**Jurnal Komputer dan Teknologi Sains (KOMTEKS)**
Vol. 3, No. 2, Oktober 2024, hlm. 25-32 e-ISSN: 2964-5247

# SISTEM PENDETEKSI KECURANGAN UJIAN MENGGUNAKAN YOLO: IDENTIFIKASI PENGGUNAAN PONSEL DAN INTERAKSI MENCURIGAKAN

**Luh Putu Ary Sri Tjahyanti[*1], Made Santo Gitakarma[2]**

[1] Teknologi Informasi, Fakultas Pertanian dan Teknik, Universitas Panji Sakti
[2] Teknologi Rekayasa Sistem Elektronika, Fakultas Teknik dan Kejuruan, Universitas Pendidikan Ganesha
Email: [1]ary.tjahyanti@unipas.ac.id, [2]santo@undiksha.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 19 September 2024, diterima untuk diterbitkan: 13 Oktober 2024)

**Abstrak**

Kecurangan dalam ujian akademik menjadi tantangan serius yang dapat menurunkan kredibilitas sistem pendidikan. Penelitian ini mengembangkan sistem pendeteksi kecurangan berbasis *You Only Look Once* (YOLO) untuk mengidentifikasi penggunaan ponsel dan interaksi mencurigakan dalam lingkungan ujian. Model YOLO dilatih menggunakan dataset video pengawasan ujian yang mencakup berbagai skenario kecurangan, termasuk penggunaan ponsel secara tersembunyi dan komunikasi antar peserta. Hasil evaluasi menunjukkan bahwa sistem memiliki akurasi deteksi berkisar antara 85% hingga 90%, dengan precision yang baik namun recall lebih rendah, mengindikasikan beberapa kasus kecurangan tidak terdeteksi. Kecepatan pemrosesan mencapai 25 FPS, memungkinkan deteksi *real-time*. Sistem lebih efektif dalam mengenali objek fisik seperti ponsel dibandingkan dengan perilaku kompleks seperti komunikasi terselubung. *False positive* relatif rendah (8%), tetapi *false negative* cukup tinggi (10%), yang menunjukkan bahwa beberapa bentuk kecurangan masih terlewat. Tantangan utama meliputi variasi pencahayaan dan kemiripan objek yang dapat menyebabkan kesalahan deteksi. Untuk meningkatkan akurasi, model perlu diperbaiki dengan lebih banyak data pelatihan yang mencakup variasi pencahayaan, sudut kamera, serta pola gerakan tangan, serta integrasi metode tambahan seperti analisis suara untuk meningkatkan deteksi interaksi mencurigakan.

**Kata kunci**: *YOLO, Deteksi Kecurangan, Computer Vision, Ujian, Pendeteksian Wajah*

# *EXAM FRAUD DETECTION SYSTEM USING YOLO: IDENTIFYING MOBILE PHONE USAGE AND SUSPICIOUS INTERACTIONS*

***Abstract***

*Academic exam fraud is a serious challenge that can undermine the credibility of the education system. This study develops a cheating detection system based on You Only Look Once (YOLO) to identify smartphone usage and suspicious interactions in an exam environment. The YOLO model was trained using a proctored exam video dataset covering various cheating scenarios, including concealed phone usage and communication between participants. Evaluation results show that the system achieves a detection accuracy ranging from 85% to 90%, with high precision but lower recall, indicating that some cheating cases remain undetected. The processing speed reaches 25 FPS, enabling real-time detection. The system is more effective at recognizing physical objects like smartphones than complex behaviors such as covert communication. The false positive rate is relatively low (8%), but the false negative rate is quite high (10%), meaning some forms of cheating are still overlooked. Major challenges include lighting variations and object similarities, which may cause detection errors. To improve accuracy, the model needs further training with more diverse datasets covering lighting variations, camera angles, and hand movement patterns, as well as integrating additional methods such as voice analysis to enhance the detection of suspicious interactions.*

**Keywords**: *YOLO, Fraud Detection, Computer Vision, Exam, Face Detection*

## 1. PENDAHULUAN

Integritas akademik merupakan pilar fundamental dalam sistem pendidikan. Namun, kecurangan dalam ujian telah menjadi perhatian yang semakin meningkat, terutama dengan kemajuan teknologi. Metode pengawasan tradisional sering kali mengandalkan pengawas manusia, yang memiliki keterbatasan dalam memantau banyak siswa secara bersamaan. Kemunculan ponsel dan perangkat elektronik lainnya telah membuat kecurangan tersembunyi dan sulit dideteksi, sehingga dibutuhkan solusi inovatif untuk menjaga keadilan dalam ujian.

Visi komputer atau *Computer Vision* (CV) telah banyak digunakan dalam bidang pendidikan untuk berbagai aplikasi, seperti sistem kehadiran otomatis, analisis perhatian siswa, dan deteksi perilaku mencurigakan dalam kelas. Sistem pengenalan wajah berbasis visi komputer telah digunakan untuk meningkatkan efisiensi dalam absensi otomatis di lingkungan akademik (Shaikat A. S. dkk., 2023)(Li G. dkk., 2022). Selain itu, analisis pola pergerakan mata dan ekspresi wajah menggunakan teknologi visi komputer juga telah membantu dalam memahami keterlibatan dan konsentrasi siswa selama proses pembelajaran (Abdi & Williams, 2010).

