AI-YOLO Based Smart Laboratory Security for Automated Face Recognition and Suspicious Activity Detection

Nurul Khaerani Hamzidah [1]*, Syahrir [2]*, Ainun Jariyah [3]*, Carlos Agunar Da Costa [4]*, Sitti Saenab [5]*, Dul Arafat Muin [6]*, Nur Ichzan As [7]*
* Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Ujung Pandang
nkhamzidah@poliupg.ac.id [1], syahrir@poliupg.ac.id [2], ainunjariyah@poliupg.ac.id [3], agunardacosta2004@gmail.com [4], sittisaenab046@gmail.com [5], dularafat@gmail.com [6], nurichzanas@poliupg.ac.id [7]

Article Info

Article history:

Received 2025-12-04
Revised 2026-01-14
Accepted 2026-01-30

Keyword:

AI-YOLO,
Face Recognition,
MediaPipe Pose,
Laboratory Security,
Smart Campus.

ABSTRACT

Ensuring laboratory security is a critical consideration within campus environments to effectively prevent theft and suspicious activities. Traditional CCTV systems predominantly rely on manual monitoring, resulting in delayed responses to incidents. This research seeks to develop and implement an Artificial Intelligence (AI)-based laboratory security system, integrating three primary models: YOLOv5 for human object detection, Face Recognition for individual identification, and Media Pipe Pose for real-time analysis of suspicious movements. The system is designed as a Flask-based monitoring website, which displays activity logs, detected individual identities, and automated notifications based on image processing results on a Raspberry Pi connected to CCTV cameras. The research methodology employs an applied experimental approach, encompassing stages such as system design, face dataset collection, data encoding utilizing the Face Recognition Library, and performance evaluation under two lighting conditions (bright and dark) and three distance variations. The test results indicate that the Face Recognition method operates optimally at a distance of 2 meters in bright lighting conditions, achieving an accuracy of up to 92%. However, its performance declines at distances exceeding 3 meters and under low-light conditions. Conversely, MediaPipe Pose exhibits high stability, with an average accuracy of 94% in bright conditions and 89% in dark conditions, and is capable of transmitting real-time notifications for activities such as lifting objects or placing hands into pockets. The AI-based laboratory security system developed has demonstrated effectiveness, adaptability, and responsiveness in the automatic detection of identities and suspicious activities. The integration of YOLO v5, Face Recognition, and MediaPipe Pose models offers an intelligent and efficient security solution that facilitates the implementation of the Smart Campus concept within educational environments.

I. Introduction

Ensuring security within university campuses, particularly in laboratory environments, is a critical concern that requires careful and systematic attention. Laboratories typically contain valuable research equipment and sensitive materials, making them vulnerable to theft, misuse, or damage caused by human negligence. The high intensity of activities involving students and staff further increases the likelihood of suspicious behaviors that may compromise safety and disrupt the academic environment. Conventional surveillance systems, such as passive Closed-Circuit Television (CCTV), rely heavily on manual monitoring, which often leads to delayed responses and reduced effectiveness in incident handling. Consequently, there is an urgent demand for intelligent security systems capable of autonomously detecting suspicious activities in real time [1], [2], [3], [4].

Recent advancements in artificial intelligence (AI) have significantly contributed to the development of more adaptive and efficient surveillance systems. By integrating AI into CCTV-based monitoring, surveillance systems can evolve from passive recording tools into intelligent platforms capable of analyzing human behavior patterns and automatically identifying potential threats. Previous studies have demonstrated the feasibility of AI-based laboratory security systems, such as Internet of Things (IoT) solutions integrating ESP32-CAM, Firebase, and instant notification services, achieving face recognition accuracy of up to 90% under optimal conditions[4], [5], [6], [7]. However, these systems are primarily limited to face-based access control and do not incorporate behavioral analysis or the detection of more complex suspicious activities within laboratory environments [8], [9].

Several recent studies indicate that integrating object detection with human pose estimation can enhance contextual understanding of human behavior in surveillance systems. Kothari et al. combined YOLO and MediaPipe Pose to detect fall events in real time, demonstrating that body pose analysis is effective for recognizing abnormal activities in controlled environments [4], [5], [10]. Similarly, Zhang et al. utilized YOLOv5 and MediaPipe for keypoint-based human motion monitoring with high accuracy in real-time scenarios [5], [11]. Despite their effectiveness, these approaches do not integrate identity recognition, which is essential for access control and accountability. Furthermore, studies on Smart CCTV systems in campus environments reveal that object-based detection alone is insufficient to accurately assess security risks without incorporating behavioral context analysis [12][4], [5].

