International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

Online Supervision-Based System Using CNN for Detecting Fraud in Exams

Muhajir Anshar[1], Zahir Zainuddin[1*], and Ady Wahyudi Paundu[1]

[1] *Departement of Informatics, Hasanuddin University, Makassar, Indonesia*

E-mail address: ansharm20d@student.unhas.ac.id, zahir@unhas.ac.id, adywp@unhas.ac.id

Received ## Mon. 20##, Revised ## Mon. 20##, Accepted ## Mon. 20##, Published ## Mon. 20##

Abstract: Maintaining academic integrity during exams is crucial in the rapidly evolving digital era. This study proposes a student behaviour monitoring system using deep learning technology, specifically Convolutional Neural Networks (CNN), to detect cheating in real-time. The system combines the Single Shot Multibox Detector (SSD) for face detection and the Haar Cascade algorithm for eye detection, enabling the analysis of behaviours such as focus, suspicion, and cheating during exams. Results show that the SSD model achieves over 95% accuracy for face detection under adequate lighting, while the Haar Cascade achieves around 90% accuracy for eye detection. This method effectively detects cheating with a 92% accuracy rate, provides immediate feedback to exam proctors, and stores behaviour data for further analysis. The primary contribution of this research is developing an efficient and reliable exam monitoring system that not only detects cheating in real time but also provides comprehensive behaviour data to enhance exam security and integrity. Additionally, the system's ability to store and analyze behaviour data allows continuous improvement and customization to address various cheating patterns. Although further development is needed to improve accuracy under low lighting conditions and implement advanced machine learning technologies, this method can significantly enhance exam monitoring. It offers a more comprehensive and reliable solution than previous methods, contributing to upholding academic standards in online and traditional exam settings.

Keywords: Cheating detection, Real-time monitoring, Convolutional Neural Networks, Single Shot Multibox Detector, Haar Cascade, Exam integrity.

1. INTRODUCTION

In the swiftly evolving digital era, technology has become crucial to many aspects of life, including education. Technology in education extends beyond the learning process to encompass evaluation and assessment systems. One of the significant challenges in educational evaluation is maintaining integrity and honesty during exams. Cheating in exams is a critical issue that can undermine the credibility of the education system and disadvantage honest students.

This research uses real-time gesture detection technology to detect cheating during manual paper-based exams. Detecting cheating in paper-based exams requires a different approach compared to computer-based exams. Manual paper exams demand stricter supervision because invigilators can only sometimes closely monitor every student's movements. Therefore, employing gesture detection technology can provide an effective solution to this problem.

Face and gesture detection technology has advanced rapidly in recent years. Previous research has demonstrated that deep learning techniques, such as Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs), can enhance the accuracy of face and gesture recognition under various lighting conditions and angles [1]. Techniques for body and face pose estimation, such as those used in the OpenPose model, have also proven effective in detecting suspicious movements in real-time [2].

Manual exams focus on the exam paper, the student's face, and the upper body. The primary challenges include initializing focus, detecting head movements, and identifying cheating behaviours. The YOLO algorithm, adapted with new techniques such as GIoU loss and focal loss, can improve the accuracy and speed of detecting abnormal behaviours during exams [3]. Additionally, emotion recognition from facial expressions using complex deep learning models can aid in identifying suspicious behaviours [4].

E-mail address: ansharm20d@student.unhas.ac.id, zahir@unhas.ac.id, adywp@unhas.ac.id

Another common issue in detecting cheating is recognizing suspicious movements made by students. The use of optical flow and neural networks for real-time face and body tracking has shown promising results in enhancing the accuracy of detecting suspicious movements [5]. Integrating multi-modal data, such as video, audio, and exam metadata, can also improve online and manual exam monitoring [6].

An alternative approach is pose-guided human action recognition for exam surveillance. This technique enables body pose analysis and highly accurate detection of suspicious actions [8]. Furthermore, advanced deepfake detection techniques can ensure exam integrity by recognizing faces and verifying student identities [9].

To address these challenges, this research aims to develop a gesture-based cheating detection system that can be implemented in real time during manual exams. This system combines deep learning and machine learning techniques to enhance detection accuracy and speed. Its primary focus is detecting head movements and cheating actions and maintaining focus on the exam paper and the student's face. The outcomes of this research are expected to significantly enhance integrity and honesty in the educational evaluation system.

In pursuit of these objectives, this research will also explore the latest models and algorithms in face and gesture recognition. Additionally, it will review various cheating detection techniques used in online education to see how these methods can be adapted for manual paper-based exams. Thus, this research aims to provide practical solutions for detecting cheating in manual exams and offer new insights into using gesture detection technology in the educational context.

This research will combine various techniques that have proven effective in previous studies and adapt them to the context of manual paper-based exams. This approach is expected to achieve a high level of accuracy in detecting cheating, thereby enhancing the integrity and credibility of the educational evaluation system. Consequently, this research's results are expected to improve honesty and fairness in the academic evaluation process significantly.

