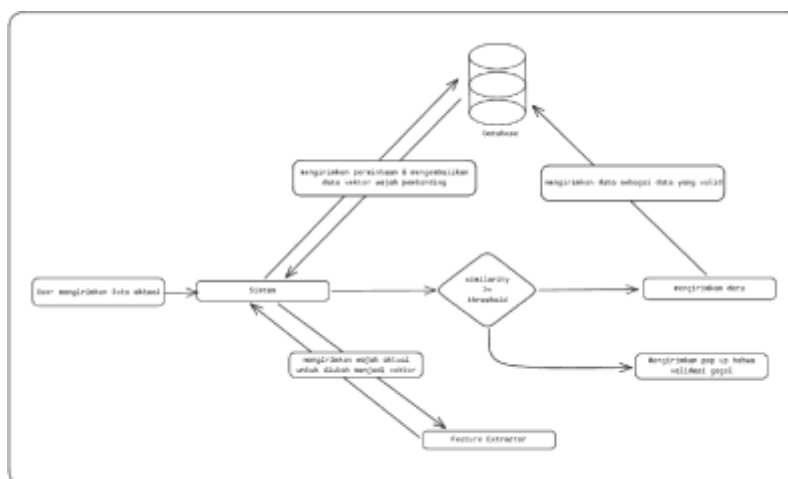
4.5 Evaluasi Keputusan Implementasi

Berdasarkan hasil perancangan dan implementasi fitur *face recognition* pada sistem presensi berbasis *mobile*, pendekatan *multi-feature similarity* berbasis *face embedding* menunjukkan kemampuan dalam meningkatkan keabsahan identitas pengguna dibandingkan metode presensi konvensional maupun berbasis *GPS*. *Face embedding* digunakan sebagai komponen utama *appearance similarity* yang dihitung menggunakan *cosine similarity*, sedangkan *geometry similarity*, *quality score*, *color similarity*, dan *texture similarity* digunakan sebagai fitur pendukung untuk meningkatkan ketahanan sistem terhadap variasi kondisi input.

Penerapan mekanisme verifikasi wajah berbasis *multi-feature similarity* terbukti dapat meminimalkan potensi kecurangan seperti *buddy punching* dan manipulasi kehadiran, karena setiap proses presensi memerlukan validasi biometrik yang bersifat unik pada masing-masing individu. Selain itu, integrasi fitur ini dalam lingkungan *Flutter* menunjukkan bahwa teknologi *face recognition* dapat diimplementasikan secara efisien pada perangkat *mobile* dengan keterbatasan sumber daya. Untuk pengembangan selanjutnya, sistem dapat ditingkatkan dengan penambahan mekanisme keamanan lain seperti *liveness detection* guna menghindari potensi *spoofing* menggunakan media gambar atau video.

4.6 Desain Logis

Pada tahap perancangan logis, sistem dirancang dalam bentuk alur proses *face recognition* yang menggambarkan mekanisme *autentikasi* pengguna berbasis *multi-feature similarity*. Berdasarkan Gambar 2, proses dimulai ketika pengguna mengirimkan citra wajah melalui perangkat. Sistem kemudian melakukan deteksi wajah dan ekstraksi fitur untuk mengubah wajah menjadi representasi vektor atau *face embedding*. *Face embedding* tersebut digunakan sebagai komponen utama *appearance similarity*, kemudian dikombinasikan dengan *geometry similarity*, *quality score*, *color similarity*, dan *texture similarity* untuk menghasilkan skor akhir verifikasi identitas.