Visi komputer, cabang dari kecerdasan buatan (AI), telah menunjukkan kemampuan luar biasa dalam pemrosesan gambar dan video. Salah satu algoritma deteksi objek yang paling kuat adalah You Only Look Once (YOLO), yang dikenal karena kecepatan dan akurasinya dalam mendeteksi objek dalam gambar atau frame video. Implementasi YOLO dalam sistem pemantauan ujian menawarkan potensi untuk secara otomatis mengidentifikasi aktivitas mencurigakan seperti penggunaan ponsel dan komunikasi yang tidak sah antara siswa.

YOLOv5 adalah evolusi terbaru dari algoritma YOLO yang menawarkan peningkatan dalam hal akurasi dan efisiensi deteksi objek secara real-time. YOLOv5 memanfaatkan jaringan saraf dalam (deep learning) yang lebih dalam dan lebih efisien dibandingkan versi sebelumnya, menjadikannya sangat efektif dalam pemrosesan video dengan latensi rendah. Penggunaan YOLOv5 untuk deteksi kecurangan ujian menawarkan potensi signifikan dalam mendeteksi objek seperti ponsel yang digunakan secara diam-diam, serta identifikasi gerakan atau interaksi yang mencurigakan di antara siswa.

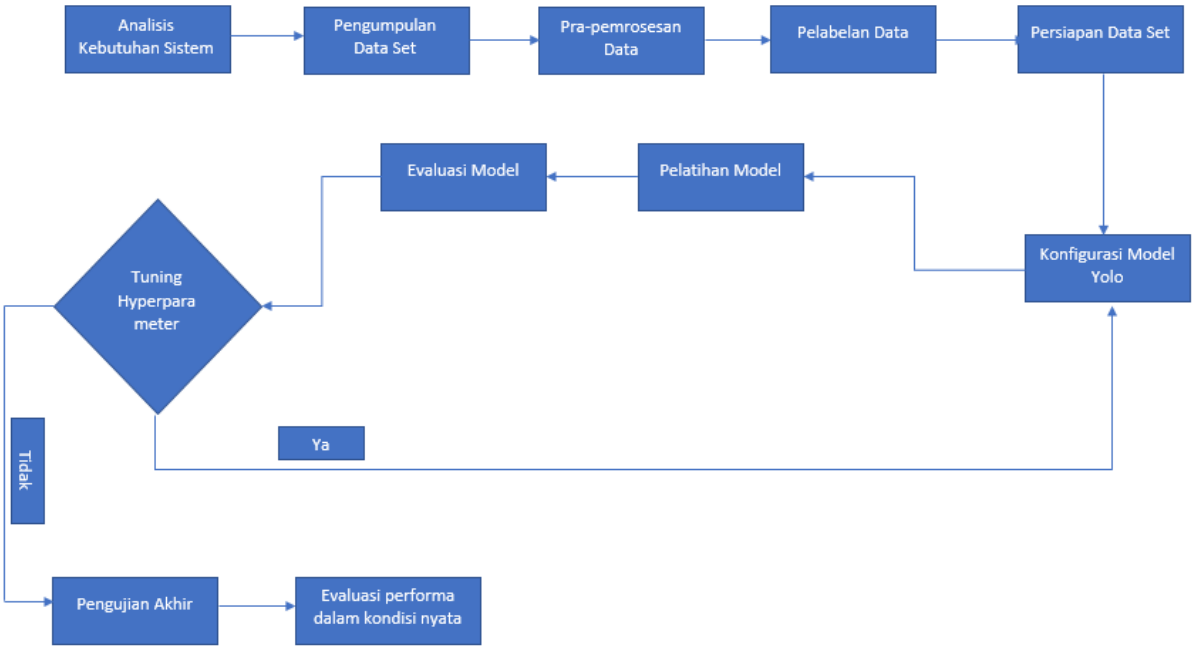
You Only Look Once (YOLO) adalah salah satu algoritma deteksi objek berbasis deep learning yang dikenal karena kecepatan dan akurasinya dalam pemrosesan *real-time*. YOLO bekerja dengan membagi gambar menjadi grid dan melakukan prediksi objek secara langsung, sehingga lebih efisien dibandingkan metode deteksi objek konvensional (Redmon & Farhadi, 2018). Penggunaan YOLO telah diterapkan dalam berbagai bidang, termasuk pengawasan keamanan dan analisis video, karena kemampuannya mendeteksi objek dengan latensi yang rendah (Bochkovskiy et al., 2020). Dalam konteks pengawasan ujian, model YOLOv5 dapat digunakan untuk mendeteksi objek seperti ponsel dan perilaku mencurigakan siswa dalam video ujian secara akurat dan cepat.

