Implementasi Aplikasi Pendeteksi Kecurangan Ujian Berbasis Kamera Dengan Pendekatan Transfer Learning

Nanang Prihatin[1], Herri Mahyar[2], Muhammad Azzahari[3], Muhammad Kahfi Aulia[4*]

[1,3] *Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*

[2] *Jurusan Teknik Sipil Politeknik Negeri Lhokseumawe*

Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

[1]nanang@pnl.ac.id

[2]herrimahyar@pnl.ac.id

[3]azzahari@pnl.ac.id

[4] *Program Studi Informatika Medis Universitas Bumi Persada*

Jln. Banda Aceh - Medan No. 59 Alue Awe 24352 INDONESIA

[4*]auliamuhammadkahfi@gmail.com

Abstrak— **Integritas akademik selama ujian masih menjadi tantangan, karena pengawasan konvensional berbasis manusia sering kesulitan mendeteksi perilaku kecurangan yang halus. Penelitian ini mengusulkan pengembangan sistem deteksi kecurangan ujian berbasis kamera dengan memanfaatkan *transfer learning* pada arsitektur *Convolutional Neural Network* (CNN) ResNet-50. Model dilatih menggunakan dataset yang dirancang untuk mencerminkan situasi ujian nyata, dengan variasi perilaku mencurigakan seperti melirik jawaban teman atau menggunakan catatan tersembunyi. Hasil eksperimen menunjukkan bahwa hanya dengan 10 *epoch*, ResNet-50 mampu mencapai akurasi pengujian sebesar 97,7% sekaligus mempertahankan konvergensi yang stabil pada data pelatihan dan validasi. Model terpilih kemudian diintegrasikan ke dalam prototipe aplikasi yang mampu melakukan pemantauan *real-time* serta mengirim notifikasi instan melalui *chatbot*, sehingga pengawas dapat melakukan intervensi tepat waktu. Temuan penelitian ini tidak hanya meningkatkan keadilan dan keandalan dalam evaluasi akademik, tetapi juga menawarkan kerangka kerja yang skalabel untuk diterapkan dalam konteks pemantauan pendidikan yang lebih luas.**

Kata kunci— Transfer Learning, Deteksi Kecurangan Ujian, Convolutional Neural Network, Pengawasan Waktu Nyata, Integritas Akademik

Abstract— **Academic integrity during examinations remains a significant challenge, as conventional human-based supervision often struggles to detect subtle cheating behaviors. This study proposes the development of a camera-based exam cheating detection system by leveraging transfer learning with the ResNet-50 Convolutional Neural Network (CNN) architecture. The model was trained on a dataset designed to reflect real exam scenarios, incorporating suspicious behaviors such as glancing at a peer's answers or using hidden notes. Experimental results demonstrate that with only 10 epochs, ResNet-50 achieved a test accuracy of 97.7% while maintaining stable convergence across training and validation data. The selected model was then integrated into a prototype application capable of real-time monitoring and instant notification delivery via a chatbot, enabling proctors to intervene promptly. These findings not only enhance fairness and reliability in academic evaluation but also offer a scalable framework for broader applications in educational monitoring.**

Keywords— Transfer Learning, Exam Cheating Detection, Convolutional Neural Network, Real-time Monitoring, Academic Integrity

I. PENDAHULUAN

Integritas akademik merupakan pilar fundamental dari pendidikan berkualitas, menjadi dasar bagi kredibilitas lembaga pendidikan [1]. Hal ini penting untuk menumbuhkan kemampuan berpikir kritis dan analitis yang diperlukan dalam membentuk warga negara yang beretika serta tenaga kerja yang kompeten [1]. Namun, tantangan kecurangan akademik yang mencakup perilaku seperti plagiarisme, pemalsuan, dan penggunaan materi tidak sah tetap menjadi masalah yang meluas [2]. Tingginya prevalensi masalah ini ditunjukkan oleh berbagai studi; misalnya, sebuah survei self-report mengungkapkan bahwa 93,4% mahasiswa mengaku pernah melakukan kecurangan akademik [1]. Sebagian besar perilaku tersebut terjadi saat ujian, dengan 55,7% mahasiswa mengaku melakukan kecurangan pada situasi tersebut [1].