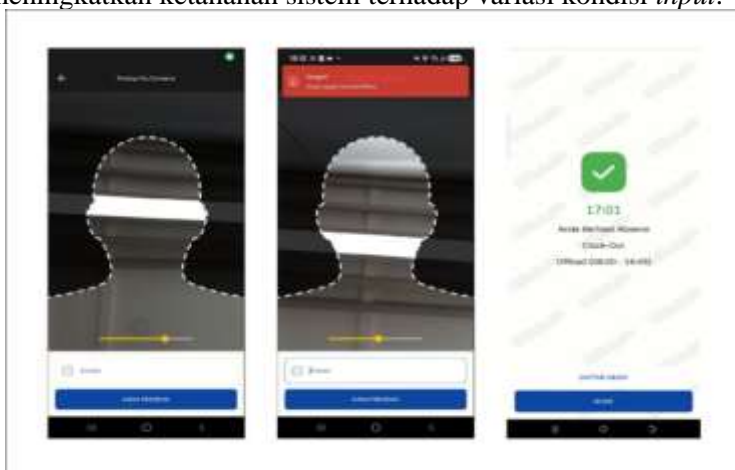


Gambar 2 Alur fitur pengenalan wajah

Selanjutnya, skor similarity akhir dibandingkan dengan data wajah yang tersimpan dalam basis data menggunakan nilai ambang batas atau *threshold*. Jika nilai *similarity* memenuhi atau melebihi *threshold*, maka sistem menganggap wajah valid dan data presensi diproses. Sebaliknya, jika nilai *similarity* berada di bawah *threshold*, sistem akan menolak autentikasi dan memberikan notifikasi kegagalan. Perancangan ini menekankan proses autentikasi yang terstruktur dan berbasis perhitungan matematis melalui pendekatan *multi-feature similarity*, sehingga mampu meningkatkan akurasi identifikasi serta meminimalkan potensi kecurangan dalam sistem presensi.

4.7 Konstruksi dan Pengujian

Berdasarkan metodologi yang telah ditetapkan pada Bab 3, implementasi sistem dilakukan dalam bentuk aplikasi mobile berbasis *Flutter* dan diuji terhadap 655 karyawan. Proses verifikasi dilakukan dengan membandingkan citra wajah yang diambil secara *real-time* dengan data wajah yang telah tersimpan sebelumnya. Validasi identitas dilakukan menggunakan pendekatan *multi-feature similarity* berbasis *face embedding*, dengan *face embedding* sebagai komponen utama *appearance similarity* serta *geometry similarity*, *quality score*, *color similarity*, dan *texture similarity* sebagai fitur pendukung untuk meningkatkan ketahanan sistem terhadap variasi kondisi *input*.



Gambar 3 Desain fitur pengenalan wajah

Alur kerja fitur ini diilustrasikan pada Gambar 3. Sistem akan memberikan umpan balik instan berdasarkan hasil pemindaian wajah. Jika wajah tidak terdeteksi atau nilai *similarity* tidak memenuhi *threshold*, sistem akan menampilkan pesan bahwa wajah tidak ditemukan atau tidak valid. Sebaliknya, apabila nilai *similarity* memenuhi *threshold*, sistem akan mengonfirmasi bahwa data wajah valid dan presensi berhasil dikirimkan.

Untuk mencapai tingkat presisi yang tinggi, sistem menerapkan *pipeline* verifikasi wajah berbasis *multi-feature similarity*. *Pipeline* ini mencakup deteksi wajah, ekstraksi area wajah berbasis

landmark, preprocessing citra, ekstraksi *face embedding* sebagai komponen utama *appearance similarity*, serta penggabungan fitur pendukung berupa *geometry similarity*, *quality score*, *color similarity*, dan *texture similarity*. Dengan *pipeline* tersebut, proses validasi identitas tidak hanya bergantung pada satu jenis fitur kemiripan, tetapi juga mempertimbangkan beberapa karakteristik citra wajah agar hasil verifikasi lebih stabil dan lebih andal.

Proses deteksi wajah dilakukan menggunakan *Google ML Kit* dengan konfigurasi mode akurat serta mengaktifkan fitur *landmark detection*. Pendekatan ini memungkinkan sistem memperoleh informasi detail terkait posisi fitur wajah seperti mata, hidung, mulut, dan telinga. Berbeda dengan metode konvensional yang hanya menggunakan *bounding box*, penelitian ini menggunakan pendekatan berbasis *landmark* untuk menentukan area wajah serta lebih presisi. Hal ini sejalan dengan temuan Golob [17] yang menyatakan bahwa area wajah seperti mulut dan hidung mengandung informasi krusial yang jika terhambat atau tidak terdeteksi akan menurunkan kinerja sistem secara signifikan. Dengan demikian, penggunaan *landmark* bertujuan untuk meminimalkan gangguan dari elemen non-wajah serta menghasilkan rasio wajah yang lebih konsisten meskipun terdapat variasi pada aksesori wajah.