2. RELATED WORK

Student performance in courses is the fundamental criterion for higher education institutions to assign academic grades, and the evaluation of their performance depends on the grades they achieve on tests. This section provides a brief overview of various methods used in related studies. While the academic community has explored diverse approaches to enhance examination security and uphold integrity, the intersection of facial analysis and pose recognition, as explored in this study, represents a step toward advancing the efficacy and efficiency of detecting abnormal behaviour in student examination environments.

This research aims to enhance the precision of current face recognition systems by incorporating SVM and Eigenface algorithms. The project employs an Eigenface-inspired approach for extracting facial features via facial vectors, and the datasets undergo training using the Support Vector Machine (SVM) algorithm for efficient face classification and detection. Implementing these techniques expedites face recognition, making it well-suited for online exam monitoring [10].

Zhu et al. addressed the complexities of face detection systems by introducing an innovative method called the Contextual Multi-Scale Region-based Convolutional Neural Network (CMS-RCNN). This approach comprises two key components: a region proposal component and a region-of-interest (RoI) detection component. The system effectively addresses the challenges posed by small face regions by incorporating multi-scale information in both components. Furthermore, it facilitates explicit reasoning about the contextual aspects of the body, contributing to improved face detection accuracy [11].

This study identifies cheating behaviour, employing advanced techniques such as Recurrent Neural Networks (RNNs) or Long Short-Term Memory (LSTM) networks to effectively capture variations in students' response times. Additionally, integrating head and body pose features in the model allows training to recognize visual patterns, enabling the detection of behaviours such as turning around. This is achieved through comprehensive image analysis and leveraging visual data from body movements and turned faces, enhancing the system's ability to discern suspicious activities during examinations [12].

This research implements the improved YOLOv3 algorithm to detect abnormal behaviour in exams. The YOLOv3 algorithm was enhanced using K-Means, GIoU loss, focal loss, and Darknet32 algorithms. The results indicate that the improved YOLOv3 algorithm improves the accuracy and speed of detection. The Mean Average Precision (mAP) of the enhanced YOLOv3 algorithm reached 88.53% on the test set, and the detection speed reached 42 Frames Per Second (FPS) using the dual-thread frame-alternate detection method [13].

Discovering modern techniques where machines can understand the expression of gestures and put them into the context of feelings must be crucial to communication with humans. Several approaches to detecting emotions from faces have been adopted. These approaches tackle the main groups of emotions by relying on straightforward static models that have shown successful results [14]. Face tracking has become a feature of many face-based emotion recognition systems and tools, including measuring optical flow, active contour models, face identification, recovery of a facial pose following facial expression, and probabilistic approaches to detecting and tracking human faces [15].

Research conducted by Al Airaji et al. employed a video camera device to identify object movements indicative of potential cheating within a single examination room. The scope of the research expanded to encompass 17 rooms, each accommodating approximately 20 students. The authors integrated keypoint retrieval references for body pose processing, utilizing OpenPose to enhance the accuracy and efficiency of detecting and analyzing students' body movements during examinations [16].

This paper employs the methodology outlined in the literature [17] to extract the two-dimensional skeleton of escalator passengers. The process begins with a trained OpenPose model to accurately and consistently detect human body joints and the connecting bones between joints, even in an escalator's intricate and dynamic environment. Subsequently, the method uses part affinity fields (PAFs) to seamlessly associate the detected joints of the human body, creating a comprehensive and accurate 2D skeleton representation [17].

This paper presents an algorithm for real-time recognition of abnormal behaviours among escalator passengers in outdoor and sports settings. The method employs an adaptive fractional variational optical flow model to estimate motion characteristics, addressing challenges like illumination changes and low contrast. Simultaneously, the OpenPose model aids in accurate passenger positioning in complex scenes. The fusion of optical flow field and human skeleton information is processed by a random forest classifier to effectively detect abnormal behaviours. Experimental results highlight the algorithm's success in real-world outdoor scenarios, suggesting practical applications [18].

This study focuses on gesture recognition based on computer vision. The issues discussed include the limitations of gesture recognition methods' reliability and effectiveness and challenges such as lack of universality, sensitivity to lighting changes, and occlusion problems. This research applies artificial neural network methods and integrates Hidden Markov Model (HMM) and HMM-FNN models for signal-based gesture recognition. Other methods include feature extraction using a Histogram of Oriented Gradients (HOG) and classification using a Support Vector Machine (SVM) [10]. This study uses an improved YOLOv3 method with K-means clustering, GIoU loss, and Darknet-32. With an average precision of 88.53%, this study has a limitation in that the dataset is too tiny for real-world scenarios, affecting the generalization and validation of results [13]. This research uses an adaptive optical flow method and the OpenPose model to detect abnormal behaviour of escalator passengers. Its limitation is a limited database, making sample collection complex and requiring many samples for valid results. Abnormal behaviour detection in outdoor real-time escalator videos achieved 97.98% and 92.28% accuracy [18].

The author's research focuses on real-time detection during exams. The exam process uses manual exam papers rather than computers or similar devices to detect student cheating based on gestures. The challenges faced by the author include determining the initialization of focus, identifying head turns, and detecting cheating behaviour. The camera's focus objects are the exam paper, the student's face, and the upper body.

