

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pengenalan wajah, sebagai cabang utama dalam visi komputer, telah berkembang pesat, terutama dengan integrasi deep learning yang meningkatkan akurasi dan keandalan teknologi [1]. Dalam penelitian Li, H., pada tahun 2024 juga menyebutkan bahwa teknologi pengenalan wajah berperan penting dalam tiga bidang utama, yang pertama di sistem keamanan di mana teknologi ini memungkinan identifikasi wajah secara realtime untuk meningkatkan keamanan sosial, yang kedua di platform media sosial, dimana teknologi ini digunakan untuk meningkatkan estetika foto, mengotentikasi akun, dan meningkatkan pengelolaan album foto sehingga memperkuat keamanan akun [2], dan yang ketiga dalam sektor kesehatan, teknologi ini memfasilitasi autentikasi pasien dan analisis struktur wajah untuk membantu diagnosis medis yang lebih cepat [3]. Seiring dengan peran penting yang dimainkan oleh teknologi pengenalan wajah dalam berbagai sektor, mulai dari keamanan hingga kesehatan, aplikasi dari teknologi ini terus berkembang dan memasuki sektor baru. Seiring dengan pengembangan teknologi pengenalan wajah perkembangan ini juga merambah ke dunia pendidikan. khususnya dalam pelaksanaan ujian yang kini banyak dilakukan secara daring, memberikan fleksibilitas dan memungkinkan mahasiswa untuk menjadi lebih mandiri [4].

Namun, fleksibilitas yang ditawarkan oleh ujian daring seringkali dimanfaatkan untuk melakukan kecurangan, termasuk praktik menggunakan joki ujian, fenomena ini pertama kali dikenalkan oleh Clarke Robert dan Lancaster Thomas pada tahun 2006 sebagai ‘contract cheating’. Fenomena ini sangat mengancam integritas pendidikan karena memungkinkan individu memperoleh nilai tanpa benar-benar memahami materi. Kecurangan ini terjadi tidak hanya dalam pembelajaran tatap muka tetapi juga lebih umum dalam konteks online, dimana pengawasan cenderung lebih lemah dan sistem autentikasi sering kali tidak cukup ketat [5]. Permasalahan ini mencerminkan kelemahan yang ada dalam pengawasan dan mekanisme autentikasi yang diterapkan dalam sistem ujian berbasis internet. Banyaknya kasus kecurangan ini menunjukkan bahwa perilaku tidak etis dalam pendidikan tidak hanya dipengaruhi oleh tingkat

pengetahuan siswa, tetapi juga oleh faktor lain seperti godaan untuk mencari jalan pintas dan memanfaatkan celah dalam sistem [6].

Dalam menghadapi tantangan peningkatan keamanan dalam sistem pengawasan ujian online, penelitian William et al., pada tahun 2019 menjelaskan bahwa teknologi Machine Learning seperti FaceNet menawarkan solusi inovatif dalam mengenali wajah [7]. Integrasi FaceNet dan teknologi anti-spoofing tidak hanya meningkatkan akurasi dalam proses autentikasi peserta ujian dengan menghasilkan representasi wajah yang unik untuk mencocokkan identitas peserta secara presisi dengan data biometrik yang terdaftar, tetapi juga meningkatkan keamanan. Selain itu berdasarkan penelitian Penelitian oleh Akhdan et al., tahun 2023 membahas teknologi anti-spoofing dalam sistem biometrik, khususnya pengenalan wajah, yang meliputi deteksi kedipan berdasarkan nilai Eye Aspect Ratio. Teknik ini diklasifikasikan menggunakan SVM dan MLP untuk menangkal upaya penipuan, menggabungkan deteksi kedipan dengan pengenalan wajah untuk menangani serangan spoofing statis, meski belum efektif terhadap spoofing dinamis [8].