Based on these limitations, there is a clear research gap in the development of a comprehensive laboratory security system that integrates identity recognition with real-time behavioral analysis. To address this gap, this study proposes an artificial intelligence-based laboratory security system that integrates YOLOv5, Face Recognition, and MediaPipe Pose. YOLOv5 is employed to rapidly detect human presence and objects using a CCTV camera connected to a Raspberry Pi, enabling efficient real-time automated surveillance [13], [14]. Face Recognition is utilized to distinguish between registered and unregistered individuals, while MediaPipe Pose analyzes human body movements to identify suspicious behaviors based on contextual motion patterns.

The primary objective of this research is to design and implement an intelligent laboratory security system capable of detecting human presence, recognizing authorized and unauthorized individuals, and automatically identifying suspicious movements in real time [15]. The proposed system is expected to enhance surveillance effectiveness, reduce dependence on manual monitoring, and support the realization of a secure and intelligent Smart Campus environment [3], [16]. In addition to its technical contributions, this study is anticipated to provide practical benefits for educational institutions by strengthening laboratory security through integrated, data-driven surveillance, while also offering experiential learning opportunities for students in the application of artificial intelligence and intelligent monitoring systems [3][4], [7], [17].

II. Method

This study employs an applied experimental methodology to develop and evaluate an Artificial Intelligence (AI)-based laboratory security system. The system is engineered to detect faces and identify suspicious activities in real-time by utilizing a combination of three models: YOLO v5 for human object detection, Face Recognition for facial identification, and MediaPipe Pose for body movement analysis. The system operates on a Raspberry Pi device connected to a webcam and is presented through a web dashboard interface developed using Flask.

The laboratory security system developed comprises several key components that are integrated, as illustrated in Figure 1 System Architecture Design. These components include a camera (webcam) that captures real-time video, serving as the primary source for analysis. A Raspberry Pi is employed to operate artificial intelligence models such as YOLO v5, Face Recognition, and MediaPipe Pose, while also managing connectivity to the web server. Additionally, a server or database is utilized to store user data, surveillance activity logs, and detection results. The internet network facilitates the connection between the Raspberry Pi, server, and monitoring dashboard, enabling synchronous system operation. Detection results are displayed via the website or monitoring dashboard, providing real-time incident logs and visual evidence of suspicious activity. Through the integration of these components, the system operates automatically, encompassing image acquisition, face detection, body pose analysis, and notification transmission to the web dashboard. Consequently, it can identify known and unknown users, detect suspicious actions such as lifting objects or concealing items, and record them as digital evidence logs.

In Figure 2, the operational sequence of the laboratory monitoring system is initiated upon the activation of the webcam, which continuously captures video frames. Each frame undergoes analysis via the YOLO v5 model to ascertain the presence of individuals within the monitored environment. In the absence of detected individuals, the system continues its monitoring function. Conversely, upon detection of an individual, the system advances to the facial recognition phase to compare the detection results with the database. Faces that are registered will have their corresponding names displayed, whereas unregistered faces are designated as "Unknown." Subsequently, the system employs MediaPipe Pose to scrutinize body movements and identify potentially suspicious activities, such as lifting, moving objects, or placing items into a pocket. Upon detection of such activities, the system automatically archives the frame as evidence, records the timestamp, and logs the real-time identity of the individual involved on the dashboard website. This process persists until the system is manually deactivated by the administrator.

A. *Face Dataset Processing Procedure*

This study employs a facial dataset to facilitate the development of a face detection and recognition system. The integration of this dataset is essential as it enhances laboratory room security by enabling the system to not only detect objects or potential physical threats but also to identify individuals who are either authorized or unauthorized to access the room. Consequently, the security of the laboratory is comprehensively maintained, encompassing both activity monitoring and personal accessibility.

In Figure 3, the collection of facial datasets was carried out by directly involving participants from the laboratory environment. A total of 55 individuals were successfully collected, consisting of 45 student facial data and 10 facial data from lecturers and laboratory technicians. The selection of these two participant groups was deliberately made to represent the actual laboratory users, where students act as daily users, while lecturers and technicians are those with higher authority and access rights.

In Figure 4, data collection is conducted utilizing a smartphone camera with a 4:3 resolution and High Definition (HD) quality. Each participant contributes a single facial sample to ensure data consistency and reduce redundancy. Despite the provision of only one sample per individual, the collection process considers lighting conditions, a front-facing angle, and facial expressions. This approach is designed to meet the requirements of the data processing stage employing the faces recognation method.

B. *Face Dataset Encoding Process*

Upon completion of the data collection process, the facial dataset undergoes further processing utilizing the Dlib library in conjunction with the face recognition library. This procedure, referred to as face encoding, entails the transformation of facial images into a unique numerical representation, or embedding, for each individual. The encoding is performed sequentially for the facial data of all participants, ensuring that each individual is assigned a distinct numerical code that functions as a digital identity. The encoding process can be seen in Figure 5.