Implikasi kecurangan akademik meluas jauh melampaui ruang kelas, karena dapat menyebabkan masuknya individu yang tidak kompeten ke dunia kerja [3]. Masalah ini semakin kompleks dengan pesatnya perkembangan teknologi [2]. Kecurangan terjadi baik pada ujian berbasis kertas maupun komputer [3]. Lanskap kecurangan yang terus berkembang menuntut respons teknologi yang adaptif untuk menjaga standar akademik. Pengembangan sistem berbasis kamera dengan kecerdasan buatan merupakan respons langsung terhadap "perlombaan teknologi" ini.

Selama berabad-abad, pengawasan ujian mengandalkan metode tradisional berupa pengawasan langsung. Namun, pengawasan manusia sering kali gagal mendeteksi perilaku kecurangan yang halus di ruang ujian, karena sulit memantau banyak mahasiswa secara bersamaan [4]. Lingkungan ujian luring yang minim pengawasan konstan menimbulkan "kesempatan" untuk berbuat curang, yang menurut teori "*fraud triangle*" merupakan kondisi utama terjadinya kecurangan [2].

Pengembangan sistem berbasis kamera berbiaya rendah dimaksudkan untuk melengkapi pengawas manusia dan mengurangi peluang kecurangan melalui pemantauan berkelanjutan [1]. Sistem ini juga menawarkan cara lebih efisien dibanding pengawasan tradisional [1]. Dengan otomatisasi deteksi perilaku anomali, pengawas dapat fokus pada tugas penting lain, seperti menjawab kebutuhan mahasiswa [4].

Kemunculan kecerdasan buatan (AI), khususnya *machine learning* (ML) dan *deep learning* (DL), menyediakan alat kuat untuk menganalisis pola data kompleks yang sulit dideteksi manusia [5]. Dalam konteks pengawasan ujian, teknologi ini diterapkan melalui *computer vision* untuk mendeteksi dan

mengklasifikasi objek pada video atau citra [5]. CNN terbukti efektif dalam klasifikasi citra dan deteksi objek [5]. Dengan memproses frame video secara berurutan, CNN dapat mengekstrak fitur spasial, dan bila dikombinasikan dengan LSTM, juga mampu mengenali pola temporal [4]. Hal ini menjadikannya cocok untuk *Human Activity Recognition* (HAR), misalnya mengidentifikasi perilaku mencurigakan seperti menoleh, menggunakan catatan ilegal, atau berkomunikasi dengan teman [1].

ResNet-50 menjadi salah satu arsitektur CNN yang paling menonjol karena mampu melatih jaringan yang sangat dalam tanpa menghadapi masalah *vanishing gradient* melalui mekanisme *skip connection* [6]. Model ini telah digunakan secara luas dalam berbagai penelitian, termasuk untuk pengenalan wajah dan deteksi perilaku mencurigakan, dengan hasil akurasi yang tinggi [3][4]. Keunggulan tersebut menjadikan ResNet-50 pilihan tepat untuk mendukung sistem deteksi kecurangan ujian berbasis kamera dengan efisiensi komputasi yang memadai untuk aplikasi real-time.

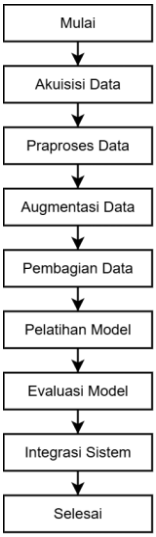
Meningkatnya ujian daring menuntut sistem pengawasan yang efektif untuk menjaga integritas akademik. Banyak penelitian telah menerapkan AI, seperti YOLOv4 [7] dan YOLOv8 [8], yang mampu mendeteksi kecurangan melalui analisis pose tubuh dan ekspresi wajah secara *real-time*. Pendekatan lain menggunakan *landmark* wajah dan orientasi kepala, seperti MediaPipe Face Mesh [9] dan sistem *deep learning* [10], yang terbukti akurat. CNN juga banyak digunakan, misalnya mencapai akurasi 98,5% dengan sensor multimodal [11] atau untuk deteksi pergerakan wajah [12]. Meski terbukti secara teknis, beberapa studi menekankan pentingnya pengalaman pengguna [13] dan perlunya pengembangan lebih luas untuk aspek keamanan dan akses yang adil [14].