Citra wajah hasil ekstraksi selanjutnya diproses melalui tahap *preprocessing* yang meliputi perubahan ukuran citra menjadi 56×56 piksel, konversi ke *grayscale*, serta normalisasi nilai piksel untuk menyederhanakan informasi citra dan menstabilkan distribusi data. Proses normalisasi dilakukan menggunakan pendekatan standar deviasi sebagaimana ditunjukkan pada Persamaan (1), di mana nilai piksel dikurangi dengan rata-rata dan dibagi dengan standar deviasi.

$$x' = (x - \mu) / \sigma \quad (1)$$

Selanjutnya, dilakukan normalisasi vektor menggunakan *L2 normalization* sebagaimana ditunjukkan pada Persamaan (2) untuk memastikan setiap vektor *embedding* memiliki panjang yang seragam sehingga proses perbandingan menjadi lebih konsisten.

$$v = v / \|v\| \quad (2)$$

Citra wajah kemudian diproses menggunakan model berbasis *deep learning* untuk menghasilkan *face embedding* berupa vektor numerik yang merepresentasikan karakteristik utama wajah. *Face embedding* ini digunakan sebagai dasar perhitungan *appearance similarity*. Perhitungan *appearance similarity* dilakukan menggunakan *cosine similarity* sebagaimana ditunjukkan pada Persamaan (3), yang mengukur kesamaan arah antara dua vektor *embedding*.

$$\cos(\theta) = (A \cdot B) / (\|A\| \|B\|) \quad (3)$$

Selain *appearance similarity*, sistem juga mempertimbangkan *geometry similarity* yang dihitung berdasarkan perbandingan posisi *landmark* wajah menggunakan *Mean Absolute Error (MAE)* sebagaimana ditunjukkan pada Persamaan (4). Nilai *MAE* yang lebih kecil menunjukkan bahwa struktur *landmark* wajah semakin mirip, sehingga dapat mendukung proses verifikasi identitas.

$$MAE = (1/n) \sum |x_i - y_i| \quad (4)$$

Selain *geometry similarity*, sistem juga mempertimbangkan *quality score*, *color similarity*, dan *texture similarity*. *Quality score* digunakan untuk menilai kualitas input citra berdasarkan ukuran wajah, pose, dan ketajaman citra. *Color similarity* digunakan untuk membandingkan distribusi warna citra, sedangkan *texture similarity* digunakan untuk membandingkan pola intensitas citra. Ketiga fitur pendukung tersebut digunakan untuk meningkatkan ketahanan sistem terhadap variasi kondisi input, seperti pencahayaan, pose wajah, jarak kamera, blur, dan oklusi sebagian wajah.

Seluruh komponen *similarity* kemudian digabungkan menggunakan metode pembobotan sebagaimana ditunjukkan pada Persamaan (5). Bobot terbesar diberikan pada *appearance similarity* karena *face embedding* merupakan representasi utama wajah, sedangkan *geometry similarity*, *quality score*, *color similarity*, dan *texture similarity* berperan sebagai fitur pendukung untuk meningkatkan stabilitas verifikasi pada kondisi input yang bervariasi.

$$\text{Similarity} = (0.82 \times \text{Appearance}) + (0.06 \times \text{Geometry}) + (0.05 \times \text{Quality}) + (0.025 \times \text{Color}) + (0.025 \times \text{Texture}) \quad (5)$$

Skenario pengujian dirancang untuk mengevaluasi kemampuan sistem dalam memvalidasi identitas pengguna pada berbagai kondisi penggunaan presensi mobile. Pengujian mencakup kondisi wajah sama dan wajah berbeda, variasi pencahayaan, ekspresi wajah, posisi wajah, jarak terhadap kamera, oklusi sebagian wajah, kondisi tanpa wajah, serta citra blur. Skenario tersebut digunakan untuk memastikan bahwa sistem tidak hanya berjalan pada kondisi ideal, tetapi juga mampu memberikan keputusan validasi yang sesuai pada kondisi input yang bervariasi. Kategori skenario pengujian yang digunakan dalam penelitian ini ditampilkan pada Tabel 1.