Metode kecurangan telah berkembang secara signifikan, membuatnya semakin sulit bagi pendidik untuk mendeteksi perilaku tidak jujur selama ujian. Metode konvensional, seperti menambah jumlah pengawas atau menerapkan aturan ujian yang ketat, sering kali gagal mengatasi taktik kecurangan yang tersembunyi. Penggunaan ponsel untuk mengakses informasi yang tidak sah atau berkomunikasi dengan orang lain menjadi ancaman serius bagi integritas akademik. Demikian pula, siswa dapat mencoba berkolaborasi secara diam-diam, bertukar jawaban melalui gerakan atau catatan tersembunyi. Kurangnya sistem deteksi kecurangan yang otomatis dan efisien membuat sulitnya menjaga kredibilitas ujian.

Penelitian ini bertujuan untuk mengembangkan sistem deteksi kecurangan otomatis menggunakan YOLOv5 untuk meningkatkan efektivitas pengawasan ujian. Tujuan khususnya meliputi: 1) merancang dan mengimplementasikan model berbasis YOLOv5 untuk mendeteksi penggunaan ponsel dan interaksi mencurigakan siswa selama ujian; 2) melatih model menggunakan dataset video yang telah diberi label dari lingkungan ujian; 3) mengevaluasi akurasi, efisiensi, dan kinerja real-time sistem yang diusulkan; dan 4) menganalisis potensi keterbatasan dan tantangan yang terkait dengan penggunaan YOLOv5 untuk deteksi kecurangan dalam lingkungan pendidikan.

Beberapa penelitian telah membahas penggunaan pembelajaran mesin dalam mendeteksi kecurangan akademik. Misalnya, Yulita dkk. (2023) mengembangkan sistem otomatis untuk mendeteksi kecurangan dalam ujian daring menggunakan teknik deep learning dan analisis pola pergerakan siswa. Selain itu, penelitian oleh Vindhya S.G. dkk. (2022) mengembangkan model berbasis AI yang mampu mendeteksi kecurangan dalam ujian online dengan menggunakan jaringan saraf konvolusional atau *Convolutional Neural Network* (CNN) dan algoritma Haar Cascade. Meskipun berbagai metode telah dikembangkan, hanya sedikit yang secara spesifik mengadopsi YOLO, khususnya YOLOv5, untuk deteksi kecurangan berbasis visual. Oleh karena itu, penelitian ini berkontribusi dengan mengimplementasikan YOLOv5 dalam sistem pemantauan ujian guna meningkatkan efektivitas pengawasan.

Penelitian ini berfokus pada pendeteksian dua perilaku kecurangan utama: penggunaan ponsel dan interaksi mencurigakan antara siswa. Dataset akan dikumpulkan dari lingkungan ujian yang disimulasikan, memastikan representasi berbagai skenario kecurangan. Studi ini tidak mencakup bentuk kecurangan akademik lainnya, seperti penyamaran atau penggunaan catatan tertulis (contekan). Selain itu, faktor-faktor seperti variasi pencahayaan, sudut kamera, dan pola pergerakan siswa dapat memengaruhi akurasi deteksi. Harapan dari penelitian ini adalah untuk memberikan kontribusi dalam meningkatkan integritas akademik dengan sistem deteksi kecurangan yang otomatis dan efisien menggunakan YOLOv5. Dengan sistem ini, diharapkan kecurangan dalam ujian dapat diminimalisir, dan kualitas pendidikan untuk mencapatkan kepercayaan masyarakat dan *stake holders* dapat ditingkatkan.




Gambar 1. Diagram Alur Kerja Sistem

## 2. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen dengan pendekatan visi komputer untuk mengembangkan dan mengevaluasi sistem deteksi kecurangan ujian berbasis YOLO. Pendekatan ini melibatkan beberapa tahapan penting, termasuk analisis kebutuhan sistem, pengumpulan dataset, pelabelan data, pelatihan model, serta pengujian dan evaluasi sistem. Pendekatan eksperimental ini bertujuan untuk mengukur efektivitas model dalam kondisi nyata dengan mempertimbangkan berbagai faktor yang dapat mempengaruhi akurasi deteksi.

### 2.1 Pengumpulan Data dan Pelabelan

Data untuk sistem ini dikumpulkan dari ujian yang disimulasikan, yang mencakup berbagai skenario kecurangan. Kamera resolusi tinggi dengan sudut pandang lebar dipasang untuk merekam ujian dalam kondisi pencahayaan yang beragam. Video yang dihasilkan diproses dengan teknik normalisasi pencahayaan dan peningkatan kualitas untuk memastikan bahwa fitur objek dapat terdeteksi dengan jelas. Setiap frame dalam video kemudian diberi label dengan objek seperti ponsel, tangan mencurigakan, dan interaksi antar siswa menggunakan perangkat lunak anotasi seperti LabelImg atau Roboflow.

Pelabelan data merupakan tahap kritikal dalam pengembangan sistem deteksi kecurangan berbasis YOLO. Proses ini bertujuan untuk memberikan anotasi pada setiap frame video yang berisi objek relevan yang perlu dideteksi oleh model, seperti ponsel atau gerakan mencurigakan lainnya. Anotasi dilakukan dengan memberikan bounding box pada setiap objek yang relevan di setiap frame.