Sejalan dengan hal ini, Andri Nugraha Ramdhon dan Fadly Febriya, pada tahun 2021 menjelaskan bahwa teknologi pengenalan wajah telah menunjukkan efektivitas dalam berbagai aplikasi presensi, dengan tingkat keberhasilan hingga 86,85% ketika menggunakan metode yang dioptimalkan. Selain itu, Ganidisastra & Bandung, 2021 menyoroti pentingnya verifikasi pengguna secara berkelanjutan dalam ujian online untuk mendeteksi kehadiran peserta palsu (joki). Penelitian mereka menunjukkan bahwa algoritma FaceNet dengan metode incremental training mampu mempertahankan akurasi tinggi hingga 98%, sambil mengurangi ukuran dataset dan waktu pelatihan dibandingkan dengan metode batch training tradisional. Solusi yang telah dijelaskan sebelumnya menunjukkan potensi besar dalam mendukung pelaksanaan ujian online yang lebih aman dan adil. Namun, untuk menguatkan argumen dan memberikan pemahaman yang lebih mendalam, penting untuk merujuk pada hasil-hasil penelitian sebelumnya yang telah menunjukkan keberhasilan dalam implementasi teknologi terkait. Penelitian-penelitian ini tidak hanya menggambarkan efektivitas teknologi seperti FaceNet dan anti-spoofing, tetapi juga mengungkapkan kekurangan yang perlu diperbaiki untuk meningkatkan sistem secara keseluruhan [10].

Sebagai contoh, dalam studi yang diterbitkan oleh Hernandez-Ortega et al., pada tahun 2019, berjudul "FaceQnet: Quality Assessment for Face Recognition Based on

Deep Learning", menunjukkan bahwa kualitas sampel wajah memiliki korelasi yang signifikan dengan akurasi sistem verifikasi biometrik. Studi tersebut mengungkapkan bahwa performa sistem pengenalan wajah meningkat sejalan dengan peningkatan kualitas data yang digunakan. Hal ini menegaskan pentingnya memastikan kualitas tinggi dalam pengambilan sampel wajah untuk mencapai tingkat verifikasi yang lebih akurat dan efisien. Selain itu, penelitian yang dilakukan oleh Yu et al. pada tahun yang sama, yang berjudul "Central Difference Convolutional Networks for Face Anti-Spoofing", menyoroti pentingnya teknologi anti-spoofing dalam sistem pengenalan wajah. Penelitian ini berfokus pada pengembangan jaringan konvolusi yang dapat membedakan antara wajah asli dan wajah yang direproduksi melalui media seperti gambar palsu [12]. Teknologi ini sangat penting untuk memastikan keabsahan identitas pengguna dan mencegah manipulasi biometrik, yang dapat mencakup penggunaan gambar untuk menipu sistem. Melalui teknologi ini, sistem pengenalan wajah tidak hanya menjadi lebih aman tetapi juga lebih dapat diandalkan dalam berbagai aplikasi keamanan dan pengawasan.

Pada sisi lain, kajian terkait FaceNet, yang dipublikasikan oleh William et al. pada tahun 2019, menunjukkan bahwa model ini mampu mencapai akurasi tinggi hingga 100% pada beberapa dataset, menjadikannya pilihan unggul untuk aplikasi pengenalan wajah. Studi ini mengungkapkan bahwa FaceNet tidak hanya mengungguli metode-metode tradisional seperti PCA (Principal Component Analysis), LDA (Linear Discriminant Analysis), dan sgFKNN (Sparse Generative Feature Kernel Nearest Neighbor) dalam berbagai pengujian, tetapi juga menunjukkan kemampuan superior dalam memanfaatkan teknologi canggih. Keunggulan FaceNet didukung oleh kemampuannya dalam memanfaatkan model pra-latih TensorFlow dan teknologi machine learning yang canggih, menghasilkan representasi wajah unik dalam ruang Euclidean yang memungkinkan pencocokan wajah dengan tingkat presisi yang tinggi. Model pra-latih seperti VGGFace2, yang juga digunakan dalam kajian ini, terbukti memberikan akurasi yang lebih baik dibandingkan dengan model-model lain seperti Casia-WebFace. Ini menunjukkan pentingnya memilih dataset dan arsitektur yang tepat untuk melatih model pengenalan wajah agar dapat berfungsi dengan optimal dalam berbagai kondisi dan aplikasi. Penerapan FaceNet dalam lingkungan nyata menawarkan berbagai manfaat, termasuk peningkatan keamanan melalui verifikasi identitas yang lebih akurat dan cepat. Hal ini sangat relevan di sektor-sektor seperti

keamanan publik, kontrol akses, dan sistem pengawasan, di mana kebutuhan untuk mengidentifikasi individu secara cepat dan tepat menjadi sangat kritikal. Dengan menggunakan model seperti FaceNet yang telah terbukti efektif dalam mengidentifikasi fitur wajah yang krusial, aplikasi-aplikasi ini dapat lebih mudah mendeteksi dan mencegah potensi ancaman keamanan atau penyalahgunaan identitas [7].