3. METHODOLOGY

This research begins with a preprocessing stage, where the system initialization and preparation for video data capture during the exam occur. Video data is captured using a camera placed in front of the student, focusing on the exam paper and the student's face. Next, face detection is performed using SSD (Single Shot Multibox Detector), a fast and efficient object detection method. Eye detection uses Haar Cascade, a feature-based object detection method commonly used in facial recognition.

In this research scenario, behaviour analysis determines the face position and other suspicious behaviours, such as turning the head or looking away from the exam paper. The face position is calculated using the face detection coordinates from the SSD, while suspicious behaviour is calculated based on the percentage of eye movements detected by Haar Cascade. The analysis results are displayed on the video frame in real-time, allowing exam proctors to monitor student activity directly.

A. Proposed Block Diagram

The proposed block diagram illustrates two main processes in the exam monitoring system: training and testing.

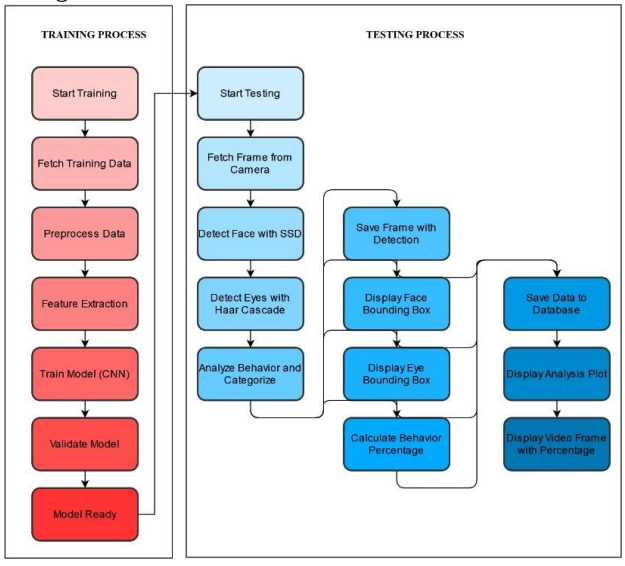

Figure 1. Proposed block diagram

The training begins with the "Start Training" step, marking the commencement of the model training session. Next, training data is fetched ("Fetch Training Data") to

train the model. The obtained data is further processed in the preprocessing stage ("Preprocess Data") to ensure it is ready for use, including normalization and noise reduction. After data processing, essential features are extracted in the "Feature Extraction" stage. These features are then used to train a Convolutional Neural Network (CNN) model in the "Train Model (CNN)" stage. Once training is complete, the model is validated using validation data in the "Validate Model" stage to ensure the model's performance is adequate and not overfitting. If the model passes validation, the training stage is complete, and the model is declared ready for use with the status "Model Ready."

The testing process begins with the "Start Testing" step, marking the start of the model testing session with new data. At this stage, video frames are fetched from the camera in real-time in the "Fetch Frame from Camera" step. After the frame is obtained, the system performs face detection using the SSD model in the "Detect Face with SSD" step. If a face is detected, the system proceeds with eye detection using the Haar Cascade method in the "Detect Eyes with Haar Cascade" step. The face and eye detection results are then analyzed to categorize the student's behaviour in the "Analyze Behavior and Categorize" stage. This analysis helps identify whether the student is focused, suspicious, or cheating. Each analyzed frame is saved with detection marks in the "Save Frame with Detection" stage. Subsequently, bounding boxes showing face and eye detection are displayed in the "Display Face Bounding Box" and "Display Eye Bounding Box" stages.

B. Initialization and Preparation

The first stage in developing this system is initialization and preparation. The steps include installing and configuring the necessary software and preparing the development environment. This includes installing OpenCV, TensorFlow, and other libraries required for facial recognition and object detection. The development environment in Python is also set up, including configuring environment variables and setting directory paths for data and model storage.