The encoding results are subsequently stored in a database under the file name encodings cache.pkl to facilitate the Face Recognition system. During system operation, facial images captured by the CCTV are compared with the stored encoding data. Upon identifying a match, the system recognizes the individual as an authorized user. For students, the system displays a label containing their name and student ID number (NIM), whereas for lecturers, it displays their name and employee ID number (NIP). Conversely, if no match is detected, the system issues an alert or records the activity as suspicious by identifying the face as unknown (an unidentified person).

C. *Suspicious Movement Data Processing*

The detection of suspicious movements utilizing the MediaPipe Pose model initiates with the extraction of body keypoints to acquire stable landmark data. Following the acquisition of this data, the system undertakes body scale normalization by calculating the distance between the shoulders, which serves as a reference for determining the analysis regions, such as the pocket area and lifting area. The analysis of the pocket area is conducted by examining the relationship between the wrist position and the hip point. If the left wrist is detected on the lower left side of the left hip within a specified radius, the system identifies this as an activity of inserting an object into the left pocket, with a similar condition applicable to the right side.

The subsequent phase entails an analysis of the photographic area by assessing whether both wrists are positioned between the waist and chest height. When both hands are proximate within this region, the system categorizes the activity as either lifting or moving an object. The outcomes of this analysis are subsequently processed during the decision-making phase to produce outputs in the form of labels indicating suspicious movements, such as activities involving lifting or inserting objects into a pocket.