Namun, masih terdapat kesenjangan penelitian: belum ada model yang terbukti konsisten tangguh untuk pengawasan ujian luring berbasis kamera dengan efisiensi komputasi tinggi untuk *real-time* dan integrasi skala besar [15]. Penelitian ini bertujuan menjawab kesenjangan tersebut dengan mengusulkan sistem deteksi kecurangan ujian berbasis kamera yang memanfaatkan *transfer learning* pada arsitektur CNN ResNet-50.

II. METODOLOGI PENELITIAN

Penelitian ini mengadopsi metodologi berbasis *deep learning* untuk merancang, melatih, dan mengevaluasi sistem deteksi kecurangan berbasis kamera dalam konteks ujian. Alur metodologis disusun dalam beberapa fase yang saling terkait: akuisisi dataset, praproses dan augmentasi, adaptasi model melalui *transfer learning*, pelatihan dan validasi, serta integrasi sistem untuk penerapan secara *real-time*. Setiap tahap dirancang dengan cermat untuk memastikan reprodusibilitas, skalabilitas, dan ketangguhan solusi yang diusulkan. Gambar 1 menunjukkan diagram blok dari proses penelitian.

Penelitian ini menggunakan satu dataset yang dikumpulkan dalam kondisi simulasi ujian. Dataset ini merekam berbagai perilaku mahasiswa, termasuk kecurangan halus yang mungkin sulit terdeteksi oleh pengawas manusia. Data disusun dengan skema klasifikasi biner, yaitu *cheating act* (mencakup perilaku seperti menoleh, memberi kode, menyerahkan objek, dan menggunakan catatan terlarang) serta *normal act.* Dataset yang telah diakuisisi memerlukan praproses sebelum digunakan untuk pelatihan model *deep learning*. Citra terlebih



Gambar 1. Diagram blok proses penelitian.

dahulu distandardisasi dengan mengubah ukuran ke 224 × 224 piksel agar sesuai dengan model ResNet-50. Normalisasi dilakukan menggunakan mean dan standar deviasi dataset ImageNet. Karena satu citra sering berisi beberapa individu, model deteksi objek YOLOv8 digunakan untuk mendeteksi kelas *person* dan membuat *bounding box* di sekitar tiap mahasiswa. Setiap individu kemudian dipotong (*cropping*) dan disimpan sebagai citra terpisah, memastikan hanya satu orang per *frame*. Setelah *cropping*, dilakukan augmentasi ekstensif dengan pustaka Albumentations, termasuk *flipping*, penyesuaian brightness/*contrast*, rotasi hingga ±20°, *Gaussian noise, motion blur*, modifikasi HSV, koreksi *gamma*, peningkatan berbasis CLAHE, dan *color jittering*. Hingga empat versi *augmented* dihasilkan untuk setiap citra, sehingga dataset semakin besar dan variatif.

Pada tahap pemodelan, transfer learning dimanfaatkan untuk menggunakan representasi dari arsitektur CNN pra-latih yaitu ResNet-50. Bagian *convolutional base* dipertahankan, sementara lapisan klasifikasi akhir diganti dengan *dense layer* khusus untuk klasifikasi biner. Dropout digunakan secara opsional untuk mengurangi risiko *overfitting*. Pelatihan model dilakukan dengan PyTorch. Optimisasi menggunakan Adam *optimizer* dengan fungsi *loss binary cross-entropy*. Pelatihan dilakukan per *epoch* dengan pembaruan bobot melalui *backpropagation*. *Early stopping* diterapkan dengan memantau performa validasi guna mencegah overfitting.