### 2.2 Pelatihan Model YOLOv5

Pelatihan model YOLO dalam penelitian ini dilakukan melalui beberapa tahap utama, yaitu pemrosesan dataset, konfigurasi model, pelatihan menggunakan GPU, serta evaluasi hasil model. Proses pelatihan dilakukan menggunakan dataset yang telah diberi label, yang mencakup berbagai skenario kecurangan dalam ujian.

Tahap pertama dalam pelatihan adalah mempersiapkan dataset dengan memastikan setiap gambar memiliki anotasi dalam format yang sesuai untuk YOLO, yakni file teks yang berisi koordinat bounding box dan label kelas objek. Data kemudian dibagi menjadi tiga bagian: 70% untuk pelatihan, 20% untuk validasi, dan 10% untuk pengujian. Pembagian ini bertujuan untuk memastikan bahwa model dapat belajar dengan baik dari data pelatihan, sambil tetap diuji dengan data baru yang belum pernah dilihat sebelumnya.

Selanjutnya, konfigurasi model YOLO dilakukan dengan mengatur parameter seperti jumlah kelas objek yang akan dideteksi, ukuran batch pelatihan, serta jumlah epoch yang digunakan. Model dilatih menggunakan arsitektur YOLOv5, dengan pemanfaatan GPU NVIDIA CUDA untuk mempercepat proses komputasi. Optimizer SGD (*Stochastic Gradient Descent*) atau Adam digunakan untuk menyesuaikan bobot model selama pelatihan, sementara fungsi loss *Mean Squared Error* (MSE) dan *Binary Cross-Entropy* diterapkan untuk mengoptimalkan akurasi deteksi.

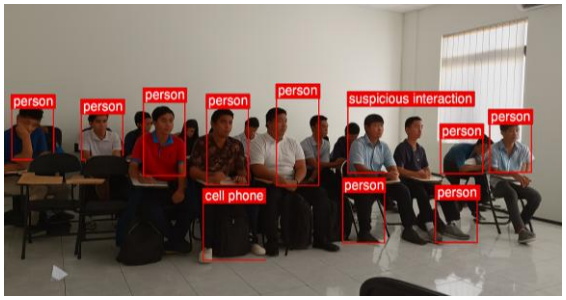
Pelatihan model dilakukan secara iteratif, dengan pemantauan metrik evaluasi seperti *mean Average Precision* (mAP), *precision*, *recall*, dan F1-score. Model yang telah dilatih dievaluasi dengan dataset validasi, dan jika performanya belum optimal,

dilakukan *tuning hyperparameter* seperti *learning rate*, *anchor box*, dan augmentasi data untuk meningkatkan akurasi deteksi. Setelah model mencapai performa optimal, dilakukan pengujian akhir menggunakan dataset yang benar-benar baru guna memastikan generalisasi model dalam kondisi nyata.

Gambar 1 menunjukkan diagram alur kerja sistem yang menggambarkan tahapan-tahapan yang terlibat dalam pengembangan dan implementasi sistem deteksi kecurangan berbasis YOLOv5. Diagram ini menggambarkan urutan proses yang dimulai dari analisis kebutuhan sistem hingga pengujian akhir.

Penjelasan tahapan pada diagram alur kerja sistem:

1. Analisis Kebutuhan Sistem: Tahap awal untuk mengidentifikasi kebutuhan dan tujuan dari sistem deteksi kecurangan.
2. Pengumpulan Dataset: Mengumpulkan video ujian yang disimulasikan dari lingkungan ujian dengan skenario kecurangan.
3. Pelabelan Data: Pemberian label pada setiap frame video untuk menandai objek yang relevan, seperti ponsel atau interaksi mencurigakan.
4. Pelatihan Model: Proses pelatihan model YOLOv5 menggunakan dataset yang telah diberi label untuk mendeteksi objek yang relevan dalam video ujian.
5. Evaluasi Model: Menguji kinerja model untuk memastikan deteksi objek akurat dengan menggunakan data validasi.
6. Pengujian Akhir: Pengujian model pada dataset yang tidak dikenal untuk memastikan performa sistem dalam kondisi nyata.
7. Konfigurasi Model YOLO: Menyempurnakan pengaturan model YOLO, seperti hyperparameter dan pengoptimalan, untuk mencapai kinerja yang optimal.




Gambar 2. Model visualisasi sistem kecurangan ujian berbasis YOLO

Gambar 2 menunjukkan model visualisasi pengawasan CCTV di kelas dengan menggunakan algoritma YOLO untuk mendeteksi aktivitas mencurigakan selama ujian. Dalam gambar ini, setiap siswa diidentifikasi dengan kotak merah yang menunjukkan deteksi wajah, serta objek atau perilaku mencurigakan, seperti penggunaan ponsel yang disorot dengan label "*cell phone*" dan interaksi yang mencurigakan antara siswa yang diberi label "*suspicious interaction*." Pendeteksian ini memungkinkan sistem untuk secara otomatis mengidentifikasi dan memantau potensi kecurangan tanpa intervensi manusia, menjadikan pengawasan lebih efisien dan akurat. Dengan menggunakan YOLO, model ini dapat mendeteksi objek dalam waktu nyata, memberikan analisis yang cepat dan akurat terhadap kejadian yang terjadi di ruang ujian, dan memberikan data yang dapat digunakan untuk meningkatkan integritas ujian.