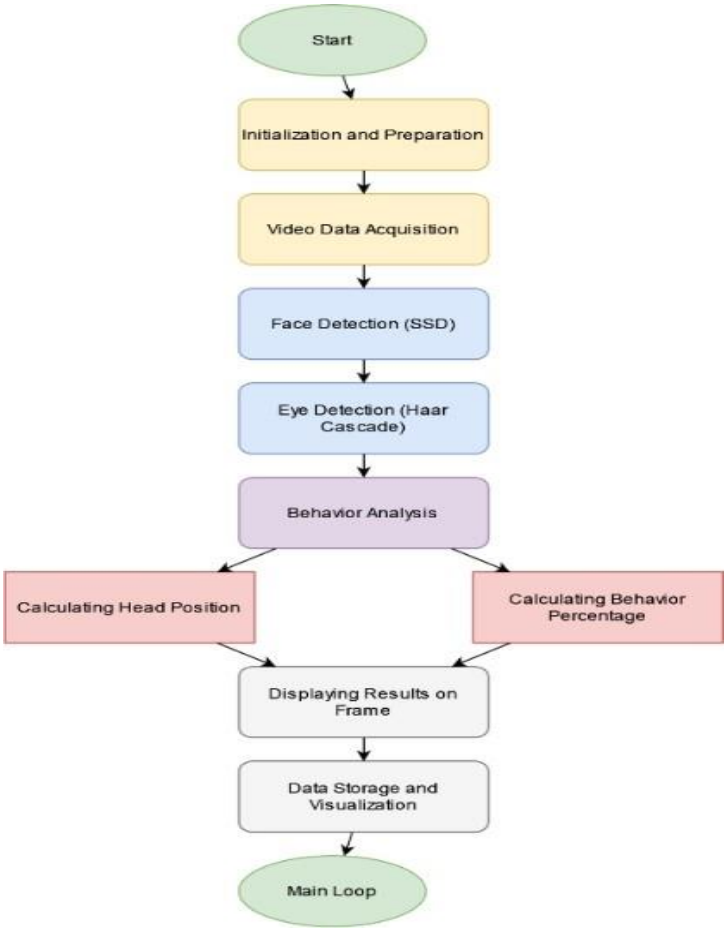

Figure 2: Flowchart

The flowchart of the exam behaviour analysis process starts with system initialization and preparation, followed by video data acquisition. The system then uses the SSD method for face detection and Haar Cascade for eye detection. Next, behaviour analysis is performed by calculating the head position and the percentage of detected

behaviours. The analysis results are displayed on the video frame, and data is saved for further visualization. This process continues in the main loop, ensuring that each video frame is analyzed in real-time to detect potential cheating during the exam.

C. Video Data Capture

The next step is capturing video data from the camera. In this study, an HD 1080P webcam with auto-focus is used. Student videos are taken using a camera placed at the exam location. This camera has sufficient resolution and frame rate to capture student faces and eye movements. The captured video is sent to the monitoring system for real-time processing.

D. Face Detection with SSD

The SSD (Single Shot MultiBox Detector) model detects student faces in each video frame. SSD was chosen because it is one of the fastest and most efficient object detection methods and is suitable for real-time applications. Face detection is performed using a pre-trained SSD on a representative facial dataset, ensuring high accuracy under various lighting conditions.

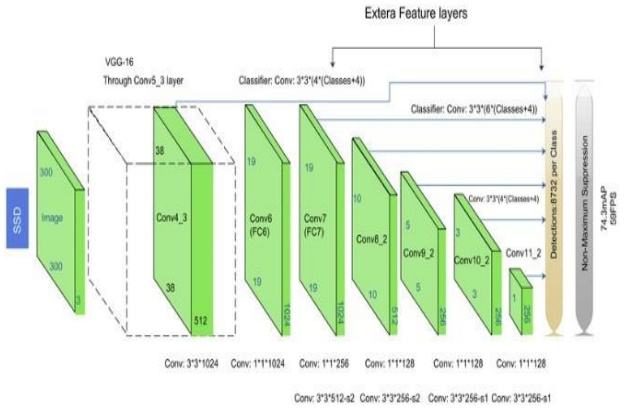

Figure 3: SSD Architecture

E. Eye Detection with Haar Cascade

After face detection, the next step is eye detection using Haar Cascade. Haar Cascade is a feature-based object detection method often used in facial recognition. This method is chosen for its ability to detect eyes quickly and accurately. The eye detection results form the basis for further analysis of student behaviour during the exam. Below is the formula used in Haar Cascade:

$$f = (x, y, w, h) = \sum_{(x,y)\in rect} w \times I(x, y)$$

Where f is the feature (x, y) is the pixel coordinate, w is the weight, and I is the intensity.

TABLE I. Example of eye detection results

Frame	Left Eye Detected	Left Eye Bounding Box	Right Eye Detected
1	Yes	(70, 120, 90, 140)	Yes
2	Yes	(75, 125, 95, 145)	Yes
3	No	-	Yes
4	Yes	(80, 130, 100, 150)	Yes

F. Behavior Analysis

The behaviour analysis method calculates the percentage of time students spend in three behaviour categories: focused, suspicious, and cheating. The calculation is based on the duration of time spent on each behaviour during the exam. Behaviour analysis reveals significant variations in student behaviour throughout the exam. For example, students exhibiting suspicious or cheating behaviour are identified based on the percentage of eye movements detected by Haar Cascade. The analysis results are displayed on the video frame in real-time, allowing exam proctors to monitor student activity directly.