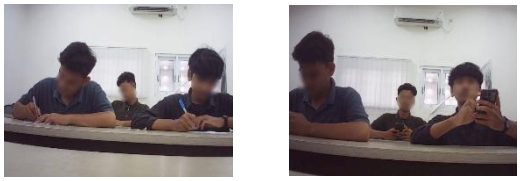
Tidak seperti studi lain yang memakai banyak metrik, penelitian ini berfokus pada akurasi sebagai ukuran utama performa. Akurasi pengujian digunakan agar mencerminkan generalisasi pada data baru. Pendekatan konsisten ini memastikan perbandingan yang jelas antar tahapan. Setelah pelatihan selesai, model final diintegrasikan ke dalam sistem aplikasi prototipe untuk pemantauan ujian. CNN terlatih di-*embed* dalam aplikasi yang memproses aliran video *real-time* dari kamera ruang ujian. Frame yang ditangkap dipraproses secara *real-time* dan dimasukkan ke model untuk inferensi. Mekanisme notifikasi ditambahkan melalui *chatbot*, yang secara otomatis mengirim peringatan bila terdeteksi aktivitas mencurigakan. Integrasi ini memungkinkan intervensi tepat waktu sekaligus mengurangi beban pengawas, terutama pada ujian skala besar.

Secara keseluruhan, kerangka metodologis ini menggabungkan eksperimen *machine learning* yang ketat dengan pertimbangan penerapan praktis. Dengan menggunakan dataset yang diakuisisi, penelitian ini memastikan evaluasi dilakukan pada kondisi beragam, sehingga meningkatkan generalisasi dan relevansi sistem. *Transfer learning* mempercepat konvergensi sekaligus memungkinkan kapasitas representasi tinggi meski dataset terbatas. Akhirnya, integrasi ke prototipe pemantauan *real-time* menegaskan nilai translasional metodologi ini, menjembatani penelitian dan aplikasi nyata.

III. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil pelatihan dan analisis model. Dataset yang diperoleh telah melalui tahap praproses dan augmentasi sebelum digunakan dalam pelatihan. Kinerja model kemudian dievaluasi dengan metrik akurasi. Evaluasi akhir dilakukan menggunakan himpunan uji khusus untuk menilai ketangguhan serta kemampuan generalisasi model. Temuan ini menjadi dasar penting bagi pembahasan selanjutnya mengenai integrasi model ke dalam sistem pemantauan ujian otomatis secara real-time.

Dataset dikumpulkan melalui simulasi kelas yang melibatkan mahasiswa dari Jurusan Teknologi Informasi dan Komputer, Politeknik Negeri Lhokseumawe. Pada tahap akuisisi awal, diperoleh 156 citra yang dikategorikan sebagai *normal act* dan 390 citra sebagai *cheating act*. Citra-citra tersebut diambil dari dua sudut pandang berbeda, yaitu depan dan samping, untuk lebih merepresentasikan perspektif yang mungkin muncul dalam pengawasan ujian nyata. Wajah pada citra sampel telah disensor untuk melindungi privasi subjek. Namun, dataset yang digunakan untuk pelatihan model terdiri dari citra tanpa sensor. Contoh citra mentah dari kedua kategori sebelum praproses ditunjukkan pada Gambar 2. Setiap citra mentah umumnya berisi lebih dari satu mahasiswa, biasanya hingga tiga individu per frame.



Gambar 2. Sampel citra mentah dari dataset pribadi

Untuk memastikan bahwa setiap sampel merepresentasikan satu subjek, YOLOv8 digunakan untuk mendeteksi dan memotong kelas person dari tiap citra. Langkah ini mengubah satu frame dengan banyak orang menjadi beberapa citra terpisah, masing-masing hanya berisi satu mahasiswa. Contoh hasil *cropping* ditunjukkan pada Gambar 3, yang memperlihatkan efektivitas deteksi dan pemotongan.

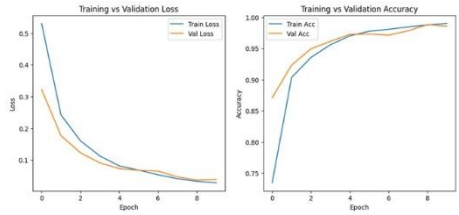
Gambar 3. Sampel citra *cropping* setelah praproses YOLOv8

Setelah proses *cropping*, Albumentations diterapkan untuk meningkatkan variasi dataset. Setiap citra hasil *cropping* diubah menjadi beberapa versi baru melalui operasi seperti *flipping*, rotasi, penyesuaian kecerahan dan kontras, injeksi *noise*, serta blur. Contoh hasil augmentasi ditampilkan pada Gambar 4, yang menunjukkan bagaimana teknik ini mengaugmentasi dataset tanpa mengubah makna kelas asli.

