# Pengembangan Model Pengawas Berbasis Kecerdasaan Buatan untuk Ujian Online

Firdaus Bagus Wicaksono[1], Yuni Yamasari[2]

[1,2] Program Studi S1Teknik Informatika, Universitas Negeri Surabaya
[1]firdausbagus.20094@mhs.unesa.ac.id
[2]yuniyamasari@unesa.ac.id

***Abstrak*— Ujian online telah menjadi pilihan utama dalam menilai kompetensi mahasiswa di era digital karena kemudahannya yang efisien. Namun, tantangan utama yang muncul adalah meningkatnya kasus kecurangan elektronik yang berpotensi merusak integritas akademik. Penelitian ini bertujuan untuk mengembangkan model pengawas berbasis kecerdasan buatan yang mampu mendeteksi berbagai perilaku curang selama ujian online secara real-time. Dengan memanfaatkan algoritma Local Binary Pattern Histogram untuk pengenalan wajah dan framework Mediapipe Face Detection untuk deteksi wajah, sistem ini dirancang untuk memberikan solusi pengawasan yang inovatif dan andal.**

**Analisis data dilakukan dengan fokus pada deteksi gerakan kepala dan mata, verifikasi identitas peserta ujian, serta identifikasi penggunaan alat bantu dan kolusi yang tidak sah. Landasan teori mengintegrasikan teknologi computer vision dan machine learning untuk menciptakan sistem pengawasan yang cerdas.**

**Hasil uji menunjukkan performa yang menjanjikan: pengenalan wajah mencapai akurasi 80% dalam waktu 576,66 detik, estimasi arah wajah meraih akurasi 100% dengan waktu 3009,68 detik, dan pelacakan multi-orang mencatat akurasi 96% dalam 827,34 detik. Temuan ini menunjukkan potensi besar dalam meningkatkan keamanan dan kejujuran pelaksanaan ujian online, sekaligus membuka jalan bagi implementasi pengawasan berbasis kecerdasan buatan yang lebih luas di masa depan.**

***Kata Kunci*— ujian online, kecerdasaan buatan, algoritma local binary pattern histogram, mediapipe, computer vision, deteksi perilaku curang**

## I. PENDAHULUAN

Ujian Ujian online telah menjadi alternatif populer di perguruan tinggi karena menawarkan efisiensi dan fleksibilitas tinggi. Dengan berbagai format soal seperti pilihan ganda, isian singkat, dan esai, ujian ini dapat diakses secara daring melalui internet atau intranet, sehingga memungkinkan institusi pendidikan mengelola ujian tanpa harus mengumpulkan peserta di lokasi tertentu [1]. Namun, fenomena kecurangan elektronik yang semakin meluas mengancam integritas ujian dan reputasi institusi pendidikan [2]. Oleh karena itu, diperlukan solusi yang lebih inovatif untuk mencegah dan mendeteksi kecurangan ini secara efektif.

Penerapan teknologi berbasis kecerdasan buatan menjadi solusi menjanjikan dalam pengawasan ujian online. Dengan teknologi ini, proses pengawasan dapat dilakukan secara otomatis dan objektif, mengurangi keterbatasan metode pengawasan manusia, terutama untuk skala ujian yang besar. Teknologi kecerdasan buatan seperti machine learning memungkinkan sistem mengenali pola tertentu dan mendeteksi perilaku mencurigakan selama ujian berlangsung, sehingga integritas ujian tetap terjaga [3].

Data penelitian terdahulu menunjukkan bahwa teknologi berbasis machine learning dapat secara signifikan meningkatkan akurasi pengawasan ujian. Menurut penelitian Singh dan Das [4] , teknologi YOLOv3, konfigurasi DenseNet, dan model Caffe dari OpenCV dapat digunakan untuk mendeteksi keberadaan alat bantu tidak sah serta melacak penanda wajah dan gerakan mata peserta ujian secara real-time. Penelitian oleh Gopalakrishnan dkk. [5] juga menunjukkan pentingnya solusi biometrik dalam pengawasan ujian jarak jauh guna meningkatkan otentikasi dan keamanan sistem. Selain itu, menurut Asker dan Al-Allaf [2], sistem berbasis kecerdasan buatan dapat mendeteksi gerakan mencurigakan dan penggunaan perangkat tambahan melalui analisis video real-time menggunakan webcam dan algoritma pembelajaran mendalam.

Machine learning, yang merupakan cabang kecerdasan buatan, memungkinkan komputer belajar dari data tanpa harus diprogram secara eksplisit. Teknologi ini terdiri dari tiga jenis pembelajaran: supervisi, tanpa supervisi, dan penguatan. Dalam pembelajaran supervisi, algoritma belajar dari data yang dilabeli; sedangkan pada pembelajaran tanpa supervisi, algoritma mengidentifikasi pola tersembunyi tanpa data label. Adapun pembelajaran penguatan, algoritma belajar melalui interaksi dengan lingkungan dan menerima umpan balik berdasarkan tindakannya [3]. Pendekatan ini memungkinkan machine learning digunakan dalam berbagai aplikasi seperti pengenalan wajah, pengenalan suara, dan deteksi perilaku mencurigakan.

Salah satu algoritma yang digunakan dalam pengenalan wajah adalah Local Binary Pattern Histogram (LBPH). LBPH bekerja dengan membagi citra wajah menjadi grid-grid kecil, menghitung pola biner lokal berdasarkan intensitas piksel, dan menghasilkan histogram yang merepresentasikan tekstur unik wajah[6]. Histogram ini menjadi dasar dalam proses identifikasi dan verifikasi wajah. Metode ini dikenal sederhana, cepat, dan andal meskipun dalam kondisi pencahayaan yang bervariasi, sehingga menjadi pilihan utama untuk mendeteksi wajah dalam pengawasan ujian online.

Framework Mediapipe juga menjadi komponen penting dalam deteksi wajah secara real-time. Dengan teknologi BlazeFace, Mediapipe Face Detection memungkinkan deteksi wajah yang efisien, bahkan pada perangkat dengan sumber

daya terbatas [7]. Mediapipe mendukung berbagai aplikasi, seperti pelacakan gerakan wajah, klasifikasi ekspresi, dan segmentasi wilayah wajah. Kemampuannya yang ringan dan responsif membuat Mediapipe sangat cocok untuk digunakan dalam pengawasan ujian berbasis video.