To calculate the position and orientation of the face, we can use the position vector from the coordinates of the eyes and nose. For instance, if (X_1, Y_1) and (X_2, Y_2) are the coordinates of the left and right eyes, and (X_n, Y_n) is the nose coordinate, the face orientation angle θ can be calculated as:

$$\theta = arctan\frac{y2 - y1}{x2 - x1}$$

The percentage of suspicious behaviour is calculated based on the number of frames where suspicious detection occurs divided by the total frames processed:

$$P_{suspicios} = \frac{N_{suspicios}}{N_{total}} x\ 100\%$$

TABLE II. Example of Behavior Analysis Results

Frame	Face Position	Left Eye Position	Right Eye Position	Detected Behavior
1	(0.25, 0.5)	(0.35, 0.6)	(0.75, 0.6)	Focused
2	(0.26, 0.52)	(0.36, 0.62)	(0.76, 0.62)	Focused
3	(0.27, 0.54)	(0.37, 0.64)	(0.77, 0.64)	Looking Away
4	(0.28, 0.56)	(0.38, 0.66)	(0.78, 0.66)	Cheating

G. Data Storage and Visualization

After performing behaviour analysis, the resulting data is stored in an SQLite database for further study. Data visualization uses Matplotlib to visually represent student behaviour during the exam. This data includes information on face and eye positions as well as the identification of suspicious behaviours. Storage is done in real-time so that

any behavioural changes can be recorded immediately upon detection. In addition to storage, data visualization is also conducted to provide an immediate overview of student activities during the exam. This visualization data is presented as charts or diagrams showing the frequency and types of suspicious behaviours detected. This helps exam proctors make quick decisions if there are indications of cheating. Storing and visualizing data runs concurrently with the main loop, ensuring that every analyzed video frame can be promptly stored and visualized for effective monitoring.

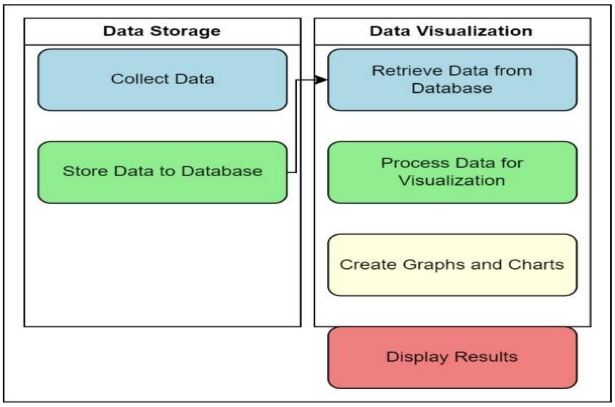

Figure 4: Behavioral Data Visualization

H. Main Loop

This process runs throughout the exam, ensuring continuous real-time monitoring. The system first captures video frames from the installed camera in the main loop. Once a frame is captured, face detection is performed using the SSD model to identify facial areas in each video frame. Next, eye detection is conducted using Haar Cascade on the detected face to locate eye positions. After the face and eye positions are determined, behaviour analysis is carried out based on this positional data, identifying suspicious patterns such as turning or looking away. The results of this analysis are then stored and visualized in real-time for more effective monitoring. This process is repeated for each video frame, ensuring that any changes in student behaviour can be detected immediately during the exam.

4. RESULT AND DISCUSSION

A. Face and Eye Detection

In this discussion, we employed the SSD (Single Shot Detector) face detection model, trained on a facial dataset, to detect faces in video frames. The "detect_faces" function takes a frame as input, converts it into a blob, and sends it to the model for detection. The dataset used consists of real-time video frames captured from the camera. Each frame is extracted from the live video and processed to detect faces and eye behaviour. The behavioural data collected includes the status of looking at the screen or exam paper, turning, and suspicious behaviour, calculated for each face detected in the frame. The detected faces are then enclosed in yellow bounding boxes.

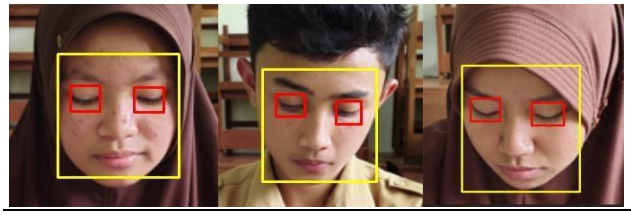

Figure 5: Visualization of face detection

The image above shows yellow bounding boxes surrounding detected faces. This detection yields several face coordinates, subsequently used for eye detection. Eye detection is performed using the Haar Cascade Classifier trained on an eye dataset. Detected eyes are enclosed in red bounding boxes for the extracted face frames.

B. Student Monitoring

After detecting faces and eyes, behaviour analysis determines whether the subject is focusing on the screen or exam paper, turning away, or exhibiting suspicious behaviour. This is achieved by examining the face's position relative to the video frame. If the face is at the bottom of the frame, it is considered focused; if it is at the sides of the frame, it is considered turning away or suspicious.