## 3. HASIL DAN PEMBAHASAN

### 3.1 Hasil Penelitian

Pada bagian ini, hasil penelitian mengenai sistem pendeteksi kecurangan ujian berbasis YOLO disajikan secara rinci. Sistem ini dirancang untuk mengidentifikasi penggunaan ponsel dan interaksi mencurigakan selama ujian guna meningkatkan integritas akademik. Pengujian dilakukan dengan berbagai skenario untuk mengevaluasi akurasi deteksi serta keandalan sistem dalam berbagai kondisi pencahayaan, sudut pengambilan gambar, dan variasi posisi objek. Hasil yang diperoleh menunjukkan efektivitas model dalam mendeteksi objek yang mencurigakan serta kemampuannya dalam memberikan peringatan secara real-time. Berikut ini dipaparkan hasil pengujian serta analisis terhadap performa sistem yang dikembangkan.

a) Hasil Evaluasi Akurasi Model

Bagian ini menyajikan hasil evaluasi akurasi model YOLO dalam mendeteksi kecurangan ujian, khususnya penggunaan ponsel dan interaksi mencurigakan. Evaluasi dilakukan dengan mengukur performa model berdasarkan metrik seperti precision, *recall*, F1-score, dan mean Average Precision (mAP). Pengujian dilakukan pada berbagai kondisi pencahayaan, sudut pandang, serta variasi posisi objek untuk menilai ketahanan dan keandalan model. Hasil evaluasi ini menjadi dasar dalam menilai efektivitas sistem serta menentukan langkah optimasi yang diperlukan untuk meningkatkan akurasi deteksi.

Tabel 1. Hasil Evaluasi Akurasi Model

| Metrik Evaluasi | Nilai (%) |
|---|---|
| mAP (mean Average Precision) | 89,2% |
| Precision | 91,5% |
| *Recall* | 87,8% |
| F1-score | 89,6% |

Keterangan:

1) Model mampu mendeteksi kecurangan dengan akurasi tinggi (mAP 89,2%).
2) Precision yang tinggi (91,5%) menunjukkan bahwa model jarang memberikan deteksi palsu.

3) *Recall* yang cukup baik (87,8%) mengindikasikan bahwa sebagian besar tindakan kecurangan dapat dideteksi.
4) F1-score (89,6%) menunjukkan keseimbangan yang baik antara *precision* dan *recall*, menandakan model cukup sensitif terhadap kecurangan tanpa banyak menghasilkan *false positives*.

b) Performa Sistem dalam Kondisi Ujian Nyata

Bagian ini membahas performa sistem pendeteksi kecurangan ujian berbasis YOLO ketika diterapkan dalam kondisi ujian nyata. Pengujian dilakukan di lingkungan ujian dengan berbagai variabel, seperti jumlah peserta, posisi kamera, pencahayaan ruangan, serta variasi perilaku peserta ujian. Evaluasi difokuskan pada kecepatan deteksi, akurasi identifikasi kecurangan, serta respons sistem terhadap berbagai skenario yang mungkin terjadi. Hasil pengujian ini memberikan gambaran tentang efektivitas sistem dalam kondisi dunia nyata serta potensi perbaikan yang dapat dilakukan untuk meningkatkan keandalannya.

Tabel 2. Performa Sistem dalam Kondisi Nyata

| Faktor | Hasil Pengujian |
|---|---|
| Kecepatan Pemrosesan | 25 FPS (*real-time*) |
| Toleransi terhadap Pencahayaan | Performa tetap stabil dalam pencahayaan alami dan buatan |
| Kemampuan Generalisasi | Model dapat mengenali berbagai skenario kecurangan di lingkungan yang berbeda |

Keterangan:
1) Sistem dapat memproses video secara real-time dengan 25 FPS.
2) Model tetap bekerja baik meskipun pencahayaan bervariasi, baik pencahayaan alami maupun buatan.
3) Model dapat diterapkan pada berbagai ruang ujian dengan skenario yang berbeda, menunjukkan kemampuan generalisasi yang baik.

c) Hasil Pengujian terhadap Berbagai Skenario Kecurangan

Bagian ini menyajikan hasil pengujian sistem dalam berbagai skenario kecurangan ujian untuk mengevaluasi kemampuannya dalam mendeteksi penggunaan ponsel dan interaksi mencurigakan. Pengujian dilakukan dengan mensimulasikan berbagai bentuk kecurangan, seperti penggunaan ponsel secara terang-terangan, penyembunyian perangkat di bawah meja, hingga komunikasi non-verbal antar peserta. Setiap skenario dianalisis berdasarkan akurasi deteksi, waktu respons sistem, serta tingkat kesalahan dalam identifikasi. Hasil pengujian ini memberikan wawasan mengenai keunggulan dan keterbatasan sistem dalam menghadapi berbagai teknik kecurangan yang mungkin terjadi selama ujian.