Teknologi neural network juga berperan penting dalam meningkatkan akurasi sistem pengawasan berbasis kecerdasan buatan. Neural network meniru cara kerja otak manusia dengan memproses data menggunakan neuron buatan yang diatur dalam lapisan-lapisan [8]. Dengan arsitektur yang kompleks, neural network mampu menangani hubungan non-linear antara input dan output, menjadikannya alat yang efektif dalam pengenalan wajah, prediksi data, dan deteksi pola kompleks dalam pengawasan ujian online.

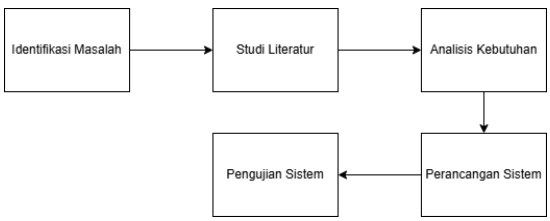
Penelitian lain seperti yang dilakukan oleh Khanna dkk. [9] menambahkan bahwa integrasi teknologi pelacakan tatapan mata, deteksi perangkat seluler, dan deteksi kehadiran orang lain mampu menjaga integritas ujian online dengan lebih baik. Tweissi dkk. [10] juga menyoroti bahwa meskipun sistem AiAP telah digunakan secara luas, masih diperlukan pembaruan untuk memenuhi standar keakuratan dan integritas akademik yang lebih tinggi.

Dengan kombinasi teknologi machine learning, LBPH, framework Mediapipe, dan neural network, penelitian ini bertujuan mengembangkan model pengawas ujian online yang lebih aman dan akurat. Model ini tidak hanya menjaga integritas ujian tetapi juga memberikan pengalaman yang lebih nyaman bagi mahasiswa dan institusi pendidikan. Hasil penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan teknologi pendidikan dan menjadi solusi inovatif untuk mengatasi tantanga pengawasan ujian online.

## II. METODOLOGI PENELITIAN

### *A. Metodologi Penelitian*

Dalam menjalankan penelitian tentang pengembangan model pengawas berbasis kecerdasan buatan untuk ujian online sejumlah batasan telah ditetapkan untuk memandu setiap langkah penelitian yang akan dijelaskan dalam bab ini. Tujuannya adalah untuk memastikan bahwa penelitian mengikuti pedoman yang ditetapkan sehingga hasilnya sesuai dengan tujuan penelitian. Gbr.1 adalah diagram yang menggambarkan langkah-langkah penelitian ini, dengan urutan tahapan sebagai berikut :




Gbr. 1 Diagram Alur Metode Penelitian

### *B. Studi Literatur*

Langkah selanjutnya, yaitu melakukan studi literatur dengan mempelajari teori mengenai machine learning dan pengolahan citra. Teori-teori tersebut didapatkan dari beberapa jurnal untuk mempermudah dalam melakukan penelitian sehingga tidak melenceng dari tujuan.

### *C. Analisis Kebutuhan*

Tahap yang dilakukan setelah studi literatur adalah menganalisis kebutuhan apa saja yang diperlukan untuk menyelesaikan masalah Pengembangan model pengawas berbasis kecerdasan buatan untuk ujian online. Untuk menunjang seluruh proses tersebut, diperlukan beberapa kebutuhan, yaitu:

*1) Kebutuhan perangkat keras (hardware)*

Berikut merupakan spesifikasi dari perangkat keras yang digunakan untuk menunjang penelitian ini:

| | |
|---|---|
| Prosesor | : Intel Core i5 11400H |
| GPU | : Nvidia Geforce RTX 3050 |
| RAM | : 16 GB |
| Penyimpanan | : SSD 1,5 TB |
| Sistem Operasi | : Windows 11 Home 64-bit |

*2) Kebutuhan perangkat lunak (software)*

Berikut beberapa kebutuhan perangkat lunak yang digunakan untuk menunjang penelitian ini:

- Python 3.7.16
- TensorFlow 2.10.0
- Mediapipe 0.9.0.1
- Flask 2.2.2
- PyCharm 2023.3.3 (Professional Edition)
- Browser Chrome versi 116.0.5845.97

### *D. Perancangan Sistem*

Penelitian ini melibatkan pengembangan model pengenalan wajah berbasis Local Binary Pattern Histogram (LBPH) dan perancangan sistem yang mencakup pengenalan wajah peserta, perkiraan arah wajah, serta deteksi dan pelacakan multi-orang.

1. Pengembangan Model Face Recognition dengan LBPH
   a) Pra-pemrosesan gambar wajah : gambar wajah dipotong, diubah ke skala abu-abu, dan dipersiapkan agar fitur-fitur lokal lebih mudah dikenali oleh model tanpa gangguan dari warna atau latar belakang
   b) Penerapan LBP pada gambar : setiap piksel wajah diproses dengan membandingkan intensitas piksel pusat dengan tetangganya, menghasilkan nilai biner. Nilai biner ini dikonversi ke kode desimal untuk membentuk matriks LBP. Misalkan $I_c$ adalah nilai intensitas piksel pusat dan $I_p$ adalah nilai intensitas piksel tetangga. Setiap piksel tetangga diberi nilai biner berdasarkan kondisi berikut: jika intensitas $I_p$ lebih besar dari $I_c$, piksel tersebut diberi nilai 1; jika lebih kecil, diberi nilai 0. Setiap piksel tetangga diberi nilai biner berdasarkan kondisi (1).

$$f(I_P, I_c) = \begin{cases} 1 \text{ jika } I_P \geq I_C \\ 0 \text{ jika } I_P < I_C \end{cases} \quad (1)$$

Nilai biner dari tetangga kemudian digabungkan dalam urutan tertentu untuk menghasilkan kode LBP desimal. Misalkan ada 8 tetangga (rata-rata pada matriks 3x3), maka rumus LBP didefinisikan sebagai berikut (2)

$$LBP(x,y) = \sum_{p=0}^{P-1} f(I_p - I_c).\, 2^p \quad (2)$$

Di mana:

- P adalah jumlah tetangga (rata-rata 8).
- $I_p$ dan $I_c$ adalah intensitas piksel tetangga dan piksel pusat.
- Nilai LBP yang dihasilkan untuk setiap piksel ini disimpan dalam bentuk matriks LBP.