Gambar 4. Sampel citra yang diaugmentasi menggunakan Albumentations

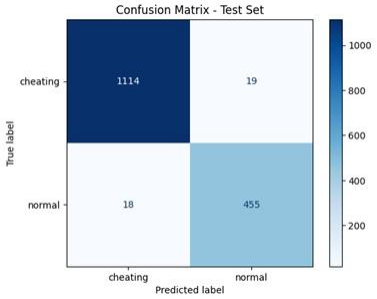
Setelah melalui tahap akuisisi mentah, cropping, dan augmentasi, dataset privat bertambah signifikan dibandingkan dengan data awal. Dataset akhir berjumlah 10.695 citra, yang dibagi menjadi subset pelatihan, validasi, dan pengujian. Set pelatihan terdiri dari 7.486 citra (2.205 *normal act* dan 5.281 *cheating act*), set validasi berjumlah 1.603 citra (472 *normal act* dan 1.131 *cheating act*), dan set pengujian mencakup 1.606 citra (473 *normal act* dan 1.133 *cheating act*). Distribusi ini memastikan model dilatih pada data yang cukup besar dan beragam, sekaligus menyisakan data terpisah untuk validasi serta evaluasi akhir.

Dataset kemudian digunakan untuk melatih model ResNet-50. Pelatihan dilakukan selama 10 *epoch* dengan pengaturan hiperparameter yang sama seperti *default*-nya. Kinerja dimonitor pada subset pelatihan dan validasi untuk melacak konvergensi serta mendeteksi potensi overfitting. Selama *epoch*, akurasi pelatihan dan validasi menunjukkan peningkatan konsisten hingga mencapai performa tinggi. Akurasi pelatihan meningkat dari 73,47% pada *epoch* pertama menjadi 99,01% pada *epoch* ke-10, sementara akurasi validasi naik dari 87,09% menjadi 98,57% pada periode yang sama. Hasil ini menegaskan kemampuan model untuk melakukan generalisasi dengan baik terhadap data yang belum pernah dilihat. Kurva pembelajaran ditunjukkan pada Gambar 5.



Gambar 5. Kurva pembelajaran ResNet-50 pada dataset selama 10 *epoch*.

Analisis proses pelatihan menunjukkan bahwa model mencapai konvergensi stabil dalam jumlah *epoch* yang telah ditentukan. Baik akurasi pelatihan maupun validasi meningkat secara bertahap sementara *loss* menurun konsisten, menandakan pembelajaran efektif tanpa indikasi *overfitting*. Kesesuaian kurva pelatihan dan validasi juga memperlihatkan generalisasi yang baik. Evaluasi pada set uji independen menghasilkan akurasi 97,70%. *Confusion matrix* pada Gambar 6 memberikan rincian lebih lanjut, memperlihatkan kemampuan model membedakan perilaku curang dan normal dengan kesalahan minimal, terutama pada kasus ambigu dengan gerakan samar atau objek yang menutupi sebagian.



Gambar 6. Confusion matrix pada set data uji

Ringkasan proses pelatihan dan hasil evaluasi akhir ditampilkan pada Tabel 1, yang menyajikan kinerja per *epoch* pada set pelatihan dan validasi. Model ResNet-50 yang telah difinalisasi kemudian disimpan dan diintegrasikan ke dalam prototipe sistem untuk penerapan waktu nyata dalam skenario ujian. Hal ini memastikan model terbaik dapat direproduksi dan langsung dimanfaatkan pada aplikasi praktis.

Tabel 1. Kinerja pelatihan dan validasi per *epoch* pada dataset privat.