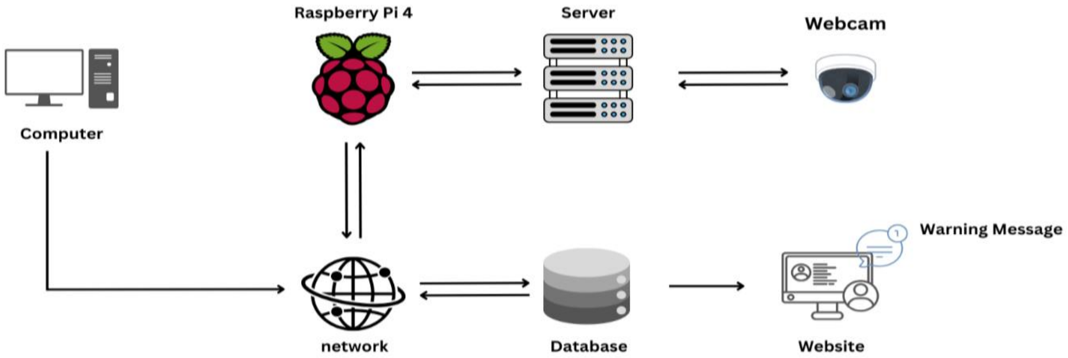


Figure 1. System Architecture Design

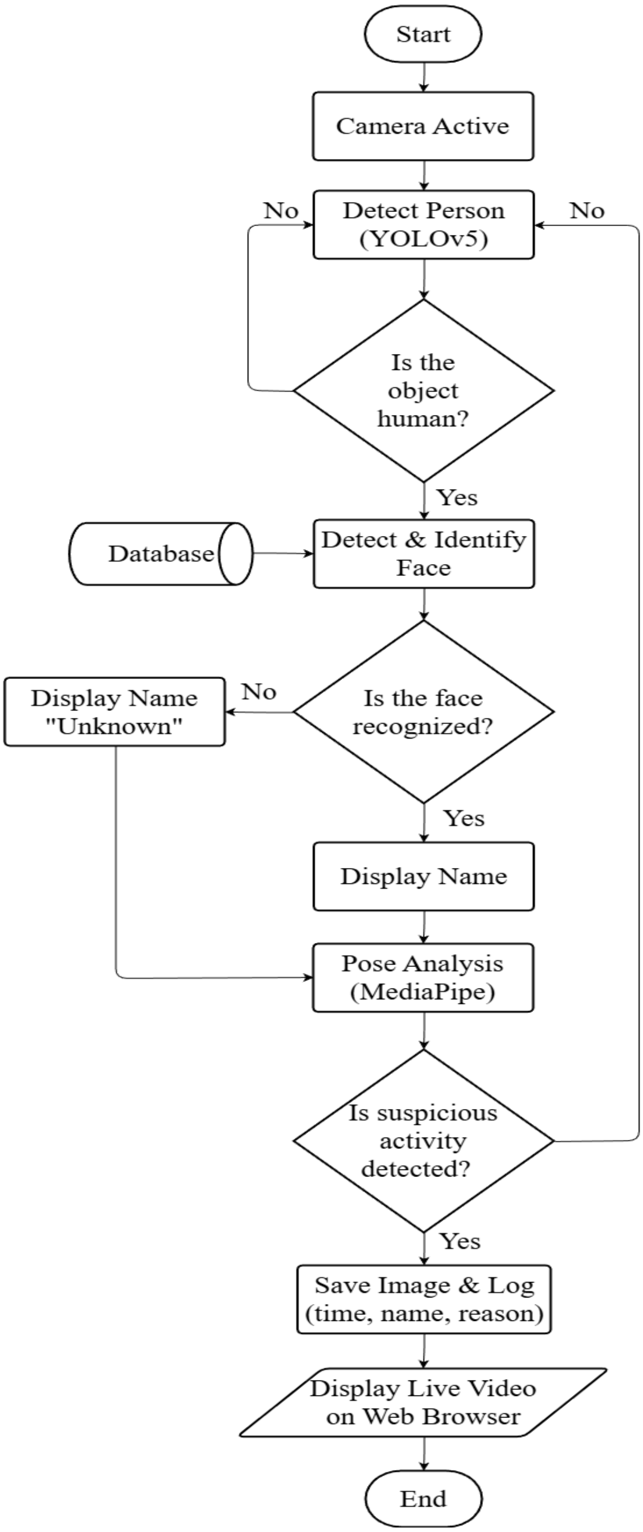


Figure 2. System Architecture Design

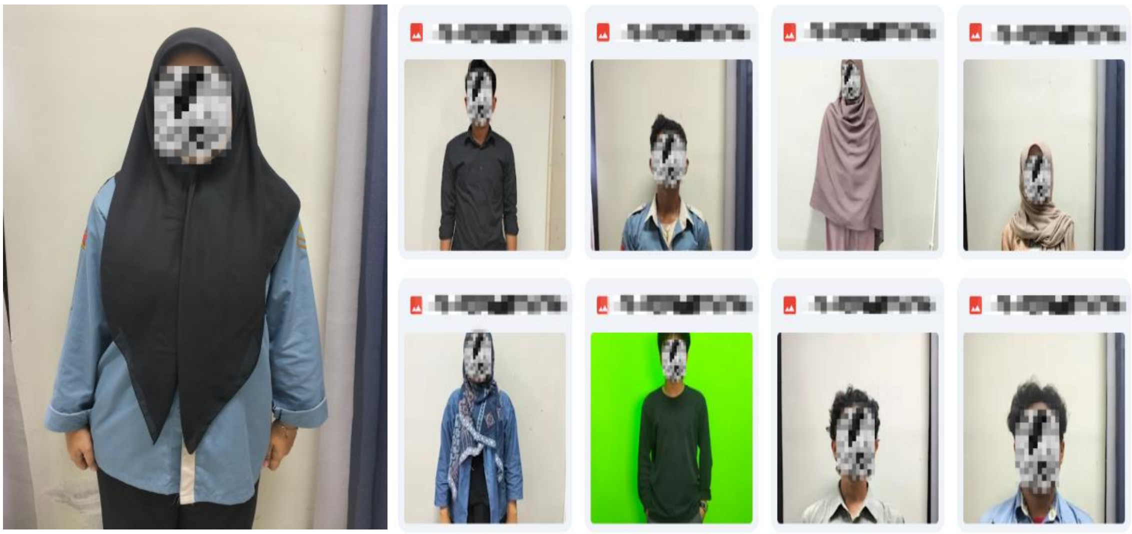


Figure 3. Dataset Collection Process

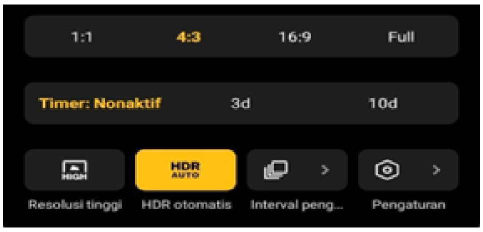


Figure 4. Camera Ratio Used in Dataset Collection

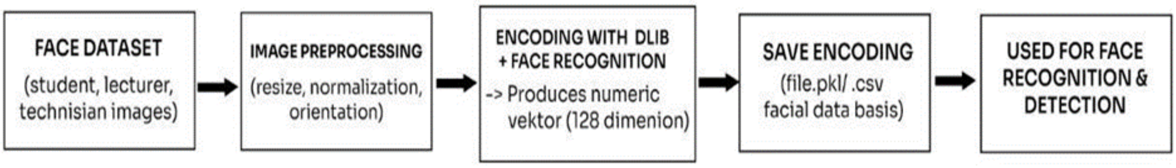

FACE DATASET
(student, lecturer, technisian images)
IMAGE PREPROCESSING
(resize, normalization, orientation)
ENCODING WITH DLIB + FACE RECOGNITION
-> Produces numeric vektor (128 dimenion)
SAVE ENCODING
(file.pkl/ .csv facial data basis)
USED FOR FACE RECOGNITION & DETECTION