Tabel 1 Skenario pengujian

No.	Kategori Pengujian	Skenario	Tujuan Pengujian
1	Identitas pengguna	Wajah sama, wajah berbeda	Menguji kemampuan sistem menerima pengguna valid dan menolak pengguna tidak valid
2	Kondisi lingkungan	Pencahayaan terang, normal, rendah	Menguji kestabilan similarity pada variasi pencahayaan
3	Variasi wajah	Ekspresi netral, ekspresi senyum, posisi miring, wajah tertutup sebagian	Menguji ketahanan sistem terhadap perubahan ekspresi, pose, dan oklusi
4	Jarak kamera	Jarak dekat, sedang, jauh	Menguji pengaruh jarak wajah terhadap proses ekstraksi fitur
5	Kualitas input	Tanpa wajah, wajah blur	Menguji kemampuan sistem menolak input yang tidak memenuhi syarat validasi

Dengan pendekatan *multi-feature similarity* tersebut, sistem diharapkan mampu menghasilkan proses verifikasi wajah yang lebih akurat dan *lebih andal* dibandingkan metode yang hanya mengandalkan satu jenis fitur kemiripan. Setelah pengembangan fitur dilakukan, sistem diuji melalui API testing dan *black-box* testing untuk memastikan bahwa proses deteksi wajah, ekstraksi fitur, perhitungan *similarity*, serta keputusan validasi dapat berjalan sesuai kebutuhan sistem. Pengujian dilakukan menggunakan *threshold similarity* sebesar 0,80. Apabila nilai *similarity* sama dengan atau lebih tinggi dari *threshold*, maka wajah dikategorikan valid. Sebaliknya, apabila nilai *similarity* berada di bawah *threshold*, maka wajah dikategorikan tidak valid. Hasil pengujian pada beberapa kondisi wajah ditampilkan pada Tabel 2.

Tabel 2 Hasil pengujian dengan beberapa kondisi

No.	Skenario Wajah	Kondisi Pengujian	Similarity	Threshold	Hasil	Kesimpulan
1	Wajah sama	Kondisi normal	0,94	0,80	Valid	Sesuai
2	Wajah berbeda	Orang berbeda	0,78	0,80	Tidak valid	Sesuai
3	Pencahayaan terang	Cahaya tinggi	0,87	0,80	Valid	Sesuai
4	Pencahayaan normal	Cahaya cukup	0,87	0,80	Valid	Sesuai
5	Pencahayaan rendah	Cahaya minim	0,87	0,80	Valid	Sesuai
6	Ekspresi netral	Tanpa perubahan ekspresi	0,89	0,80	Valid	Sesuai
7	Ekspresi senyum	Perubahan ekspresi	0,86	0,80	Valid	Sesuai
8	Posisi miring	Wajah sedikit miring	0,77	0,80	Tidak valid	Sesuai
9	Jarak dekat	Wajah dekat	0,85	0,80	Valid	Sesuai

No.	Kondisi	Indikator	Similarity	Threshold	Validasi	Status
		kamera				
10	Jarak sedang	Jarak normal	0,94	0,80	Valid	Sesuai
11	Jarak jauh	Wajah jauh kamera	0,86	0,80	Valid	Sesuai
12	Tanpa wajah	Tidak ada wajah dalam gambar	0,0	0,80	Tidak valid	Sesuai
13	Wajah tertutup sebagian	Masker/tangan	0,85	0,80	Valid	Sesuai
14	Wajah blur	Gambar tidak jelas	0,0	0,80	Tidak valid	Sesuai