Epoch	Akurasi Pelatihan (%)	Akurasi Validasi (%)
1	73.47	87.09
2	90.34	92.33
3	93.56	94.95
4	95.59	96.13
5	97.02	97.26
6	97.76	97.32
7	98.06	97.13
8	98.45	97.82
9	98.76	98.81
10	99.01	98.57

Model ResNet-50 final kemudian diimplementasikan ke dalam kerangka aplikasi berbasis web menggunakan Flask. Sistem ini dirancang dengan arsitektur *client–server*, di mana aplikasi dihosting pada server pusat, sementara proses akuisisi citra memanfaatkan kamera yang terhubung ke mesin klien di ruang ujian. Untuk menangkap beragam perspektif perilaku mahasiswa, digunakan tiga kamera: satu di depan serta dua di sisi kiri dan kanan. Setiap kamera dikonfigurasi dengan interval tangkap dua detik dan resolusi 320×240 piksel pada 10 frame per detik, menyeimbangkan kualitas citra dengan efisiensi komputasi.

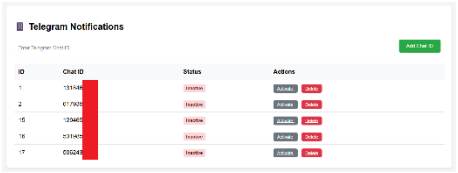
Frame yang ditangkap dialirkan ke server, di mana operasi praproses dilakukan sebelum tahap inferensi. Operasi ini mencakup pengubahan ukuran setiap citra menjadi 224×224 piksel, konversi nilai piksel ke format tensor, dan normalisasi menggunakan nilai mean serta standar deviasi dari ImageNet. Setelah praproses, citra diteruskan ke model ResNet-50 yang telah di-*finetune*. Model menghasilkan label prediksi, yaitu *normal act* atau *cheating act*, beserta skor kepercayaan. Sebuah ambang keputusan diterapkan: jika label prediksi adalah cheating dan tingkat kepercayaan melebihi 90%, sistem menandai kejadian tersebut sebagai percobaan kecurangan.

Ketika kondisi ini terpenuhi, sistem memicu dua respons penting. Pertama, hasil deteksi disimpan ke dalam basis data lokal SQLite, yang merekam stempel waktu, label prediksi, nilai kepercayaan, sumber kamera, dan jalur citra yang ditangkap. Hal ini memastikan bahwa seluruh aktivitas

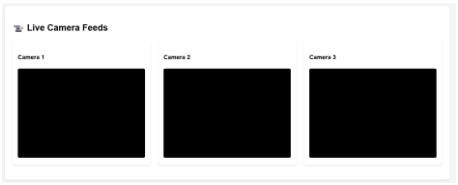
mencurigakan terdokumentasi secara sistematis untuk ditinjau setelah ujian. Kedua, sebuah peringatan langsung dikirim melalui chatbot Telegram terintegrasi. Peringatan tersebut memuat citra tangkapan sebagai bukti visual, hasil klasifikasi, skor probabilitas, waktu tangkap yang tepat, serta identifikasi kamera sumber. Mekanisme ini memungkinkan pengawas ujian menerima notifikasi secara real time di perangkat seluler mereka, sehingga dapat melakukan intervensi tepat waktu tanpa perlu memantau feed kamera secara terus-menerus.

Antarmuka web aplikasi dikembangkan untuk mendukung pemantauan dan manajemen yang komprehensif. Gambar 7 menunjukkan modul CRUD yang memungkinkan administrator menambah, memperbarui, atau menghapus ID chat Telegram yang berhak menerima notifikasi. Gambar 8 memperlihatkan antarmuka feed kamera real time, di mana aliran video dari tiga kamera ditampilkan secara paralel untuk memberikan kesadaran situasi secara simultan. Gambar 9 menampilkan dasbor log yang mengompilasi semua deteksi sebelumnya dalam format pencarian dengan halaman bertahap, sehingga supervisor dapat meninjau catatan kecurangan historis secara efisien. Terakhir, Gambar 10 menggambarkan contoh notifikasi chatbot Telegram, yang menunjukkan bagaimana sistem mengirimkan metadata penting dan bukti citra langsung ke perangkat pengawas.