Figure 5 Process Flow Diagram for Encoding Face Dataset

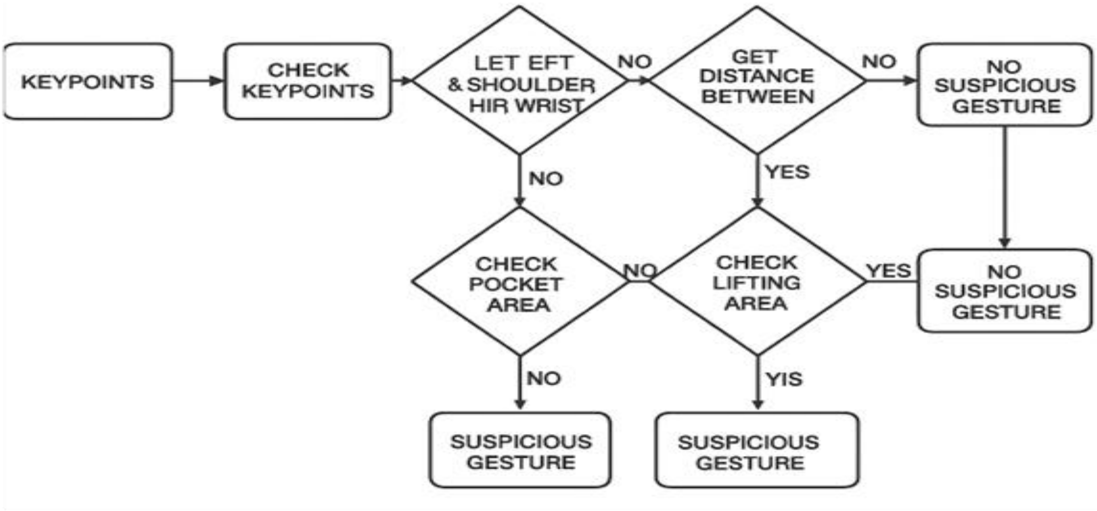


Figure 6 Flowchart of Suspicious Gesture Processing

III. Results and Discussion

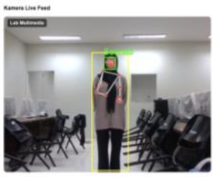
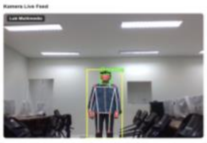
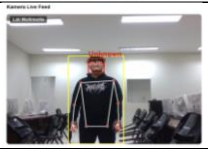
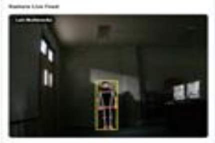
A. Face Recognition Detection

Face recognition testing was conducted to assess the system's capability to identify faces under varying lighting conditions, including both bright and low lighting, as well as at different distances of 2 meters, 3 meters, and 5 meters. Each test scenario was documented based on the correspondence between the detected label and the actual label, in addition to whether the system successfully displayed a bounding box around the detected face. The objective of this test is to evaluate the system's optimal functionality in real-world scenarios within the campus laboratory environment.

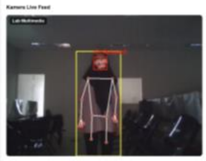
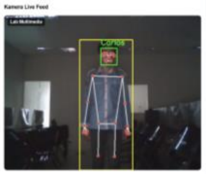
B. Pose Detection Media for Suspicious Movements

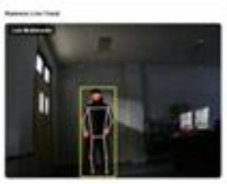
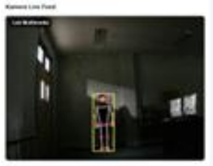
The testing of the Pipe Pose Media focused on detecting suspicious movements, such as lifting or moving objects, as well as putting hands or items into trouser pockets. The tests were conducted under two lighting conditions (bright lighting and low lighting) and at various distances (2 meters, 3 meters, and 5 meters) to ensure the system could accurately detect these types of movements. Each detection that falls under the suspicious category will trigger the real-time sending of notifications to the monitoring system. The aim of this test is to ensure the system's reliability in promptly and efficiently detecting suspicious activities in the laboratory environment.

TABEL I
RESULTS OF FACE RECOGNITION TESTING UNDER BRIGHT-LIGHTING CONDITIONS

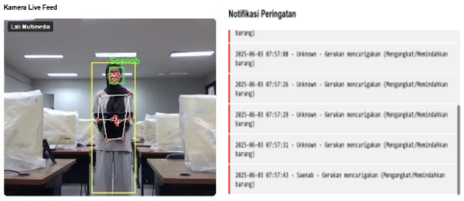
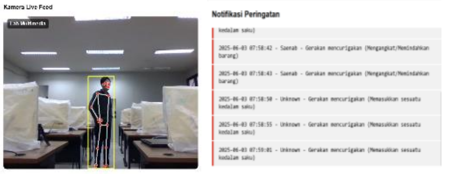
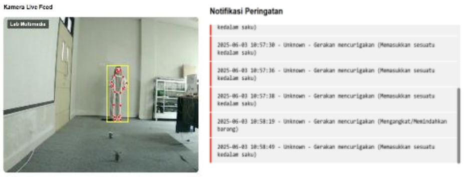
Capture Result	Result Label	Original label	Distance (meters)	Description
	“Saenab”	“Saenab”	2.00	the system successfully detected the face accurately according to the original label and displayed the bounding box at a distance of 2 meters
	“Carlos	Carlos”	3.00	the system successfully detected faces correctly according to the original labels and displayed the bounding box at a distance of 3 meters
	unknown	unknown	2.00	the system successfully detected "unknown" and displayed a bounding box at a distance of 2 meters
	bounding box not showing	unknown	5.00	the system does not display a bounding box, but the face is automatically detected as "unknown" at a distance of 5 meters