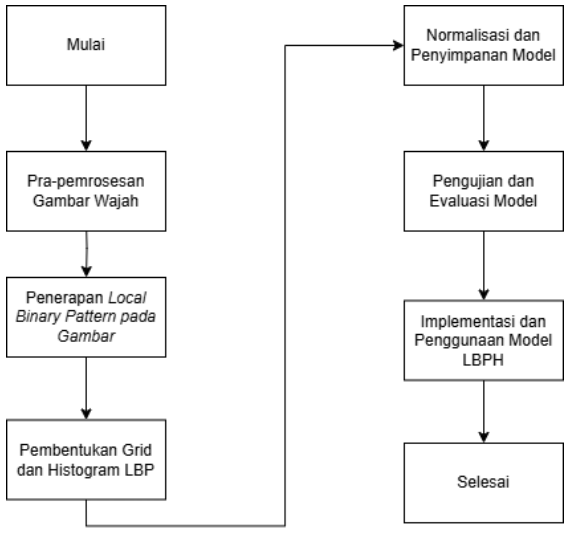
c) Pembentukan Grid dan Histogram LBP Gambar dibagi menjadi grid kecil untuk menghasilkan histogram LBP di setiap area. Histogram ini menunjukkan frekuensi pola LBP, mencatat tekstur lokal wajah.

d) Normalisasi dan Penyimpanan Model Histogram dinormalisasi untuk menjaga konsistensi antar-fitur, kemudian disimpan bersama identitas yang relevan.

e) Pelatihan dan Pembuatan Model LBPH Model dilatih dengan menghitung jarak histogram antara data input dan database menggunakan metrik jarak seperti Euclidean.

f) Pengujian dan Evaluasi Model Model diuji menggunakan dataset untuk mengukur akurasi dalam berbagai kondisi, seperti pencahayaan, sudut pandang, dan ekspresi wajah.

Gbr. 2 menunjukan langkah -langkah dari alur proses pengembangan model face recognition dengan LBPH yang akan dibangun :




Gbr. 2 Flowchart pengembangan model Local Binary Pattern Histogram

2. Perancangan Perancangan model keseluruhan sistem ini menggunakan analisis rekaman video ujian atau Recorded Proctoring, yang memusatkan perhatian pada peninjauan rekaman video sepanjang sesi ujian. Recorded Proctoring menjadi solusi efisien dan andal untuk pendidikan jarak jauh dalam hal efektivitas biaya dan kemudahan pemantauan terbaru.[11] . Proses ini meliputi:
   - Pengumpulan Rekaman Video: Rekaman disimpan dalam basis data aman.
   - Analisis Rekaman: Sistem AI menganalisis rekaman untuk mendeteksi perilaku mencurigakan.
   - Pendeteksian Kecurangan: Tanda-tanda seperti berbicara dengan orang lain atau penggunaan alat bantu ilegal diidentifikasi.
   - Tindakan Lanjutan: Bukti kecurangan diproses sesuai kebijakan institusi.

3. Kriteria Batas Toleransi Kecurangan
   - Tidak Menghadap Kamera lebih dari 5 Detik
     Peserta ujian yang tidak menghadap kamera selama lebih dari 5 detik dianggap melampaui batas toleransi, mengingat gerakan mata alami biasanya berlangsung dalam rentang waktu yang jauh lebih singkat Lla . Durasi ini cukup untuk mengindikasikan adanya upaya menghindari pengawasan atau mencari bantuan eksternal.
   - Kehadiran Lebih dari Dua Orang
     Kehadiran lebih dari dua orang dalam frame kamera selama ujian berlangsung dianggap sebagai indikasi adanya bantuan dari pihak luar, yang dapat meningkatkan risiko kecurangan. Sistem deteksi ini menggunakan algoritma deteksi wajah dan pelacakan multi-orang untuk memantau jumlah individu dalam frame, sehingga mampu mendeteksi potensi pelanggaran secara efektif tanpa memerlukan pengawasan langsung [12].
   - Ketidaksesuaian Identitas Wajah
     Ketidaksesuaian wajah peserta ujian dengan data terdaftar merupakan pelanggaran serius yang dapat mengindikasikan penyamaran atau penggunaan joki ujian. Teknologi pengenalan wajah digunakan untuk mencocokkan identitas peserta dengan data sistem dan mendeteksi perilaku tidak adil. Sistem ini memantau siswa secara efisien, mengidentifikasi tindakan tidak etis, ilegal, dan curang tanpa memerlukan pengawas langsung [13] .

### *E. Implementasi dan Pengujian*

Dalam pengujian sistem pengawas berbasis kecerdasan buatan untuk ujian online, terdapat dua aspek utama yang perlu diuji: akurasi pendeteksian kecurangan peserta dan kecepatan analisis sistem. Berikut adalah langkah-langkah dan hal-hal yang perlu diukur dalam pengujian tersebut:

1. Akurasi Pendeteksian Kecurangan Peserta:

- Skenario Ujian: Menyusun berbagai skenario ujian yang mencakup berbagai jenis perilaku mencurigakan, seperti berkomunikasi dengan orang lain, mencari jawaban di internet, atau menggunakan perangkat tambahan.
- Rekaman Ujian: Merekam ujian yang dilakukan oleh peserta dengan berbagai skenario yang telah disusun. Analisis oleh Sistem: Menggunakan teknik kecerdasan buatan untuk menganalisis rekaman ujian dan mendeteksi tindakan mencurigakan.
- Perbandingan dengan Perilaku Sebenarnya: Membandingkan hasil deteksi sistem dengan perilaku sebenarnya yang terjadi selama ujian untuk memastikan sistem mampu mengenali kecurangan dengan akurat.

2. Kecepatan Analisis Sistem:
   - Waktu Respons: Mengukur waktu yang diperlukan sistem untuk menganalisis rekaman ujian dan mengidentifikasi tindakan mencurigakan.
   - Efisiensi: Memastikan bahwa sistem mampu mengolah rekaman ujian dengan cepat dan efisien tanpa mengorbankan akurasi deteksi.
   - Pengujian Kinerja: Melakukan pengujian dengan memperhitungkan jumlah dan kompleksitas rekaman ujian untuk mengevaluasi kinerja sistem dalam kondisi yang berbeda-beda.