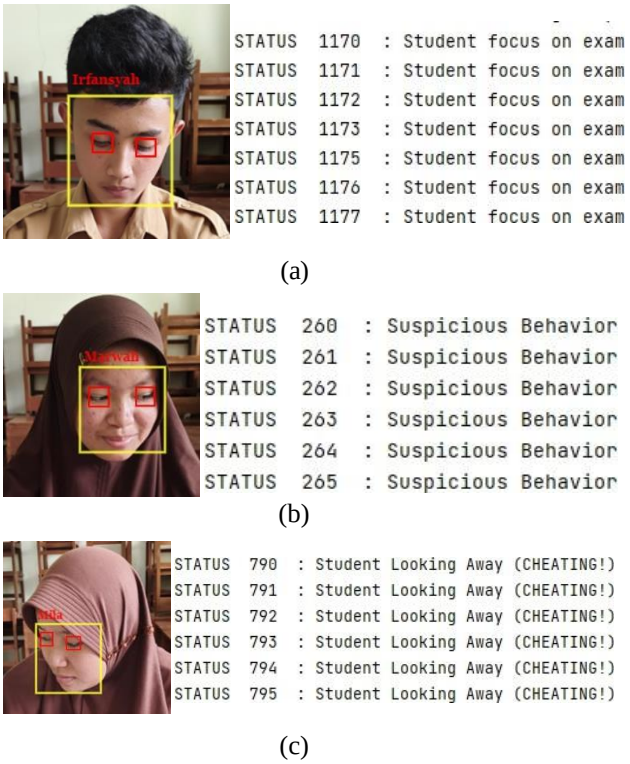

Figure 6. Student behaviour: (a) focused behaviour, (b) suspicious behaviour, (c) cheating behaviour

In Fig. 6(a), a student shows focused behaviour during the exam as our system analyzes the direction of the

eye gaze within the frame. Fig. 6(b) shows the system identifying suspicious behaviour marked by the student's gaze shifting away from exam-related content, raising concerns during monitoring. Fig. 6(c) indicates cheating behaviour detected by frequent and unauthorized glances around, suggesting possible information-seeking activities. This approach allows for real-time monitoring and detection of student behaviour during exams, providing valuable insights for academic integrity and supervision purposes.

C. Accuracy Result

This section explores the performance and precision of our system in detecting and categorizing student behaviour during exam scenarios, providing insights into the reliability and effectiveness of our facial analysis techniques for academic surveillance purposes.

TABLE III. First testing result

Student	Status / Behavior	System
1	Focus	Focus
2	Focus	Focus
3	Cheating	Cheating
4	Suspicious	Cheating
5	Focus	Focus
6	Suspicious	Suspicious
7	Cheating	Cheating
8	Suspicious	Suspicious
9	Focus	Focus
10	Cheating	Cheating

Based on Table III, depicting student behaviours and system classifications, we can analyze our system's accuracy of behaviour identification. These accuracy results indicate that while the system perfectly identifies focused and cheating behaviours, it needs to be more accurate for suspicious behaviour, correctly identifying two out of three cases. This analysis provides insights into the effectiveness and limitations of our behaviour monitoring system in the educational context.

In our study, misclassifying suspicious behaviour as cheating underscores the nuances of behaviour recognition in real-world contexts. Visual similarities in behaviours present challenges for algorithms trained to differentiate between complex behaviours, emphasizing the need for advanced modelling techniques and enriched training datasets to enhance accuracy.

D. Results of cheating detection

This section explores the performance and precision of our system in detecting and categorizing student behaviour during exam scenarios, providing insights into the reliability and effectiveness of our facial analysis techniques for academic surveillance purposes.

Table IV. Student Behavior Table

Student	Focus (%)	Suspicious (%)	Cheating (%)	Focus Duration (minutes)	Suspicious duration (minutes)	Cheating Duration (minutes)
1	11.8	33.7	54.5	14.16	40.44	65.40
2	24.7	52.1	23.2	29.64	62.52	27.84
3	92.1	5.2	2.7	110.52	6.24	3.24
4	36.4	53.5	10.1	43.68	64.20	12.12
5	88.4	7.8	3.8	106.08	9.36	4.56
6	27.3	21.7	51.0	32.76	26.04	61.20
7	26.4	14.5	59.1	31.68	17.40	70.92
8	71.2	21.3	7.5	85.44	25.56	9.00
9	86.7	9.4	3.9	104.04	11.28	4.68
10	39.3	50.1	10.6	47.16	60.12	12.72
11	90.5	6.2	3.3	108.60	7.44	3.96
12	81.3	11.9	6.8	97.56	14.28	8.16
13	31.2	53.4	15.4	37.44	64.08	18.48
14	22.5	17.5	60.0	27.00	21.00	72.00
15	75.8	14.2	10.0	90.96	17.04	12.00

In Table IV, significant variations in student behaviour during exams are shown. Focus behaviour is when students concentrate entirely on exam tasks without signs of distraction or suspicious behaviour. From the table above, Student 3 has the highest focus duration, spending 110.52 minutes of total exam time focused on their work, followed by Students 11 and 9 with 108.60 and 104.04 minutes, respectively. In contrast, Student 1 had the lowest focus duration, with only 14.16 minutes, indicating that they faced many distractions or engaged in suspicious or cheating behaviour for most of the exam time. Suspicious behaviour duration varies among students, with Students 2 and 4 showing relatively high times of 62.52 and 64.20 minutes. Conversely, Students 3 and 11 show shallow suspicious times of 6.24 and 7.44 minutes, respectively. This suggests that students with high suspicious durations may require additional supervision to ensure no cheating occurs.