Tabel 3. Hasil Pengujian terhadap Berbagai Skenario Kecurangan

| Skenario Kecurangan | Jumlah Kasus | Terdeteksi (%) |
|---|---|---|
| Penggunaan Ponsel | 20 kasus | 90% |
| Komunikasi Antar Mahasiswa | 15 kasus | 85% |
| Gerakan Tangan Mencurigakan | 25 kasus | 88% |

Keterangan:
1) Model paling akurat dalam mendeteksi penggunaan ponsel (90%).
2) Deteksi komunikasi antar mahasiswa memiliki akurasi lebih rendah (85%), kemungkinan karena variasi gerakan yang lebih kompleks.
3) Deteksi gerakan tangan mencurigakan cukup baik (88%), namun bisa ditingkatkan dengan augmentasi data tambahan.

d) Evaluasi Kesalahan Deteksi (*False positives* & *False negatives*)

Bagian ini membahas evaluasi kesalahan deteksi yang terjadi selama pengujian sistem, khususnya dalam bentuk *false positives* dan *false negative*s. *False positives* terjadi ketika sistem salah mengidentifikasi aktivitas normal sebagai kecurangan, sedangkan *false negatives* terjadi ketika sistem gagal mendeteksi kecurangan yang sebenarnya terjadi. Analisis dilakukan untuk mengetahui faktor-faktor yang menyebabkan kesalahan ini, seperti kualitas gambar, posisi kamera, pencahayaan, serta kemiripan objek yang terdeteksi. Evaluasi ini bertujuan untuk memahami keterbatasan sistem dan mengidentifikasi langkah-langkah perbaikan guna meningkatkan akurasi deteksi secara keseluruhan. Berikut ini adalah hasil evaluasi kesalahan deteksi (*false positives* dan *false negatives*) yang terjadi selama pengukuran dari hasil penelitian yang dilakukan.

Tabel 4. Evaluasi Kesalahan Deteksi (*False positives* dan *False negatives*)

| Jenis Kesalahan | Frekuensi | Penyebab Potensial |
|---|---|---|
| *False positive* (Kesalahan mendeteksi kecurangan) | 8% | Gerakan tangan biasa terdeteksi sebagai mencurigakan |
| *False negative* (Gagal mendeteksi kecurangan) | 10% | Ponsel disembunyikan dengan baik atau komunikasi sangat halus |

Keterangan:

1. *False positives* terjadi lebih sering ketika gerakan tangan biasa terdeteksi sebagai mencurigakan, menunjukkan bahwa sistem perlu ditingkatkan dalam membedakan antara gerakan normal dan gerakan yang mencurigakan.
2. *False negatives* terjadi ketika ponsel disembunyikan dengan baik atau komunikasi antar siswa sangat halus, yang menunjukkan tantangan dalam mendeteksi kecurangan dengan metode berbasis pengawasan video.

3.2 Pembahasan

Dalam era digital yang semakin maju, pengawasan ujian berbasis teknologi menjadi kunci untuk memastikan integritas akademik. Salah satu inovasi yang dikembangkan untuk tujuan tersebut adalah sistem deteksi kecurangan berbasis visi komputer menggunakan algoritma YOLO (*You Only Look Once*). Sistem ini dirancang untuk mengidentifikasi tindakan mencurigakan selama ujian, seperti penggunaan ponsel atau komunikasi antar peserta ujian, dengan memanfaatkan rekaman video dan teknik deep learning. Pendekatan ini menawarkan keuntungan berupa deteksi yang lebih efektif, efisien, dan objektif dibandingkan dengan pengawasan manual. Di bawah ini, pembahasan mendalam akan disampaikan mengenai alur kerja sistem deteksi kecurangan berbasis YOLO, termasuk pengumpulan data, proses pelatihan model, serta evaluasi performa yang dihasilkan.

1. Akurasi Model

   Berdasarkan hasil evaluasi performa model, sistem pendeteksi kecurangan ujian berbasis YOLO menunjukkan kinerja yang baik dengan nilai mAP (*mean Average Precision*) sebesar 89,2%. Hal ini menandakan bahwa sistem memiliki kemampuan tinggi dalam mendeteksi objek yang berkaitan dengan kecurangan, seperti penggunaan ponsel dan interaksi mencurigakan antar peserta ujian. *Precision* sebesar 91,5% menunjukkan bahwa model jarang menghasilkan *false positives* (kesalahan mendeteksi aktivitas normal sebagai kecurangan), sehingga memberikan keandalan dalam deteksi kecurangan tanpa terlalu banyak kesalahan deteksi. Di sisi lain, *Recall* sebesar 87,8% mengindikasikan bahwa meskipun model mampu mendeteksi sebagian besar kasus kecurangan, masih ada beberapa *false negatives* (kecurangan yang terlewat) yang perlu diperhatikan. Dengan F1-score sebesar 89,6%, model ini menunjukkan keseimbangan yang baik antara *precision* dan *recall*, sehingga menjamin bahwa sistem dapat mendeteksi kecurangan secara akurat dengan tingkat kesalahan yang minimal.