TABEL II
RESULTS OF FACE RECOGNITION TESTING IN LOW-LIGHT CONDITIONS

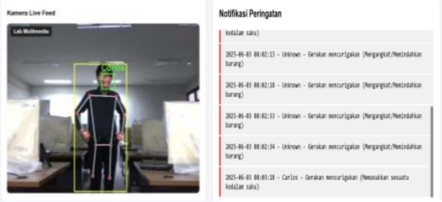
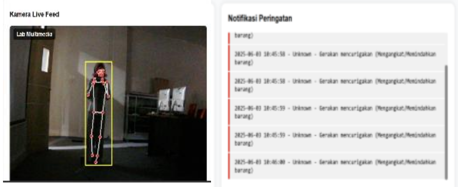
Capture Result	Result Label	Original label	Distance (meters)	Description
	unknown	“Saenab”	2.00	the system detects the face as unknown at a distance of 2 meters because the room is dark, making it difficult for the face to be recognized properly
	“Carlos”	“Carlos”	2.00	the system successfully detected faces according to their original labels at a distance of 2 meters, even in low-light conditions

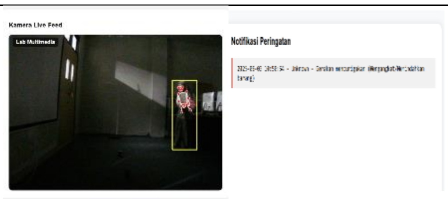
	without bounding box	unknown	3.00	the system does not display a bounding box, but the face is automatically detected as "unknown" at a distance of 3 meters
	without bounding box	unknown	5.00	the system does not display a bounding box, but faces are automatically detected as "unknown" at a distance of 5 meters

TABEL III
MEDIAPIPE POSE TEST RESULTS FOR SUSIPICIOUS MOVEMENTS IN WELL-LIT ROOM CONDITIONS

Type of Movement	**Detection Result**	**Distance (meters)**	**Description**
moving item	 Notifikasi Peringatan barang) 2025-06-03 07:57:08 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 07:57:26 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 07:57:29 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 07:57:31 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 07:57:43 - Saenab - Gerakan mencurigakan (Mengangkat/Memindahkan barang)	2.00	the system successfully detected suspicious movement (lifting/moving items) at a distance of 2 meters and sent a notification
putting something into a pocket	 Notifikasi Peringatan kedalam saku) 2025-06-03 07:58:42 - Saenab - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 07:58:43 - Saenab - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 07:58:50 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku) 2025-06-03 07:58:55 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku) 2025-06-03 07:59:01 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)	3.00	the system successfully detected suspicious movement (putting something into a pocket) at a distance of 3 meters and sent a notification
putting something into a pocket	 Notifikasi Peringatan kedalam saku) 2025-06-03 10:57:30 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku) 2025-06-03 10:57:36 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku) 2025-06-03 10:57:38 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku) 2025-06-03 10:58:19 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 10:58:49 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)	5.00	the system successfully detected suspicious movement (putting something into a pocket) at a distance of 5 meters and sent a notification

TABEL IV
MEDIAPIPE POSE TEST RESULTS FOR SUSIPICIOUS MOVEMENTS IN DARK ROOM CONDITIONS

Type of Movement	**Detection Result**	**Distance (meters)**	**Description**
Putting something into a pocket	 Notifikasi Peringatan kedalam saku) 2025-06-03 08:02:13 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 08:02:18 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 08:02:33 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 08:02:34 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 08:03:18 - Carlos - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)	2.00	The system successfully detected suspicious movement (lifting/moving items) at a distance of 2 meters and sent a notification
moving items	 Notifikasi Peringatan barang) 2025-06-03 10:45:58 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 10:45:58 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 10:45:59 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 10:45:59 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang) 2025-06-03 10:46:00 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)	3.00	The system successfully detected suspicious movement (putting something into a pocket) at a distance of 3 meters and sent a notification

moving items	 Kamera Live Feed Lab Multimedia Notifikasi Peringatan 2025-05-08 19:58:54 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)	5.00	The system successfully detected suspicious movement (putting something into a pocket) at a distance of 5 meters and sent a notification

The laboratory security system developed in this study incorporates two primary models: Face Recognition for the identification of individuals and MediaPipe Pose Estimation for the real-time detection of suspicious movements. The system's performance was evaluated through testing at various distances (2 m, 3 m, and 5 m) and under two lighting conditions (bright and dark) to assess its responsiveness to changes in viewing distance and light intensity within the laboratory environment.