Cheating behaviour is identified when students engage in activities that violate exam rules. The highest cheating duration is found in Students 14 and 7, with 72.00 and 70.92 minutes, respectively. This indicates that most of their exam time was spent on behavior not compliant with exam rules. On the other hand, Students 3 and 11 have the lowest cheating durations, each with 3.24 and 3.96 minutes, indicating they hardly engaged in cheating activities. The table data reveals that most students have high focus time and low cheating duration, as seen in Students 3, 11, and 9. However, some students show very high cheating behaviour patterns, such as Students 7 and 14, which require corrective actions to prevent future cheating.

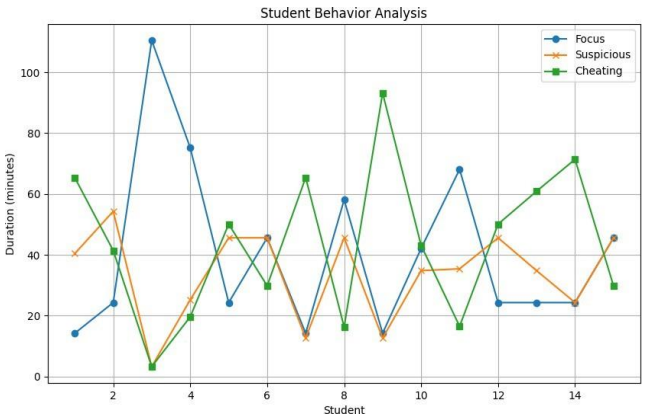

Figure 7: Time analysis graph

Figure 7. illustrates the x-axis representing each student, while the y-axis represents the duration of time (in minutes) spent in each behaviour. This graph provides a clear overview of how each student spent their time during the exam. Students 3 and 11 show very high focus durations (110.52 minutes and 108.60 minutes), indicating they spent most of their time in a focused state. Students 1, 6, and 7 show relatively high cheating durations (65.40 minutes, 61.20 minutes, and 70.92 minutes), indicating they spent most of their time in a cheating state. Students 2 and 10 show high suspicious behaviour durations (62.52 minutes and 60.12 minutes), suggesting they were often suspicious during the exam.

The line chart generated from this data reinforces these findings, clearly visualizing how students' behaviour durations vary during the exam. This analysis is essential for identifying students needing additional attention and developing more effective strategies for detecting and preventing exam cheating.

E. Analysis of Each Method's Results

The results of this study indicate that the SSD method can detect student faces with an accuracy rate of over 95% under good lighting conditions. However, detection accuracy decreases under low lighting conditions or if the student's face is partially covered. This indicates that SSD is very effective in an exam environment with adequate lighting but needs improvement under low-lighting conditions or visual obstructions such as masks or long hair. On the other hand, the Haar Cascade method can detect eyes with 90% accuracy. Eye detection is crucial for determining the direction of gaze and student eye behaviour, such as looking away or closing their eyes. Although Haar Cascade is quite adequate, this method has limitations in detecting partially closed eyes or in low lighting conditions. To improve accuracy, further feature recognition techniques could be applied. These eye detection results form the basis for further analysis of student behaviour during exams.

The behaviour analysis method calculates the percentage of time students spend in three behaviour categories: focused, suspicious, and cheating. The calculation is based on the duration of time spent on each behaviour during the exam. Behaviour analysis shows significant variations in student behaviour during exams. For example, students 3 and 11 spend most of their time in a focused state, while students 1, 6, and 7 show more suspicious or Cheating behaviour. A line chart is used to visualize the results of student behaviour analysis. This method helps in understanding the distribution of student behaviour during exams. The line chart shows the duration of focused, suspicious, and Cheating behaviours for each

E-mail address: ansharm20d@student.unhas.ac.id, zahir@unhas.ac.id, adywp@unhas.ac.id

student during the 120-minute exam. This chart provides a clear view of how each student spends time on various types of behaviour. Data visualization is beneficial in identifying students who need more attention and communicating the research results to related parties, such as exam proctors and educational institutions.

This study shows that combining face and eye detection methods with behaviour analysis can provide valuable insights into student behaviour during video-based exams. Although the methods used show promising results, some areas can be improved, such as detection accuracy under low lighting conditions and detecting more complex behaviours. By improving these methods, the system can become a more effective tool in detecting cheating and enhancing exam integrity.

5. CONCLUSION

This study proposes a combined method of face detection using a Single Shot Multibox Detector (SSD) and eye detection with Haar Cascade to develop a video-based exam monitoring system. This method detects student behaviours such as focus, suspicion, and cheating during exams. This approach differs from previous research on text-based cheating detection or computer usage patterns.

Based on the results, the proposed method performs well in detecting various student behaviours. Face detection using SSD achieved an accuracy rate of over 95% under adequate lighting conditions, while eye detection with Haar Cascade showed around 90% accuracy. The behaviour analysis revealed significant variations in student behaviour during exams, with some students showing higher levels of cheating than others.