## III. HASIL DAN PEMBAHASAN

Bab ini membahas hasil implementasi dan pengujian akurasi sistem pengawasan ujian berbasis kecerdasan buatan, serta analisis faktor-faktor yang memengaruhi performa sistem.

A. Pengumpulan Data

- Persiapan Video untuk Pengenalan Wajah Video peserta ujian dikumpulkan dengan kondisi pencahayaan optimal dan latar belakang sederhana. Rekaman mencakup berbagai sudut pandang (depan, kiri, dan kanan) untuk meningkatkan akurasi pengenalan wajah.
- Ekstraksi Frame dan Pengolahan Gambar Wajah peserta diekstraksi dari video menggunakan Mediapipe, yang mendeteksi wajah pada setiap sepuluh frame per detik. Gambar wajah kemudian dikonversi ke format grayscale untuk mendukung analisis lebih lanjut. Proses ini memungkinkan deteksi wajah yang efisien dan konsisten.
- Pengumpulan Data untuk Pengujian Sistem Simulasi ujian dirancang menyerupai kondisi sebenarnya untuk merekam perilaku peserta dan mendeteksi potensi pelanggaran. Data dikumpulkan dari 20 mahasiswa, tetapi hanya 13 data yang layak digunakan setelah seleksi akibat kendala teknis seperti kualitas video rendah, kamera buram, dan kegagalan penyimpanan file.

Gbr. 3 menunjukan proses pengambilan data untuk memastikan bahwa sistem diuji dalam kondisi realistis, mendukung analisis performa sistem secara mendalam, dan memberikan gambaran yang mendekati situasi ujian sesungguhnya.

Gbr. 3 Pengambilan data untuk pengujian sistem

B. Pengembangan Model Local Binary Pattern Histogram

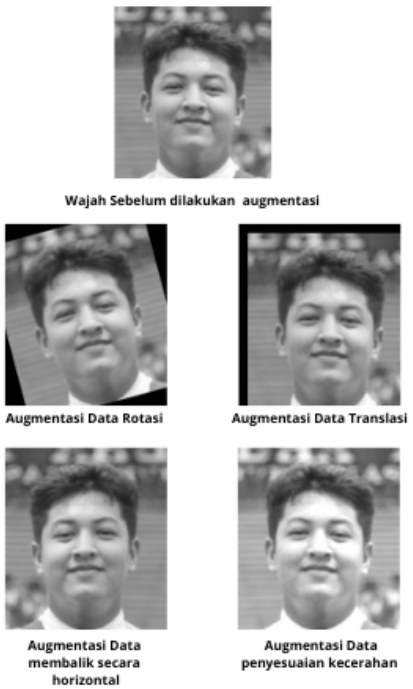
- Persiapan Dataset

Dataset wajah dihasilkan dari video yang diproses menjadi frame individu, mencakup berbagai ekspresi dan sudut pandang. Augmentasi data diterapkan untuk memperkaya variasi, meliputi:

- Rotasi: Memutar gambar 15 derajat.
- Flip Horizontal: Membalik gambar secara horizontal untuk menangkap simetri wajah.
- Penyesuaian Kecerahan: Menambah kecerahan 20%.
- Translasi: Menggeser gambar 10 piksel ke kanan dan ke bawah.

Gbr. 4 menunjukan wajah sebelum dan setelah dilakukan augmentasi data untuk memperkaya dataset sehingga model lebih tangguh terhadap variasi seperti pencahayaan dan orientasi.

Gbr. 4 wajah sebelum dan setelah dilakukan augmentasi



- Ekstraksi Fitur dengan Local Binary Pattern (LBP)

  Fitur diekstraksi dari gambar grayscale menggunakan Local Binary Pattern Histogram (LBPH). Setiap gambar diubah menjadi histogram LBP yang merepresentasikan pola tekstur unik dari wajah. Representasi ini kemudian digunakan untuk pelatihan model.
- Membuat Histogram

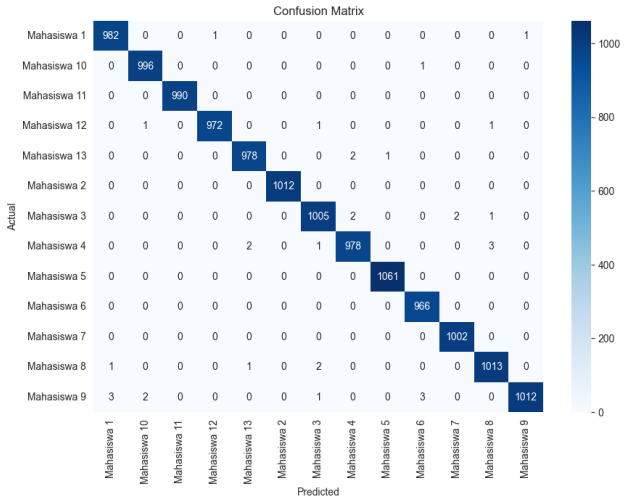
  Hasil ekstraksi LBP divisualisasikan sebagai grafik batang. Beberapa histogram sampel diambil secara acak untuk menunjukkan distribusi pola tekstur. Variasi histogram antar individu membantu model mengenali perbedaan tekstur wajah.
- Pelatihan Model LBPH dan Penyesuaian Parameter

  Model Neural Network digunakan untuk mengklasifikasikan histogram LBPH. Dataset dibagi menjadi data latih (80%) dan data uji (20%). Model terdiri dari beberapa lapisan tersembunyi dengan fungsi aktivasi ReLU dan dropout untuk mencegah overfitting. Proses pelatihan berlangsung selama 50 epoch dengan optimasi menggunakan Adam. Evaluasi dilakukan dengan data uji, menghasilkan akurasi tinggi, menunjukkan kemampuan model dalam mengenali pola-pola wajah.
- Evaluasi Kinerja

  Evaluasi dilakukan menggunakan metrik akurasi, presisi, recall, dan F1-score, dengan hasil akurasi keseluruhan sebesar 99% yang terlihat pada Gbr. 5. Confusion matrix digunakan untuk memvisualisasikan prediksi benar dan salah seperti pada Gbr. 6. Mayoritas prediksi berada di diagonal matriks, menandakan kinerja yang sangat baik. Kesalahan prediksi kecil menunjukkan bahwa model secara umum mampu mengklasifikasikan wajah dengan sangat baik dan dapat digunakan untuk aplikasi pengenalan wajah.