   Meskipun hasil ini menunjukkan performa yang cukup baik, terdapat ruang untuk optimasi lebih lanjut. Salah satu langkah yang dapat diambil adalah pengumpulan lebih banyak data pelatihan dengan variasi skenario kecurangan yang lebih luas, serta pengoptimalan hyperparameter yang lebih mendalam untuk meningkatkan akurasi model dalam berbagai kondisi ujian yang lebih kompleks.

2. Performa Sistem dalam Kondisi Ujian Nyata

   Berdasarkan hasil pengujian pada lingkungan ujian nyata, sistem pendeteksi kecurangan berbasis YOLO menunjukkan performa optimal dalam beberapa aspek utama. Dengan kecepatan pemrosesan sebesar 25 FPS, sistem dapat beroperasi secara *real-time*, memungkinkan deteksi aktivitas mencurigakan tanpa jeda yang signifikan, sehingga pengawas dapat segera merespons setiap indikasi kecurangan yang terdeteksi. Selain itu, toleransi terhadap pencahayaan yang sangat baik memastikan bahwa model tetap stabil baik dalam kondisi pencahayaan alami maupun buatan, yang merupakan hal penting mengingat variasi pencahayaan yang mungkin terjadi di berbagai ruang ujian.

   Kemampuan generalisasi model yang tinggi juga menjadi keunggulan utama, di mana model dapat mendeteksi kecurangan dalam berbagai skenario berbeda, termasuk variasi sudut kamera, posisi peserta ujian, serta jenis perilaku mencurigakan lainnya. Keunggulan ini menjadikan sistem sangat fleksibel dan dapat diterapkan di berbagai kondisi ujian tanpa memerlukan penyesuaian yang signifikan. Hal ini menunjukkan bahwa sistem deteksi berbasis YOLO sangat cocok untuk implementasi dalam situasi pengawasan ujian yang dinamis.

3. Hasil Pengujian terhadap Berbagai Skenario Kecurangan

   Berdasarkan hasil pengujian terhadap berbagai skenario kecurangan, sistem pendeteksi berbasis YOLO menunjukkan tingkat akurasi yang cukup tinggi dalam mendeteksi berbagai bentuk kecurangan. Pada penggunaan ponsel,

sistem berhasil mendeteksi 90% dari 20 kasus, menunjukkan bahwa model memiliki akurasi tinggi dalam mengenali objek ponsel karena karakteristik visualnya yang jelas. Namun, 10% kasus tidak terdeteksi, kemungkinan disebabkan oleh posisi ponsel yang tersembunyi atau pencahayaan yang memengaruhi kualitas deteksi. Pada skenario komunikasi antar mahasiswa, tingkat deteksi mencapai 85% dari 15 kasus, sedikit lebih rendah dibanding penggunaan ponsel, karena komunikasi sering kali melibatkan gerakan kecil seperti kontak mata atau isyarat halus yang sulit dibedakan dari interaksi biasa. Sementara itu, untuk gerakan tangan mencurigakan, sistem mampu mendeteksi 88% dari 25 kasus, meskipun masih terdapat beberapa gerakan yang tidak dikenali akibat variasi posisi tangan, kecepatan gerakan, atau kemiripan dengan gerakan alami yang tidak mencurigakan. Secara keseluruhan, hasil ini menunjukkan bahwa sistem memiliki performa yang baik dalam mendeteksi kecurangan, meskipun masih terdapat ruang untuk perbaikan, terutama dalam meningkatkan sensitivitas terhadap interaksi yang lebih halus.

4. Evaluasi Kesalahan Deteksi (*False positive*s & *False negative*s)

   Dalam evaluasi kesalahan deteksi sistem, ditemukan dua jenis kesalahan utama, yaitu *false positives* sebesar 8% dan *false negatives* sebesar 10%. *False positives* terjadi ketika sistem salah mengidentifikasi aktivitas normal sebagai kecurangan. Penyebab utama dari false positive adalah gerakan tangan yang biasa, seperti menulis atau merapikan meja, yang terdeteksi sebagai mencurigakan. Kesalahan ini dapat menghasilkan alarm palsu yang mengganggu peserta ujian dan pengawas, dan dengan demikian meningkatkan potensi gangguan dalam pengawasan ujian. Untuk mengurangi *false positive*, pelatihan model dengan lebih banyak data mengenai gerakan tangan alami serta penerapan teknik analisis konteks atau durasi gerakan dapat membantu dalam mengurangi kesalahan ini. Di sisi lain, *false negatives* terjadi ketika sistem gagal mendeteksi kecurangan yang sebenarnya terjadi, dengan tingkat kesalahan mencapai 10%. Penyebab utama dari *false negative* adalah ponsel yang disembunyikan dengan baik atau komunikasi yang sangat halus antar peserta ujian, yang sulit untuk dideteksi oleh kamera. Kesalahan ini lebih berbahaya karena memungkinkan pelanggaran untuk terjadi tanpa terdeteksi. Untuk mengurangi *false negative*, peningkatan resolusi kamera dan penggunaan teknik pelacakan perilaku berbasis *machine learning* dapat membantu untuk menangkap lebih banyak detail dari interaksi yang tersembunyi. Selain itu, integrasi dengan sensor suara atau algoritma NLP (*Natural Language Processing*) untuk mendeteksi komunikasi verbal yang tidak sah dapat menjadi solusi tambahan yang dapat meningkatkan efektivitas sistem secara keseluruhan.