Namun, penelitian lain mengungkapkan keterbatasan pendekatan manual dalam mendeteksi kecurangan ujian online, seperti kesulitan memverifikasi kemiripan antara foto identitas dan wajah peserta. Hal ini membutuhkan waktu yang lama dan rentan terhadap kesalahan manusia [13]. Sebagaimana yang telah dibahas dalam literatur sebelumnya, teknologi pengenalan wajah dan anti-spoofing telah terbukti meningkatkan keamanan dan keadilan dalam pelaksanaan ujian online. Misalnya, studi FaceQnet menunjukkan bahwa kualitas sampel wajah yang tinggi berkontribusi pada akurasi sistem verifikasi biometrik yang lebih tinggi, sedangkan kajian terkait FaceNet mendemonstrasikan bahwa model ini mampu mencapai akurasi hingga 100% pada beberapa dataset, menawarkan solusi yang sangat efektif dibandingkan metode tradisional. Namun, penelitian Suhandana et al., 2023. mengungkapkan bahwa metode manual masih menghadapi tantangan dalam verifikasi identitas, menyoroti kebutuhan akan teknologi yang lebih canggih. Oleh karena itu, penemuan-penemuan ini memperkuat argumen bahwa integrasi teknologi canggih, seperti pengenalan wajah dan anti-spoofing, adalah langkah yang sangat diperlukan untuk meningkatkan keandalan dan efisiensi sistem pengawasan ujian online [13].

Berdasarkan literatur di atas, penelitian ini bertujuan untuk membuat model deteksi yang berfokus pada eye blink detection untuk anti-spoofing. Kehadiran teknologi pengenalan wajah telah menjadi komponen kunci dalam banyak sektor, mulai dari keamanan hingga pendidikan, menggabungkan teknologi ini dalam pengawasan ujian online membuka peluang besar untuk menangani kecurangan. Sejalan dengan hal ini, model yang akan dikembangkan bertujuan untuk mengintegrasikan teknologi deteksi kedipan dengan pengenalan wajah guna memberikan solusi komprehensif yang tidak hanya mendeteksi tetapi juga mencegah upaya manipulasi biometrik yang semakin canggih.

1.2. Rumusan Masalah

Berdasarkan penjabaran latar belakang di atas, kecurangan dalam ujian online menjadi tantangan yang semakin serius di era digital, dengan kehadiran "joki" yang mengancam integritas akademis. Teknologi pengenalan wajah, khususnya yang berbasis FaceNet, telah menunjukkan potensi signifikan dalam mengidentifikasi peserta secara akurat. Namun, teknologi ini masih rentan terhadap manipulasi, seperti penggunaan gambar atau video palsu, yang dapat mengurangi efektivitas sistem pengawasan. Dengan mengintegrasikan teknologi anti-spoofing, diharapkan dapat meningkatkan kemampuan sistem untuk mendeteksi dan mencegah upaya kecurangan semacam ini maka dirumuskan masalah sebagai berikut :

1. Bagaimana penerapan teknologi pengenalan wajah berbasis FaceNet yang dikombinasikan dengan solusi Eye Blink Detection untuk anti-spoofing dapat secara efektif mendeteksi dan mengeliminasi kehadiran joki dalam ujian online, serta apa saja tantangan yang mungkin dihadapi dalam implementasinya?
2. Bagaimana efektivitas dan akurasi model pengenalan wajah berbasis FaceNet yang dikombinasikan dengan Eye Blink Detection dalam mendeteksi kecurangan dalam ujian online dapat dievaluasi, serta apa saja metrik yang akan digunakan untuk mengukur kinerja dan keandalan sistem ini dalam kondisi nyata?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan, penulis memiliki tujuan dalam penelitian ini yang dapat diidentifikasi sebagai berikut :