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| 0 | 0.99 | 1.00 | 0.99 | 984 |
| 1 | 1.00 | 1.00 | 1.00 | 997 |
| 2 | 0.99 | 0.99 | 0.99 | 990 |
| 3 | 0.99 | 0.99 | 0.99 | 975 |
| 4 | 0.99 | 1.00 | 0.99 | 981 |
| 5 | 1.00 | 0.99 | 0.99 | 1012 |
| 6 | 1.00 | 1.00 | 1.00 | 1010 |
| 7 | 1.00 | 0.98 | 0.99 | 984 |
| 8 | 0.98 | 0.99 | 0.99 | 1061 |
| 9 | 1.00 | 0.99 | 0.99 | 966 |
| 10 | 1.00 | 1.00 | 1.00 | 1002 |
| 11 | 0.99 | 1.00 | 0.99 | 1017 |
| 12 | 0.99 | 0.99 | 0.99 | 1021 |
| accuracy | | | 0.99 | 13000 |
| macro avg | 0.99 | 0.99 | 0.99 | 13000 |
| weighted avg | 0.99 | 0.99 | 0.99 | 13000 |

Gbr. 5. Hasil evaluasi model LBPH




Gbr. 6. Hasil confusion matrix

C. Pengembangan Skrip

1. Pengenalan Wajah

   Program pengenalan wajah dirancang untuk mengenali wajah dalam video menggunakan deep learning dan Mediapipe. Model Keras dan label dari LabelEncoder digunakan untuk prediksi identitas, sementara Mediapipe dan LBPH dari OpenCV mendeteksi serta menghasilkan histogram wajah. Setiap frame diproses untuk mencatat hasil ke file CSV, menyimpan tangkapan layar, dan menghitung waktu pemrosesan. Program juga mendukung pemrosesan batch untuk semua video dalam folder tertentu.
2. Perkiraan Arah Wajah Peserta

   Skrip ini mendeteksi wajah dan memperkirakan arah wajah dari video menggunakan Mediapipe. Face Detection dan Face Mesh digunakan untuk estimasi pose 3D dengan solvePnP, menentukan arah seperti kanan, kiri, atau bawah berdasarkan sudut rotasi. Jika perubahan arah berlangsung lebih dari 5 detik, segmen video disimpan. Skrip memproses seluruh video dalam folder untuk analisis arah wajah.
3. Deteksi dan Pelacakan Multi-Orang

   Fitur ini mendeteksi wajah dalam video dan mengambil tangkapan layar jika lebih dari satu wajah terdeteksi pada frame tertentu. Mediapipe digunakan untuk deteksi wajah, dan setiap frame yang memenuhi kriteria disimpan dengan nama yang disesuaikan. Direktori hasil dibuat secara otomatis, dan proses ini diterapkan untuk semua video dalam folder. Waktu pemrosesan dan jumlah pelanggaran dihitung secara keseluruhan.

D. Analisis Sistem

Analisis akurasi deteksi kecurangan dan kecepatan analisis sistem sangat penting untuk menjaga integritas dan efisiensi ujian. Sistem yang andal harus dapat mendeteksi berbagai bentuk kecurangan dengan akurat dan memproses data secara real-time, memungkinkan tindakan korektif segera. Berikut hasil evaluasi sistem terhadap fitur-fitur yang dikembangkan:

TABLE 1
KINERJA SISTEM PENGENALAN WAJAH DENGAN VIDEO PENGUJIAN

| Nama | Waktu pemrosesan | wajah keseluruhan | yang Sesuai dengan Peserta | dengan Peserta namun Terdeteksi Salah oleh Sistem | Wajah yang Tidak Sesuai dengan Peserta Sebenarnya | rasio deteksi wajah yang benar dari total yang diharapkan |
|---|---|---|---|---|---|---|
| Mahasiswa 1 | 26.83 Detik | 38 | 36 | 2 | 0 | 95% |
| Mahasiswa 2 | 45.12 Detik | 60 | 45 | 3 | 12 | 94% |
| Mahasiswa 3 | 74.20 Detik | 49 | 47 | 2 | 0 | 96% |
| Mahasiswa 4 | 42.61 Detik | 54 | 51 | 3 | 0 | 94% |
| Mahasiswa 5 | 47.26 Detik | 59 | 27 | 32 | 0 | 46% |
| Mahasiswa 6 | 39.61 Detik | 59 | 56 | 3 | 0 | 95% |
| Mahasiswa 7 | 42.99 Detik | 49 | 27 | 22 | 0 | 55% |
| Mahasiswa 8 | 45.17 Detik | 48 | 11 | 5 | 32 | 69% |
| Mahasiswa 9 | 43.59 Detik | 57 | 8 | 13 | 36 | 38% |
| Mahasiswa 10 | 41.73 Detik | 58 | 24 | 1 | 33 | 96% |
| Mahasiswa 11 | 41.07 Detik | 61 | 58 | 3 | 0 | 95% |
| Mahasiswa 12 | 42.77 Detik | 62 | 54 | 8 | 0 | 87% |
| Mahasiswa 13 | 43.71 Detik | 49 | 30 | 19 | 0 | 61% |
| Total | 576,66 Detik | 703 | 474 | 116 | 113 | 80% |

1. Pengenalan Wajah Peserta

Rumus perhitungan rasio akurasi wajah sebagai berikut:

$$Rasio\ akurasi\ wajah = \frac{Wsesuai}{Jumlah\ total - W\ tidak\ sesuai} \quad (1)$$

- $Wsesuai$ = jumlah wajah yang sesuai dengan peserta.
- $W\ tidak\ sesuai$ = jumlah wajah yang tidak sesuai dengan peserta sebenarnya.

Berdasarkan pengujian pada Table I terhadap 13 mahasiswa, waktu pemrosesan deteksi wajah bervariasi antara 26,83 hingga 74,20 detik, dengan total waktu 576,66 detik. Variasi ini dipengaruhi oleh jumlah wajah terdeteksi, kesalahan deteksi, dan kompleksitas analisis sistem.