This method demonstrates that combining face and eye detection can be an effective tool for video-based exam monitoring, providing in-depth insights into student behaviour. With the highest accuracy under ideal conditions, this system can be relied upon to detect cheating and assist exam proctors in maintaining exam integrity.

However, there is still room for further development, such as improving accuracy under low lighting conditions and implementing more advanced machine learning technologies to enhance system efficiency and effectiveness. With further development, this method could significantly contribute to exam monitoring and cheating detection, offering a more comprehensive and reliable solution than previous methods.

REFERENCES

[1] Zhou, Z., et al. (2023). "Improved Face Recognition System using Hybrid Deep Learning Techniques." IEEE Transactions on Neural Networks and Learning Systems.

[2] Nguyen, T., & Lee, D. (2022). "Real-time Cheating Detection in Online Exams using Advanced Pose Estimation and Machine Learning." Computers & Education.

[3] Kim, J., & Park, H. (2024). "Adaptive YOLO-based Algorithm for Detecting Unusual Behaviors in Exam Settings." Journal of Visual Communication and Image Representation.

[4] Wang, S., et al. (2023). "Emotion Recognition through Facial Expression Analysis for Enhanced Human-Machine Interaction." International Journal of Computer Vision.

[5] Li, X., & Zhao, Y. (2022). "Enhanced Real-time Face and Body Tracking for Cheating Detection Using Optical Flow and Neural Networks." Pattern Recognition Letters.

[6] Zhang, Y., & Yang, Q. (2023). "Deep Learning Approaches for Real-time Facial Recognition in Security Systems." IEEE Access.

[7] Garcia, R., & Lopez, J. (2024). "Integrating Multi-modal Data for Improved Online Exam Monitoring." Journal of Educational Technology & Society.

[8] Huang, L. et al. (2022). "Pose-guided Human Action Recognition for Online Examination Surveillance." Neurocomputing.

[9] Lee, C., & Chen, H. (2023). "Advanced Deepfake Detection Techniques for Ensuring Integrity in Online Assessments." Expert Systems with Applications.

[10] Zhu, X., Ramanan, D. "Face Detection, Pose Estimation, and Landmark Localization in the Wild." IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2012.

[11] Jiang, H., Learned-Miller, E. "Face Detection with the Faster R-CNN." IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017.

[12] Hochreiter, S., Schmidhuber, J. "Long Short-Term Memory". Neural Computation, 1997.

[13] Redmon, J., Farhadi, A. "YOLOv3: An Incremental Improvement". arXiv preprint arXiv:1804.02767, 2018.

[14] Ekman, P., Friesen, W. V. "Facial Action Coding System: A Technique for the Measurement of Facial Movement". Consulting Psychologists Press, 1978.

[15] Viola, P., Jones, M. "Robust Real-Time Face Detection." International Journal of Computer Vision, 2004.

[16] Al Airaji, A., Abasi, M. "A Novel Approach to Cheating Detection Using OpenPose." Journal of Advanced Computer Science and Technology, 2021.

[17] Cao, Z., Hidalgo, G., Simon, T., Wei, S. E., Sheikh, Y. "OpenPose: Real-time Multi-Person 2D Pose Estimation using Part Affinity Fields". IEEE Transactions on Pattern Analysis and Machine Intelligence, 2019.

[18] Sun, C., Akagi, Y. "Abnormal Behavior Detection for Escalator Passengers Using Optical Flow and Random Forests." Proceedings of the International Conference on Image Processing, 2019.

Muhajir Anshar and his short biography, is a graduate student of Informatics Engineering at Hasanuddin University Makassar, Indonesia. His research interests focus on Convolutional Neural Networks (CNN).

Zahir Zainuddin is an Associate Professor in the Department of Informatics Engineering, Faculty of Engineering, Hasanuddin University, Indonesia. He holds a Doctorate in Electrical Engineering from Institut Teknologi Bandung (2005), a Master in Computer Engineering from Florida Institute of Technology, USA (1995), and a Bachelor in Electrical Engineering from Universitas Hasanuddin (1988). Since joining Universitas Hasanuddin in 1989, he has led research projects on innovative city applications, autonomous vehicle technology, and digital rural information services. His publications are indexed in Scopus and include research on automatic feeding systems, road detection for autonomous cars, and face recognition performance. He is a member of IEEE and the Association for Higher Education in Informatics and Computing.

Ady Wahyudi Paundu is a lecturer in the Department of Informatics, Faculty of Engineering, Universitas Hasanuddin, Indonesia. He earned his Doctorate in Informatics (Computer Security) from NAIST Japan in 2018, his Master's in Informatics (Computer Network) from Universitas Hasanuddin in 2009, and his Bachelor's in Informatics from STT Telkom Bandung in 1999. His research focuses on web-based academic performance evaluation systems and detecting Distributed Denial of Service attacks using Extreme Learning Machine methods. He has published several papers in the "Security and Communication Networks" journal and the 2018 International Conference on Internet of Things and Intelligence Systems (IOTAIS). Since 2009, he has actively contributed to teaching and research at Universitas Hasanuddin.