1. Mengembangkan model pengenalan wajah berbasis FaceNet yang efektif untuk identifikasi dan verifikasi peserta ujian online.
2. Mengintegrasikan teknologi anti-spoofing ke dalam model pengenalan wajah untuk meningkatkan keamanan dengan mencegah penggunaan identitas palsu melalui gambar.
3. Evaluasi performa model berdasarkan akurasi, dan efisiensi model gabungan FaceNet dan anti-spoofing dalam mendeteksi kehadiran joki dan memverifikasi identitas yang sah.

1.4. Manfaat Penelitian

Diharapkan dengan kegunaan pada penelitian ini dapat diambil beberapa manfaat sebagai berikut :

1. Manfaat Akademis:
 - a. Menjadi referensi penting bagi penelitian selanjutnya dalam bidang pengenalan wajah dan teknologi anti-spoofing berbasis FaceNet.
 - b. Memperkaya literatur terkait inovasi teknologi machine learning, khususnya deep learning, dalam meningkatkan keamanan sistem ujian online.
2. Manfaat Praktis:
 - a. Menyediakan solusi yang efektif, efisien, dan dapat diandalkan dalam pengenalan wajah serta deteksi spoofing berbasis FaceNet.
 - b. Memperkuat sistem autentikasi dalam ujian online untuk mengurangi praktik joki ujian.
3. Manfaat Aplikasi Luas:
 - a. Membuka peluang penerapan teknologi pengenalan wajah dan anti-spoofing dalam berbagai bidang, seperti sektor perbankan, keamanan, dan layanan publik.
 - b. Mendukung pengembangan autentikasi biometrik yang akurat dan aman untuk berbagai kebutuhan.
4. Manfaat Inovasi Teknologi:
 - a. Menginspirasi pengembangan sistem keamanan yang lebih canggih dan adaptif terhadap ancaman baru.
 - b. Membantu menciptakan standar baru dalam pengujian integritas akademik secara digital.
5. Manfaat Sosial dan Industri:
 - a. Memberikan dampak positif yang lebih luas dalam dunia pendidikan, terutama dalam meningkatkan integritas akademik.
 - b. Berkontribusi pada pengembangan teknologi keamanan untuk industri terkait.

1.5. Batasan Penelitian

Batasan-batasan dalam penelitian ini dirancang untuk memastikan fokus pada pengembangan dan evaluasi algoritma berbasis FaceNet dengan integrasi teknik anti-spoofing sebagai solusi yang efisien untuk aplikasi pengenalan pola dalam visi komputer secara real-time. Penelitian ini secara khusus tidak mencakup aspek-aspek

di luar konteks pengenalan pola yang dapat memperluas ruang lingkup secara tidak terkendali. Adapun batasan-batasan penelitian ini sebagai berikut :

- a. Penelitian ini difokuskan pada proses pengenalan wajah berdasarkan identitas mahasiswa yang terdiri atas 150 gambar dari 15 identitas mahasiswa sebagai data primer.
- b. Algoritma yang dikembangkan dan diuji dalam penelitian ini dirancang untuk aplikasi visi komputer secara real-time, namun pengujian dilakukan dalam lingkungan simulasi menggunakan perangkat lunak python, tanpa implementasi langsung pada perangkat keras.
- c. Penelitian ini hanya mencakup mengenali wajah dalam format berbasis gambar dan deteksi kedipan mata untuk fitur anti-spoofing.
- d. Penelitian ini tidak mencakup serangan video (*replay attack*).
- e. Penelitian ini tidak mencakup serangan *deepfake*.
- f. Penelitian ini tidak mencakup penggunaan masker wajah.
- g. Validasi hasil deteksi dilakukan terbatas pada dataset yang digunakan dalam penelitian ini, tanpa melibatkan data eksternal atau dataset tambahan.
- h. Gambar uji yang digunakan berupa citra standar dengan format 'JPG'.

Dataset yang digunakan memiliki format penamaan file yang spesifik dari nama mahasiswa untuk mengidentifikasi pemilik identitas dari mahasiswa.

Halaman ini sengaja dikosongkan