In face recognition evaluations conducted under well-lit conditions, the system demonstrated the capability to accurately detect registered individuals, such as "Saenab" and "Carlos," by displaying distinct bounding boxes at close proximity. At intermediate distances, the system maintained effective identification, albeit with a marginally increased detection time. Conversely, at extended distances, the bounding box failed to manifest, resulting in the system classifying faces merely as "Unknown." Under low-light conditions, system performance deteriorated due to insufficient illumination, which compromised the clarity of facial features. While face detection remained feasible at close range, the system frequently failed to accurately recognize identities at medium to long distances.

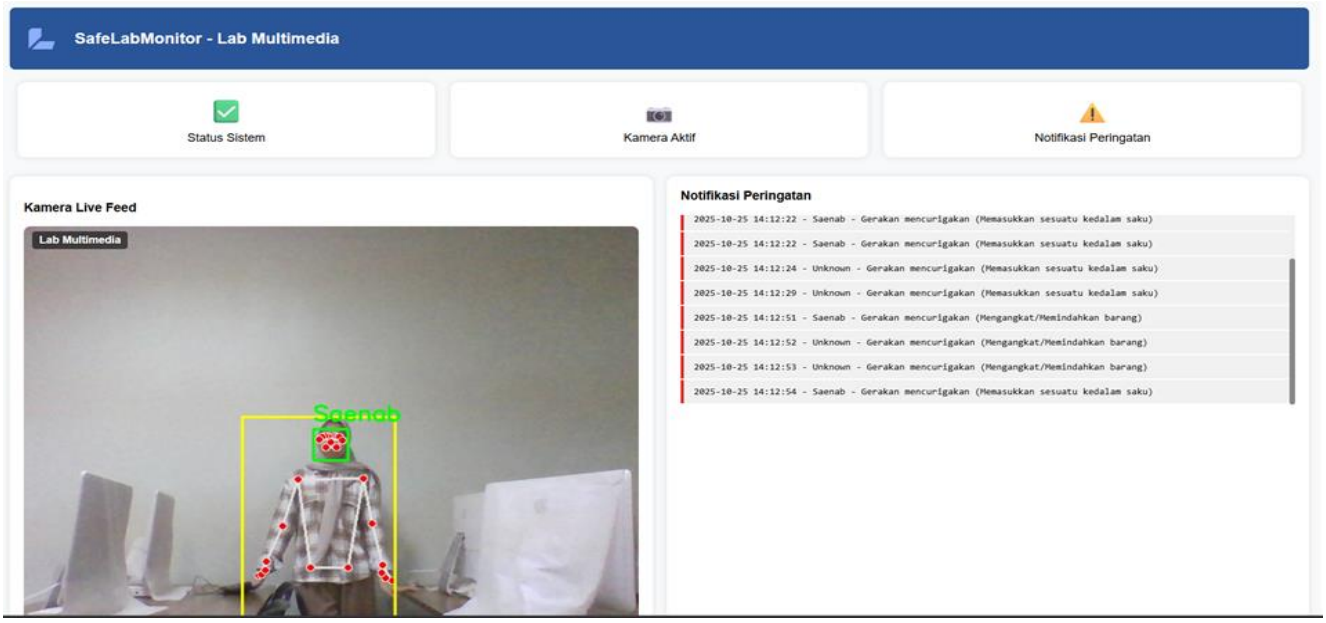
MediaPipe Pose Estimation exhibited consistently stable performance across a range of distances and lighting conditions. The system reliably detected suspicious movement patterns, such as the lifting or moving of objects and the placement of hands inside pockets, in both well-lit and dim environments. Furthermore, the system maintained a rapid response time, enabling real-time notifications even when objects were positioned at greater distances from the camera [4], [5].

Optimal system performance was attained at a distance of two meters under bright lighting conditions, where both methods operated synergistically, facilitating rapid and stable detection. MediaPipe Pose Estimation demonstrated greater adaptability to variations in distance and low lighting conditions compared to Face Recognition, thereby establishing itself as a critical component in ensuring the effectiveness and reliability of the laboratory security system.