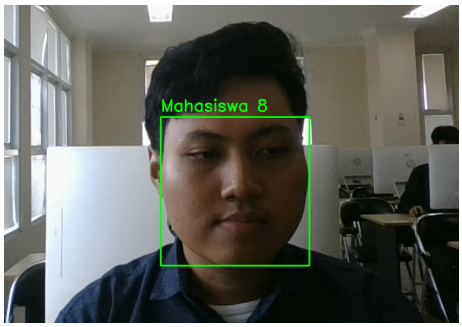
Mahasiswa dengan lebih banyak kesalahan atau jumlah wajah terdeteksi lebih tinggi cenderung membutuhkan waktu lebih lama. Contohnya, Mahasiswa 3 memiliki waktu pemrosesan tertinggi (74,20 detik) dengan 49 wajah terdeteksi dan akurasi 96%, sementara Mahasiswa 1 memiliki waktu terendah (26,83 detik) dengan 38 wajah terdeteksi dan akurasi 95%.

Akurasi deteksi bervariasi, dari 96% (Mahasiswa 3) hingga 38% (Mahasiswa 9). Mahasiswa dengan lebih banyak wajah sesuai umumnya memiliki akurasi lebih tinggi. Misalnya, Mahasiswa 6 mendeteksi 56 dari 59 wajah sesuai (akurasi 95%), sedangkan Mahasiswa 9 hanya 8 dari 57 wajah sesuai, dengan akurasi terendah 38%.

Beberapa faktor yang memengaruhi hasil deteksi wajah ini antara lain:

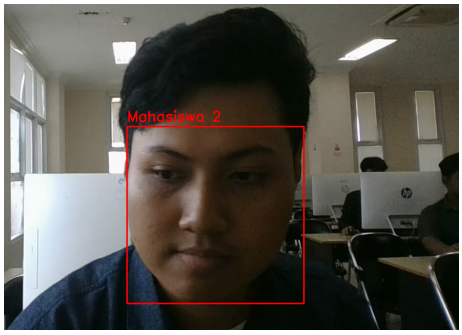
- Jumlah dan Kualitas Wajah yang Terlihat: Mahasiswa yang tampil di video dengan jelas dan konsisten cenderung memiliki akurasi deteksi yang lebih baik, sedangkan mahasiswa yang tampil dengan kondisi pencahayaan yang buruk atau posisi wajah yang tidak jelas mengalami lebih banyak kesalahan deteksi.
- Kesalahan Algoritma: Beberapa kesalahan terdeteksi berasal dari sistem yang salah mengklasifikasikan wajah yang sebenarnya sesuai dengan peserta, tetapi diidentifikasi secara tidak akurat.

Pada Gbr. 7, Gbr. 8, dan Gbr. 9. terdapat tiga kemungkinan hasil yang dapat diperoleh. Pertama pada Gbr. 7, hasil yang diharapkan benar, yaitu ketika sistem berhasil mengenali wajah peserta ujian dengan akurat dan sesuai dengan data identitas yang sudah terdaftar. Pada kondisi ini, wajah yang terekam sesuai dengan wajah peserta ujian sebenarnya, sehingga sistem dapat memberikan validasi bahwa peserta tersebut adalah orang yang berhak mengikuti ujian. Kedua pada Gbr. 8, hasil yang diharapkan benar dalam kondisi yang berbeda, di mana wajah yang terekam tidak sesuai dengan identitas peserta yang terdaftar. Pada kondisi ini, sistem berhasil mendeteksi bahwa wajah peserta tidak cocok dengan data yang ada, sehingga terjadi penolakan yang sesuai dengan kebijakan keamanan ujian. Hasil ini juga dianggap akurat karena sistem mampu mengenali ketidaksesuaian identitas dengan benar. Terakhir pada gambar Gbr. 9, ada kemungkinan hasil yang tidak diharapkan, yaitu ketika wajah peserta ujian sebenarnya sesuai dengan data yang ada, tetapi sistem mendeteksi wajah tersebut sebagai wajah yang tidak sesuai. Hal ini dapat terjadi karena adanya kesalahan dalam pengenalan wajah atau ketidaktepatan pada algoritma yang digunakan oleh sistem. Pada situasi ini, perlu dilakukan pengecekan ulang atau penyesuaian pada sistem agar tidak ada peserta yang sah mengalami kendala akibat hasil verifikasi yang keliru.




Gbr. 7 Hasil yang diharapkan (Kesesuaian wajah peserta ujian dengan data yang telah terdaftar dalam sistem).


Gbr. 8 Hasil yang diharapkan (Wajah peserta ujian tidak sesuai dengan data yang terdaftar di sistem, sehingga terindikasi adanya kecurangan).




Gbr. 9 Hasil yang tidak diharapkan (Wajah sesuai dengan peserta ujian tetapi terdeteksi sistem tidak sesuai dengan peserta ujian)

2. Perkiraan arah wajah peserta

Berdasarkan hasil pada Table II menunjukkan waktu pemrosesan deteksi pelanggaran pada 13 mahasiswa berkisar antara 138,45 hingga 335,01 detik, dipengaruhi oleh durasi video dan jumlah pelanggaran. Waktu terpanjang dialami Mahasiswa 9 dengan 335,01 detik dan 3 pelanggaran yang divalidasi 100 persen. Total 22 pelanggaran terdeteksi pada semua mahasiswa dengan akurasi validasi 100 persen. Mahasiswa 5 mencatat pelanggaran terbanyak sebanyak 6, diikuti Mahasiswa 7 dengan 5 pelanggaran.

Mahasiswa 3, 10, 11, dan 12 tidak memiliki pelanggaran yang disimpan atau divalidasi, menunjukkan bahwa selama video mereka, tidak ada pelanggaran yang terdeteksi oleh sistem. Akurasi deteksi pada tabel II, menunjukkan performa sistem yang sangat baik, dengan 100% akurasi pada semua mahasiswa yang memiliki pelanggaran. Ini berarti setiap pelanggaran yang terdeteksi oleh sistem berhasil divalidasi dengan tepat. Mahasiswa yang tidak memiliki pelanggaran tetap tercatat dengan akurasi 0%, yang menandakan bahwa tidak ada pelanggaran yang perlu divalidasi.