Berdasarkan pengujian pada Tabel 2, sistem secara konsisten memvalidasi identitas berdasarkan threshold 0,80. Skenario dengan nilai *similarity* sama dengan atau lebih tinggi dari *threshold* dikategorikan sebagai valid, sedangkan skenario dengan nilai *similarity* di bawah *threshold* dikategorikan sebagai tidak valid. Penolakan pada skenario wajah berbeda, posisi miring, tanpa wajah, dan wajah blur menunjukkan bahwa sistem mampu membedakan kondisi input yang tidak memenuhi kriteria validasi. Secara teknis, wajah blur menghilangkan detail tekstur sehingga proses ekstraksi *face embedding* dan *texture similarity* menjadi tidak optimal. Sementara itu, posisi wajah yang miring dapat meningkatkan perbedaan posisi *landmark* sehingga memengaruhi *geometry similarity* dan menurunkan nilai *similarity* akhir.

Berdasarkan 14 skenario *black-box* testing pada Tabel 2, seluruh keluaran sistem sesuai dengan hasil yang diharapkan. Dari pengujian tersebut, terdapat 10 skenario valid yang berhasil diklasifikasikan sebagai valid dan 4 skenario tidak valid yang berhasil ditolak oleh sistem. Dengan demikian, diperoleh nilai *true positive* sebanyak 10, *true negative* sebanyak 4, *false positive* sebanyak 0, dan *false negative* sebanyak 0. Berdasarkan nilai tersebut, akurasi, presisi, recall, dan *F1-score* pada pengujian skenario masing-masing mencapai 100%. Nilai ini merepresentasikan performa sistem pada skenario pengujian yang dirancang, sedangkan evaluasi operasional terhadap data pengguna dilakukan melalui pengukuran *False Acceptance Rate*, waktu verifikasi, dan perbandingan indikasi manipulasi kehadiran sebelum dan sesudah penerapan sistem.

Tabel 3 Hasil evaluasi metrik klasifikasi skenario pengujian

No.	Indikator	Nilai
1	True Positive	10
2	True Negative	4
3	False Positive	0
4	False Negative	0
5	Akurasi	100%
6	Presisi	100%
7	Recall	100%
8	F1-Score	100%

Selain pengujian fungsional, evaluasi juga dilakukan dari aspek keamanan biometrik dengan memperhatikan kemampuan sistem dalam menolak identitas yang tidak valid (Tabel 3). Indikator yang digunakan adalah *False Acceptance Rate (FAR)*, yaitu persentase kondisi ketika sistem menerima pengguna yang seharusnya ditolak. Nilai FAR digunakan untuk menilai tingkat risiko penerimaan identitas yang tidak sah pada proses presensi.

Pengujian komparatif dilakukan terhadap 655 karyawan yang tersebar di kantor pusat dan sebelas cabang regional. Berdasarkan data historis sistem presensi berbasis GPS, teridentifikasi sebanyak 70 karyawan atau 10,7% yang terindikasi melakukan manipulasi kehadiran, dengan 88% kasus terkonsentrasi pada cabang di luar kantor pusat. Praktik yang dominan meliputi *buddy punching* dan penggunaan aplikasi *mock location*. Setelah integrasi *face recognition* berbasis *multi-feature similarity* diterapkan, pengujian ulang dengan skenario identik menunjukkan penurunan signifikan. Kasus terindikasi kecurangan berkurang menjadi 1 kasus atau 0,15%, sedangkan *False Acceptance Rate* turun dari 12,8% menjadi 0,2%. Waktu verifikasi rata-rata tercatat 1200 ms, sehingga masih berada dalam batas toleransi untuk interaksi real-time pada perangkat *mobile*.

Tabel 4 Hasil perbandingan kuantitatif

No.	Indikator	Sistem GPS	Sistem Usulan	Perubahan
1	Indikasi manipulasi kehadiran	70 kasus / 10,7%	1 kasus / 0,15%	Menurun 69 kasus
2	False Acceptance Rate	12,8%	0,2%	Menurun 12,6 poin persentase
3	Mekanisme validasi presensi	GPS dan data	Face recognition berbasis multi-feature similarity	Validasi biometrik lebih kuat
4	Waktu verifikasi	-	1200 ms	Real-time pada perangkat mobile