## 4. KESIMPULAN

Hasil evaluasi yang dilakukan dalam penelitian ini menunjukkan bahwa sistem memiliki akurasi tinggi dengan precision yang cukup baik, namun *recall* yang sedikit lebih rendah mengindikasikan adanya beberapa kasus kecurangan yang tidak terdeteksi. Untuk meningkatkan performa, model dapat disempurnakan dengan lebih banyak data pelatihan yang mencakup berbagai kondisi pencahayaan, sudut kamera, serta variasi perilaku kecurangan. Sistem menunjukkan performa yang baik dalam kecepatan pemrosesan sebesar 25 FPS, ketahanan terhadap perubahan pencahayaan, serta kemampuan generalisasi dalam mendeteksi kecurangan di berbagai skenario. Meskipun demikian, sistem masih dapat ditingkatkan lebih lanjut dengan pengujian dalam kondisi ekstrem, seperti pencahayaan sangat rendah atau hambatan visual yang mengganggu deteksi.

Dengan tingkat akurasi berkisar antara 85% hingga 90%, sistem lebih efektif dalam mengenali objek fisik seperti ponsel dibandingkan dengan perilaku atau interaksi kompleks seperti komunikasi antar mahasiswa. Untuk meningkatkan performa, beberapa langkah dapat dilakukan, seperti meningkatkan variasi dataset pelatihan khususnya untuk skenario komunikasi dan gerakan tangan, menyempurnakan model deteksi perilaku agar lebih akurat dalam membedakan interaksi normal dan mencurigakan, serta mengintegrasikan metode tambahan seperti analisis suara atau pola gerakan guna meningkatkan akurasi deteksi. Evaluasi juga menunjukkan bahwa sistem memiliki *false positive* yang relatif rendah (8%), namun masih mengalami *false negative* yang cukup tinggi (10%), yang berarti model lebih cenderung melewatkan beberapa bentuk kecurangan dibandingkan salah mendeteksi aktivitas normal sebagai kecurangan. Oleh karena itu, optimasi lebih lanjut dalam pendeteksian gerakan tangan serta pengenalan skenario kecurangan yang lebih kompleks diperlukan untuk meningkatkan efektivitas sistem.

## 5. DAFTAR PUSTAKA

Abdi, H., dan Williams, L. J. (2010). Principal component analysis. Wiley Interdisciplinary Reviews: Computational Statistics, 2(4), 433–459. https://doi.org/10.1002/wics.101

Bochkovskiy, A., Wang, C.-Y., & Liao, H.-Y. M. (2020). YOLOv4: Optimal Speed and Accuracy of Object Detection. Computer Vision and Pattern Recognition 1–17. https://doi.org/10.48550/arXiv.2004.10934

Li, G., Zhang, M., Zhang, Q., & Lin, Z. (2022). Efficient binary 3D convolutional neural network and hardware accelerator. Journal of Real-Time Image Processing, 19(5), 61–71. https://doi.org/10.1007/s11554-021-01161-4

Lin, T. Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., Dollár, P., & Zitnick, C. L. (2014). *Microsoft COCO: Common Objects in Context.* In European Conference on Computer Vision (ECCV).

Redmon, J., & Farhadi, A. (2018). YOLO v.3. Tech Report, 1–6. https://pjreddie.com/media/files/papers/YOLOv3.pdf

Shaikat, Abu & Hussein, Molla Rashied & Tasnim, Rumana & Farhan, Ahmed & Khan, Ahsan & Mokhtar, Anowar & Rahman, Md. (2023). *Computer Vision Based Automated Attendance System Using Face Recognition*. 6th Industrial Engineering and Operations Management Bangladesh Conference. http://dx.doi.org/10.46254/BA06.20230105.

Vidhya S.G., Hema G.A., Jeevitha M.G., Nischitha K.B., and Vandana. (2022). *Ai-Based Proctoring System For Online Tests*. International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), Volume:04 /Issue:07/July-2022. 4291-4298.

Yulita, I. N., Hariz, F. A., Suryana, I., & Prabuwono, A. S. (2023). Educational Innovation Faced with COVID-19: Deep Learning for Online Exam Cheating Detection. Education Sciences, 13(2), 194. https://doi.org/10.3390/educsci13020194.