TABLE II

KINERJA SISTEM PERKIRAAN ARAH WAJAH PESERTA DENGAN VIDEO PENGUJIAN

| No | Nama | Waktu pemrosesan | Jumlah pelanggaran yang disimpan | Jumlah pelanggaran yang divalidasi | Akurasi |
|---|---|---|---|---|---|
| 1 | Mahasiswa 1 | 138,45 detik | 1 | 1 | 100% |
| 2 | Mahasiswa 2 | 217,91 detik | 1 | 1 | 100% |
| 3 | Mahasiswa 3 | 255,65 detik | 0 | 0 | 0% |
| 4 | Mahasiswa 4 | 209,41 detik | 1 | 1 | 100% |
| 5 | Mahasiswa 5 | 223,73 detik | 6 | 6 | 100% |
| 6 | Mahasiswa 6 | 210,25 detik | 1 | 1 | 100% |
| 7 | Mahasiswa 7 | 229,04 detik | 5 | 5 | 100% |
| 8 | Mahasiswa 8 | 257,04 detik | 2 | 2 | 100% |
| 9 | Mahasiswa 9 | 335,01 detik | 3 | 3 | 100% |
| 10 | Mahasiswa 10 | 290,60 detik | 0 | 0 | 0% |
| 11 | Mahasiswa 11 | 210,21 detik | 0 | 0 | 0% |
| 12 | Mahasiswa 12 | 208,43 detik | 0 | 0 | 0% |
| 13 | Mahasiswa 13 | 223,95 detik | 2 | 2 | 100% |
| | Total | 3009,68 detik | 22 | 22 | 100% |

3. Deteksi Pelacakan Multi orang

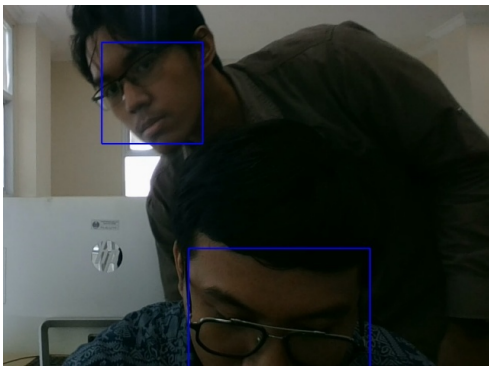
Dari data Table III menunjukkan hasil pengujian sistem pengawas ujian berbasis kecerdasan buatan pada 13 peserta dengan parameter waktu pemrosesan, jumlah pelanggaran yang terdeteksi, jumlah pelanggaran yang divalidasi, serta akurasi. Waktu pemrosesan bervariasi antara 39,59 detik hingga 82,26 detik, dengan total waktu keseluruhan 827,34 detik untuk seluruh peserta. Jumlah pelanggaran yang terdeteksi berkisar dari 0 hingga 495, dengan total 1133 pelanggaran yang disimpan oleh sistem. Dari jumlah tersebut, 1091 pelanggaran berhasil divalidasi, menghasilkan akurasi keseluruhan sebesar 96%. Beberapa peserta mencapai akurasi

sempurna (100%), sementara ada yang lebih rendah, seperti Mahasiswa 8 dengan akurasi 24%. Hasil ini menunjukkan bahwa sistem berfungsi dengan tingkat keandalan yang tinggi, meskipun terdapat variasi pada waktu pemrosesan dan akurasi validasi pelanggaran di beberapa kasus. Hal ini menunjukkan perlunya penyesuaian lebih lanjut untuk meningkatkan kinerja sistem pada kondisi tertentu.

TABLE III

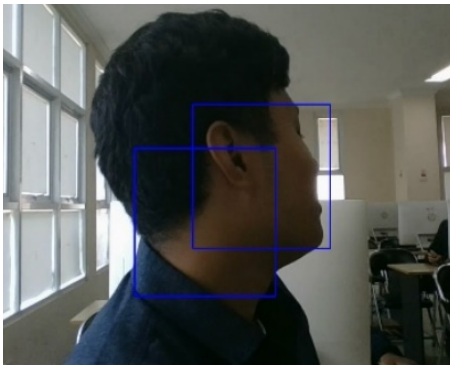
KINERJA SISTEM PERKIRAAN ARAH WAJAH PESERTA DENGAN VIDEO PENGUJIAN

| No | Nama | Waktu pemrosesan | Jumlah pelanggaran yang disimpan | Jumlah pelanggaran yang divalidasi | Akurasi |
|---|---|---|---|---|---|
| 1 | Mahasiswa 1 | 39,59 detik | 7 | 4 | 57% |
| 2 | Mahasiswa 2 | 59,80 detik | 1 | 1 | 100% |
| 3 | Mahasiswa 3 | 82,26 detik | 24 | 15 | 63% |
| 4 | Mahasiswa 4 | 63,19 detik | 59 | 52 | 88% |
| 5 | Mahasiswa 5 | 64,09 detik | 221 | 221 | 100% |
| 6 | Mahasiswa 6 | 59,06 detik | 31 | 31 | 100% |
| 7 | Mahasiswa 7 | 67,21 detik | 163 | 153 | 94% |
| 8 | Mahasiswa 8 | 62,99 detik | 17 | 4 | 24% |
| 9 | Mahasiswa 9 | 76,10 detik | 495 | 495 | 100% |
| 10 | Mahasiswa 10 | 64,94 detik | 105 | 105 | 100% |
| 11 | Mahasiswa 11 | 62.00 detik | 1 | 1 | 100% |
| 12 | Mahasiswa 12 | 63,34 detik | 0 | 0 | 0% |
| 13 | Mahasiswa 13 | 62,77 detik | 9 | 9 | 100% |
| | Total | 827,34 detik | 1133 | 1091 | 96% |



Gbr. 10 Hasil pendeteksian sesuai dengan yang diharapkan, karena berhasil mendeteksi keberadaan lebih dari dua orang.

Berdasarkan Gbr. 10 menunjukkan contoh keberhasilan dalam deteksi dan pelacakan multi-orang. Terlihat bahwa kotak-kotak deteksi (bounding boxes) berada pada area yang tepat, seperti pada wajah masing-masing individu. Sistem deteksi berhasil mengenali wajah dengan akurat, menempatkan kotak deteksi pada posisi yang sesuai tanpa ada kesalahan di area lain, seperti telinga atau bagian tubuh lainnya. Meskipun orang di dalam gambar tampak dari sudut pandang yang tidak sepenuhnya frontal, sistem deteksi mampu mengenali wajah dengan baik. Hasil ini menunjukkan bahwa model deteksi yang digunakan cukup andal dalam mengenali wajah meskipun dalam kondisi sudut pandang dan pencahayaan yang beragam.