Berdasarkan Tabel 4, sistem usulan menunjukkan peningkatan dibandingkan sistem sebelumnya berbasis *GPS*. Penurunan indikasi manipulasi kehadiran dari 70 kasus menjadi 1 kasus menunjukkan bahwa validasi biometrik mampu meminimalkan praktik *buddy punching* dan manipulasi lokasi. Selain itu, penurunan *False Acceptance Rate* dari 12,8% menjadi 0,2% menunjukkan bahwa sistem lebih selektif dalam menerima autentikasi pengguna, sehingga risiko penerimaan identitas yang tidak valid dapat ditekan. Waktu verifikasi rata-rata sebesar 1200 ms juga menunjukkan bahwa pendekatan *multi-feature similarity* masih layak digunakan pada perangkat *mobile* secara *real-time*.

Kasus residual yang tersisa menunjukkan adanya potensi ancaman manipulasi menggunakan citra wajah hasil generasi *AI* atau *deepfake* statis. Temuan ini menunjukkan bahwa pendekatan *multi-feature similarity* berbasis *face embedding* efektif dalam menekan manipulasi konvensional, seperti *buddy punching* dan penggunaan *mock location*. Namun, untuk menghadapi ancaman *spoofing* berbasis citra atau generatif *AI* secara lebih andal, sistem masih perlu dikembangkan dengan lapisan keamanan tambahan berupa *passive liveness detection*.

Kegagalan autentikasi di bawah threshold bertujuan untuk meminimalkan *False Acceptance* dan mencegah praktik *buddy punching*. Penggunaan citra wajah yang jelas dan tidak terhalang menjadi syarat penting agar sistem dapat melakukan ekstraksi *face embedding*, *landmark*, warna, tekstur, dan kualitas citra secara optimal. Dengan demikian, penerapan *multi-feature similarity* berbasis *face embedding* terbukti lebih andal dalam menjamin keabsahan kehadiran dibandingkan metode presensi konvensional yang hanya mengandalkan *GPS*.

4.8 Instalasi dan Pengiriman

Tahap instalasi dan pengiriman dilakukan setelah proses konstruksi dan pengujian fitur selesai. Pada tahap ini, aplikasi presensi berbasis *Flutter* dibangun ke dalam format *Android App Bundle (AAB)* agar siap didistribusikan kepada pengguna melalui *Google Play Store* sebagai pembaruan aplikasi. Dalam implementasinya, *Flutter* digunakan untuk mengintegrasikan modul kamera, proses pemanggilan API, pengiriman citra wajah, penerimaan hasil verifikasi, serta tampilan status validasi wajah dalam satu alur penggunaan. Integrasi ini memungkinkan pengguna melakukan presensi, memperoleh status validasi wajah, dan menerima notifikasi keberhasilan atau kegagalan secara langsung melalui perangkat *mobile*.

Proses pengiriman aplikasi juga disertai dengan penyampaian panduan penggunaan, khususnya terkait cara pengambilan citra wajah dan proses verifikasi identitas agar fitur *face recognition* dapat digunakan dengan benar. Berdasarkan hasil implementasi pada perangkat *Android*, fitur validasi identitas berbasis *multi-feature similarity* dapat berjalan dengan waktu verifikasi rata-rata 1200 ms, sehingga masih sesuai untuk kebutuhan presensi *real-time*. Dengan demikian, implementasi aplikasi berbasis *Flutter* mampu mendukung distribusi fitur *face recognition* secara praktis, sekaligus meningkatkan keamanan dan validitas data presensi pengguna.