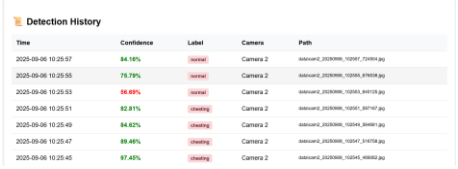
Dalam praktiknya, sistem menunjukkan operasi yang efisien meskipun hanya menggunakan CPU, menegaskan kelayakannya untuk diterapkan di lingkungan tanpa GPU khusus. Penggunaan multi-threading memastikan ketiga kamera dapat beroperasi secara bersamaan tanpa penundaan signifikan, sementara pengaturan tangkapan video yang ringan mengurangi beban komputasi.



Gambar 7. Antarmuka CRUD untuk mengelola ID chat Telegram yang diizinkan menerima notifikasi.



Gambar 8. Antarmuka tampilan langsung kamera yang menampilkan pemantauan simultan dari tiga kamera.



Gambar 9. Dashboard pencatatan yang menampilkan hasil deteksi yang disimpan dalam basis data.

Gambar 10. Contoh notifikasi chatbot Telegram yang berisi bukti yang terekam, hasil klasifikasi, dan metadata.

Notifikasi secara konsisten terkirim dalam hitungan detik setelah deteksi, mengonfirmasi responsivitas implementasi. Namun, terdapat keterbatasan pada penempatan kamera: karena kamera dipasang pada level lantai, bukan dari atas, pemantauan kelompok besar peserta ujian secara bersamaan menjadi kurang optimal. Meskipun demikian, sistem secara andal mendeteksi perilaku mencurigakan dari individu yang berada dalam bidang pandang kamera, sehingga memvalidasi kelayakan desain yang diusulkan.

IV. KESIMPULAN

Penelitian ini berhasil mendemonstrasikan pengembangan sistem deteksi kecurangan ujian berbasis kamera dengan memanfaatkan transfer learning pada arsitektur CNN ResNet-50. Hasil eksperimen menunjukkan bahwa model mampu mencapai akurasi pengujian sebesar 97,7% sekaligus menjaga kestabilan konvergensi pada fase pelatihan maupun validasi. Temuan ini mengonfirmasi kemampuan generalisasi ResNet-50, sehingga menjadikannya pilihan yang tepat untuk implementasi nyata dalam skenario pemantauan ujian.

Model final kemudian diintegrasikan ke dalam prototipe sistem berbasis web yang dibangun menggunakan Flask, dengan memanfaatkan tiga kamera sisi klien untuk menangkap aktivitas ujian secara real-time. Sistem ini menjalankan tahapan praproses, inferensi, dan pengambilan keputusan berbasis ambang kepercayaan, yang dilanjutkan dengan notifikasi instan melalui chatbot Telegram serta pencatatan terstruktur ke dalam basis data lokal. Implementasi eksperimental membuktikan bahwa sistem dapat beroperasi secara efisien bahkan tanpa dukungan GPU, dengan notifikasi yang terkirim hanya dalam hitungan detik setelah deteksi. Meskipun penempatan kamera memberikan keterbatasan dalam menjangkau kelompok besar secara simultan, kinerja keseluruhan membuktikan kelayakan kerangka kerja yang diusulkan. Dengan demikian, penelitian ini memberikan kontribusi berupa pendekatan yang terukur, berbiaya rendah, dan praktis dalam meningkatkan integritas akademik melalui pemantauan berbasis AI.

REFERENSI

[1] P. Anitha and S. Sundaram, “Prevalence, Types and Reasons for

Academic Dishonesty among College Students," *J. Stud. Soc. Sci. Humanit.*, no. 1, p. 1, 2021, [Online]. Available: http://www.jssshonline.com/

[2] O. L. Holden, M. E. Norris, and V. A. Kuhlmeier, "Academic Integrity in Online Assessment: A Research Review," *Front. Educ.*, vol. 6, no. July, pp. 1–13, 2021, doi: 10.3389/feduc.2021.639814.