Gbr. 11 Menunjukkan hasil pendeteksian yang tidak sesuai dengan yang diharapkan, di mana sistem mendeteksi dua orang, sementara seharusnya hanya terdeteksi satu orang.

Sebaliknya, Gbr. 11 menunjukkan kesalahan dalam deteksi multi-orang, di mana kotak deteksi ditempatkan di bagian tubuh yang salah, seperti telinga, dan tidak mencakup wajah dengan baik, yang mungkin disebabkan oleh kesulitan mengenali wajah dari sudut samping atau gangguan pencahayaan.

## IV. KESIMPULAN

Kesimpulan dari penelitian Pengembangan Model Pengawas Berbasis Kecerdasan Buatan untuk Ujian Online sebagai berikut :

1. Penelitian ini menunjukkan bahwa algoritma LBPH yang sederhana dan efisien efektif dalam skenario ujian online dengan kondisi terkontrol. Namun, untuk mengatasi variasi pencahayaan, ekspresi wajah, dan pose ekstrem, diperlukan kombinasi teknologi Mediapipe dan Neural Network. Sistem ini mampu mendeteksi pelanggaran arah wajah dengan akurasi validasi hingga 100%, pelacakan multi-orang dengan akurasi 96%, dan pengenalan wajah peserta dengan akurasi 80%.
2. Hasil penelitian membuktikan bahwa sistem berbasis kecerdasan buatan ini mampu mencatat pelanggaran dengan validasi akurasi tinggi, meskipun terdapat tantangan seperti waktu pemrosesan yang bervariasi dan

kesalahan deteksi pada kondisi tertentu. Sistem ini memungkinkan pengawasan otomatis yang dapat mendukung pengawas manual dalam analisis kasus tertentu, meningkatkan efisiensi pengawasan secara keseluruhan.

Kombinasi teknologi yang digunakan menghasilkan sistem pengawasan yang akurat, efisien, dan adaptif. Dengan augmentasi data dan pelatihan yang baik, sistem ini mampu mengenali wajah dan memantau perilaku peserta ujian secara real-time. Selain pengawasan ujian, sistem ini memiliki potensi besar untuk aplikasi di bidang keamanan dan analisis perilaku.Penelitian ini menjadi langkah awal dalam pengembangan sistem pengawasan berbasis AI yang canggih dan andal untuk berbagai kebutuhan di masa depan.

## UCAPAN TERIMA KASIH

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT, atas limpahan rahmat dan karunia-Nya sehingga penelitian ini dapat diselesaikan dengan baik. Penulis juga menyampaikan terima kasih yang sebesar-besarnya kepada kedua orang tua atas doa dan dukungan yang tiada henti. Ucapan terima kasih yang mendalam juga penulis sampaikan kepada dosen pembimbing atas bimbingan dan arahan terbaiknya selama proses penelitian ini. Tak lupa, terima kasih kepada teman-teman yang telah memberikan bantuan dan dukungan sehingga penelitian ini dapat terselesaikan dengan baik.

## REFERENSI

[1] M. R. Hameed and Firas. A. Abdullatif, “Online Examination System,” *IARJSET*, vol. 4, no. 3, pp. 106–110, Mar. 2017, doi: 10.17148/IARJSET.2017.4321.

[2] B. H. Asker and A. F. Al-Allaf, “Detecting cheating in electronic exams using the artificial intelligence approach,” *International Journal of Mechanical Engineering*, vol. 7, no. 2, 2022.

[3] G. Di Franco and M. Santurro, “Machine learning, artificial neural networks and social research,” *Qual Quant*, vol. 55, no. 3, pp. 1007–1025, Jun. 2021, doi: 10.1007/s11135-020-01037-y.

[4] A. Singh and S. Das, “A Cheating Detection System in Online Examinations Based on the Analysis of Eye-Gaze and Head-Pose,” European Alliance for Innovation n.o., Jun. 2022. doi: 10.4108/eai.16-4-2022.2318165.

[5] K. Gopalakrishnan, N. Dhiyaneshwaran, and P. Yugesh, “Online proctoring system using image processing and machine learning,” *Int J Health Sci (Qassim)*, Jun. 2022, doi: 10.53730/ijhs.v6ns5.8777.

[6] Chirag, “Overview of Neural Network,” *International Journal of Advanced Research in Science, Communication and Technology*, pp. 531–534, Jun. 2022, doi: 10.48175/ijarsct-4851.

[7] K. P. Kamble and V. R. Ghorpade, “Video Interpretation for Cost-Effective Remote Proctoring to Prevent Cheating,” in *Lecture Notes in Networks and Systems*, Springer Science and Business Media Deutschland GmbH, 2021, pp. 259–269. doi: 10.1007/978-981-33-4073-2_25.

[8] E. Llapashtica, “Eye Movements & the Integrated Saccade Latency Test,” 2019.

[9] V. Khanna, S. Brodiya, and D. Chaudhary, “ARTIFICIAL INTELLIGENCE BASED AUTOMATED EXAM PROCTORING SYSTEM,” *International Research Journal of Engineering and Technology*, 2021, [Online]. Available: www.irjet.net

[10] A. Tweissi, W. Al Etaiwi, and A. Eisawi, “The Accuracy of AI-Based Automatic Proctoring in Online Exams,” 2022. [Online]. Available: www.ejel.org

[11] S. Satre, S. Patil, T. Mane, V. Molawade, T. Gawand, and A. Mishra, “Online Exam Proctoring System Based on Artificial Intelligence,” in *Proceedings of 2023 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication, IConSCEPT 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/IConSCEPT57958.2023.10170577.

[12] R. Moyo, S. Ndebvu, M. Zimba, and J. Mbelwa, “A Video-based Detector for Suspicious Activity in Examination with OpenPose,” Jul. 2023, [Online]. Available: http://arxiv.org/abs/2307.11413

[13] M. A. Sulaiman, “DEVELOPMENT OF AN ELECTRONIC EXAMINATION PLATFORM USING FACE RECOGNITION METHODS,” *Science Journal of University of Zakho*, vol. 12, no. 3, pp. 308–315, Jul. 2024, doi: 10.25271/sjuoz.2024.12.3.1289.

.