5 Kesimpulan

Berdasarkan hasil implementasi dan pengujian, sistem presensi berbasis *Flutter* dengan pendekatan *multi-feature similarity* berbasis *face embedding* mampu meningkatkan validasi identitas pengguna. *Face embedding* digunakan sebagai komponen utama *appearance similarity* yang dihitung menggunakan *cosine similarity*, sedangkan *geometry similarity*, *quality score*, *color similarity*, dan

<http://sistemasi.ftik.unisi.ac.id>

texture similarity digunakan sebagai fitur pendukung untuk meningkatkan ketahanan sistem terhadap variasi kondisi input. Pengujian dilakukan terhadap 655 karyawan melalui uji coba langsung, *API testing*, dan *black-box testing* dengan *threshold similarity* 0,80. Hasil pengujian menunjukkan bahwa indikasi manipulasi kehadiran menurun dari 70 kasus atau 10,7% menjadi 1 kasus atau 0,15%. Selain itu, *False Acceptance Rate* menurun dari 12,8% menjadi 0,2%, dengan waktu verifikasi rata-rata 1200 ms. Dengan demikian, pendekatan yang diusulkan terbukti lebih andal dibandingkan metode presensi berbasis *GPS* dalam meminimalkan *buddy punching* dan manipulasi lokasi. Namun, sistem masih perlu dikembangkan dengan mekanisme *passive liveness detection* untuk mengantisipasi *spoofing* berbasis citra atau generatif AI.

Referensi

- [1] Y. W. S. Putra and M. F. Adhim, "Sistem Informasi Presensi Online menggunakan Teknologi *Face Recognition* dan *GPS*," *Jurnal Tekno Kompak*, Vol. 16, No. 1, pp. 149–161, 2022. <https://doi.org/10.33365/jtk.v16i1.1470>
- [2] S. Supriyadi, "Integrasi Sistem Informasi Manajemen SDM dalam Transformasi Digital: Pengaruh terhadap Efisiensi Operasional," *Jurnal Ekonomi dan Bisnis*, Vol. 4, No. 2, pp. 236–242, 2024. <https://doi.org/10.56145/jurnalekonomidanbisnis.v4i2.280>
- [3] I. Novianti and K. Khamimah, "Pengaruh Dukungan Manajemen Puncak, Pemanfaatan Teknologi Informasi, dan Pengalaman Kerja terhadap Efektivitas Sistem Informasi Akuntansi," *Serat Acitya*, Vol. 12, No. 1, pp. 221–232, 2023. <https://doi.org/10.56444/sa.v12i1.689>
- [4] N. Kurniasih and N. A. Sari, "Strategi Inovasi Manajemen untuk Meningkatkan Efisiensi dan Produktivitas di Era Digital Transformasi," *Jurnal Dinamika Sosial dan Sains*, Vol. 1, No. 3, pp. 186–192, 2025. <https://doi.org/10.60145/jdss.v1i3.68>
- [5] A. Oktavian, W. Gunawan, and M. E.-K. Kesuma, "A Reusable Library for Secure Attendance Systems: Fraud Mitigation based on QR Code and Geolocation," in *Proc. 2025 IEEE Int. Conf. Data and Software Engineering (ICoDSE)*, pp. 37–41, 2025. <https://doi.org/10.1109/ICoDSE68111.2025.11351816>
- [6] A. Khuran, B. P. Lohani, V. Bibhu, and P. K. Kushwaha, "An AI Integrated Face Detection System for Biometric Attendance Management," in *Proc. 2nd Int. Conf. Intelligent Engineering and Management (ICIEM)*, 2021. <https://doi.org/10.1109/ICIEM51511.2021.9445295>
- [7] F. Mar'i and G. Pangestu, "Classification of Fake GPS in GOJEK Application using Logistic Regression," in *Proc. 2021 Int. Conf.*, pp. 94–99, 2021. <https://doi.org/10.1145/3479645.3479657>
- [8] M. S. M. Alburaiqi, G. M. Johar, R. A. A. Helmi, and M. H. Alkawaz, "Mobile-based Attendance System: Face Recognition and Location Detection using Machine Learning," in *Proc. IEEE Int. Conf. Smart Grid Renewable Energy (ICSGRC)*, 2021. DOI: [10.1109/ICSGRC53186.2021.9515221](https://doi.org/10.1109/ICSGRC53186.2021.9515221)
- [9] R. A. Firdaus, E. D. Wahyuni, and A. Agussalim, "Rancang Bangun Sistem Presensi Pegawai berbasis Geo Lokasi dan Pengenalan Wajah menggunakan *Facenet*," *Jurnal Media Infotama*, Vol. 20, No. 2, pp. 410–416, 2024. <https://doi.org/10.37676/jmi.v20i2.6219>
- [10] E. Sudaryanto and A. Suryanto, "Sistem Presensi Pengenalan Wajah dengan Metode *Principal Component Analysis (PCA)*," *Teodolita: Media Komunikasi Ilmiah di Bidang Teknik*, Vol. 21, No. 2, pp. 55–60, 2021. <https://doi.org/10.53810/jt.v21i2.378>
- [11] T. Susim and C. Darujati, "Pengolahan Citra untuk Pengenalan Wajah (*Face Recognition*) menggunakan *OpenCV*," *Jurnal Syntax Admiration*, Vol. 2, No. 3, pp. 534–545, 2021. <https://doi.org/10.46799/jsa.v2i3.202>
- [12] M. Fikri, J. S. Kurniawan, Y. Tatiana, and Z. Abidin, "Analisis Pengaruh Efektivitas Penerapan Teknologi Biometrik, Persepsi Kegunaan, dan Persepsi Kemudahan terhadap Peningkatan Penggunaan Teknologi Biometrik di Bandara dengan Kepuasan Pelanggan sebagai Variabel Intervening," *Syntax Literate: Jurnal Ilmiah Indonesia*, Vol. 10, No. 5, pp. 4831–4840, 2025. <https://doi.org/10.36418/syntax-literate.v10i5.59090>
- [13] V. K. Hahn and S. Marcel, "Towards Protecting Face Embeddings in Mobile Face Verification Scenarios," *IEEE Trans. Biometrics, Behavior, Identity SCI.*, Vol. 4, No. 1, pp. 117–134, 2022. <https://doi.org/10.1109/TBIOM.2022.3140472>