[3] T.-C. Phan, A.-C. Phan, and H.-D. Tran, "Exam Cheating Detection Based on Action Recognition Using Vision Transformer," 2023, pp. 65–77. doi: 10.1007/978-981-99-7649-2_6.

[4] A. Sarwat, K. Vaidehi, and M. Sowmya, "Human Activity Recognition Using CNN and LSTM Methods," *J. Basic Sci.*, vol. 22, no. 11, pp. 367–381, 2022, doi: 10.37896/JBSV22.11/1541.

[5] B. Erdem and M. Karabatak, "Cheating Detection in Online Exams Using Deep Learning and Machine Learning," *Appl. Sci.*, vol. 15, no. 1, p. 400, Jan. 2025, doi: 10.3390/app15010400.

[6] K. Lipianina-Honcharenko, M. Telka, and N. Melnyk, "Comparison of ResNet, EfficientNet, and Xception architectures for deepfake detection," in *Proceedings of the 1st International Workshop on Advanced Applied Information Technologies CEUR-WS*, 2024, pp. 26–34.

[7] T. Nur, Huzaeni, and M. Khadafi, "Implementasi Metode Object Detection Dengan Algoritma You Only Look Once (YOLO) Untuk Deteksi Kecurangan Di Dalam Ruang Ujian," *J. Teknol. Rekayasa Inf. dan Komput.*, vol. 6, no. 2, pp. 28–33, 2023.

[8] A. N. A. Thohari, M. F. Lathief, L. Triyono, and K. Santoso, "Deteksi Kecurangan Ujian Pada Ruangan Tertutup Menggunakan Algoritma YOLOv8," *J. Comput. Sci. Informatics Eng.*, vol. 4, no. 2, pp. 61–71, May 2025, doi: 10.55537/cosie.v4i2.1100.

[9] E. Bimantoro, M. F. Hidayattullah, and D. I. Af'idah, "Learning Management System (LMS) Pada Kursus Online Berbasis Deteksi Kecurangan Ujian Menggunakan Model Mediapipe Face Mesh," *JIKO (Jurnal Inform. dan Komputer)*, vol. 8, no. 2, p. 268, 2024, doi: 10.26798/jiko.v8i2.1167.

[10] F. B. Wicaksono and Y. Yamasari, "Pengembangan Model Pengawas Ujian Berbasis Kecerdasaan Buatan untuk Ujian Online," *J. Informatics Comput. Sci.*, vol. 6, no. 03, pp. 882–890, Jan. 2025, doi: 10.26740/jinacs.v6n03.p882-890.

[11] M. P. Pangestu, S. Wiyono, and D. I. Af'idah, "Platform Ujian Online Berbasis Pendeteksi Gerakan Kecurangan Menggunakan Kamera," *Infomatek*, vol. 26, no. 1, pp. 55–62, 2024, doi: 10.23969/infomatek.v26i1.11208.

[12] M. I. Thohir, A. P. Iskandar, I. L. Kharisma, Kamdan, and A. Fergina, "Implementasi Gerakan Wajah pada Sistem Ujian Online menggunakan Algoritma Convolutional Neural Network," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 5, no. 2, pp. 483–492, Sep. 2024, doi: 10.37859/coscitech.v5i2.7270.

[13] Erik, S. G. Amalga, and S. N. Adzani, "Evaluasi UI/UX Aplikasi Web Deteksi Kecurangan Ujian Online Berbasis Video Dengan Sistem Usability Scale," *J. Pas. Inform.*, vol. 3, no. 1, 2024, doi: 10.23969/pasinformatik.v3i1.12545.

[14] R. Setiawan, "OPTIMASI PENGALAMAN PENGGUNA DAN PROTOTYPING UNTUK PENILAIAN OTOMATIS DAN PENCEGAHAN KECURANGAN," *bit-Tech*, vol. 7, no. 2, pp. 299–306, Dec. 2024, doi: 10.32877/bt.v7i2.1758.

[15] S. Essahraui *et al.*, "Deep Learning Models for Detecting Cheating in Online Exams," *Comput. Mater. Contin.*, no. August, pp. 1–10, 2025, doi: 10.32604/cmc.2025.067359.

.