- [14] S. Setiawansyah, P. Parjito, D. A. Megawaty, N. Nuralia, and Y. Rahmanto, "Implementation of the Framework for the Application of System Thinking for School Financial Information Systems," *Tech-E*, Vol. 5, No. 1, pp. 1–10, 2021. <https://doi.org/10.31253/te.v5i1.619>
- [15] T. Ueki, K. Yoshii, S. Shimamoto, K. Mizuno, and K. Matsufuji, "Evaluation of Impact of Intermediate GPS Spoofing to Mobile Terminals," in *Proc. 2022 IEEE 19th Annu. Consumer Commun. & Networking Conf. (CCNC)*, pp. 717–718, 2022. <https://doi.org/10.1109/CCNC49033.2022.9700524>
- [16] I. Arfianto, I. A. Ashari, and Purwono, "Implementation of Geolocator for Location Manipulation Detection in GPS-based Attendance Application at Watumas Clinic," in *Int. Conf. Health and Biological Science (ICHBS)*, pp. 124–140, 2024. <https://ichbs.uhb.ac.id/index.php/proceeding/article/view/55>
- [17] O. Golob, "Analysis of Face Detection, Face Landmarking, and Face Recognition Performance with Masked Face Images," *arXiv*, 2022. <https://doi.org/10.48550/arXiv.2207.06478>
- [18] R. Ryu, S. Yeom, S.-H. Kim, and D. Herbert, "Continuous Multimodal Biometric Authentication Schemes: A Systematic Review," *IEEE Access*, Vol. 9, pp. 34541–34557, 2021. <https://doi.org/10.1109/ACCESS.2021.3061589>
- [19] M. A. Firmansyah and A. M. Bakti, "Implementasi metode FAST untuk Pengembangan Sistem Simpan Pinjam pada Koperasi Tarbiyah berbasis Android," *Journal of Software Engineering Ampera*, Vol. 3, No. 3, pp. 133–144, 2022. <https://doi.org/10.51519/journalsea.v3i3.243>
- [20] P. R. Nisa, M. Husaini, M. E. Kesuma, and F. Satria, "Pengembangan Sistem Informasi Kasir Penjualan Obat pada Apotek dengan Pendekatan metode FAST," *Information System Journal (INFOS)*, Vol. 8, No. 2, pp. 95–108, 2025. <https://doi.org/10.24076/infosjournal.2025v8i02.2328>