C. Real-Time Detection

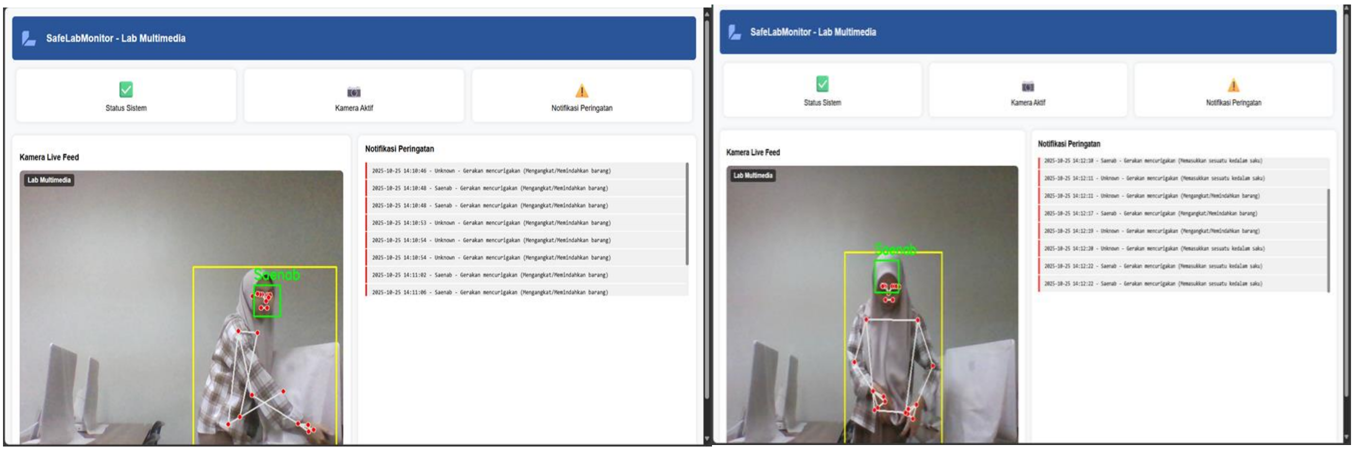
The developed laboratory security system is engineered to function in real-time, facilitating simultaneous and continuous processes of facial detection and suspicious activity monitoring. By integrating YOLO v5, Face Recognition, and MediaPipe Pose models, the system is capable of visually analyzing each video frame received directly from the camera. Facial detection is executed by comparing captured images against a registered face dataset, with the system automatically displaying bounding boxes and corresponding individual identities on the monitoring interface. Should a face not detected in the database be encountered, the system will automatically classify it as "Unknown" and document it in the activity log [5], [7].

Furthermore, the system employs MediaPipe Pose to monitor bodily movements, identifying suspicious activity patterns such as lifting objects, relocating items, or placing hands into pockets. Upon detection of any such movement patterns, the system automatically dispatches real-time warning notifications, which are displayed on the Flask-based website dashboard. These notifications are accompanied by the time of the incident and captured images serving as visual evidence. This mechanism enables supervision processes in laboratory environments to operate intelligently, adaptively, and responsively without requiring manual intervention from operators, thereby facilitating the implementation of real-time AI-based security monitoring concepts. Realtime detection testing can be seen in Figure 7 and Figure 8 This testing consists of realtime face identification detection testing and realtime suspicious movement identification detection testing [6], [7], [17].



```
2025-10-25 14:12:22 - Saenab - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
2025-10-25 14:12:22 - Saenab - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
2025-10-25 14:12:24 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
2025-10-25 14:12:29 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
2025-10-25 14:12:51 - Saenab - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:12:52 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:12:53 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:12:54 - Saenab - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
```

Figure 7 Real-Time Face Identification Detection Testing



```
2025-10-25 14:10:46 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:10:48 - Saenab - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:10:48 - Saenab - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:10:53 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:10:54 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:10:54 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:11:02 - Saenab - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:11:06 - Saenab - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
```

```
2025-10-25 14:12:10 - Saenab - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
2025-10-25 14:12:11 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
2025-10-25 14:12:11 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:12:17 - Saenab - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:12:19 - Unknown - Gerakan mencurigakan (Mengangkat/Memindahkan barang)
2025-10-25 14:12:20 - Unknown - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
2025-10-25 14:12:22 - Saenab - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
2025-10-25 14:12:22 - Saenab - Gerakan mencurigakan (Memasukkan sesuatu kedalam saku)
```

Figure 8 Real Time Detection Testing to Identify Suspicious Movements

IV. CONCLUSION

The laboratory security system developed has effectively integrated two primary methodologies Face Recognition and MediaPipe Pose estimation into a cohesive real-time monitoring mechanism. The Face Recognition technique is employed to identify individuals based on facial images, while MediaPipe Pose estimation is utilized to detect suspicious movement patterns, such as lifting items, moving objects, or placing hands into pockets.

Performance evaluation results indicate that the system attains optimal functionality at a distance of 2 meters under bright lighting conditions, facilitating rapid and precise detection of both facial features and suspicious movements. The face recognition method demonstrates the highest accuracy in bright, close-range scenarios, achieving a value of 92%. This accuracy diminishes to 78% at medium range and becomes unstable at distances exceeding 5 meters. In low-light conditions, system performance deteriorates, with an average accuracy of 65%, attributed to lighting limitations that adversely affect the discernibility of facial features.

In contrast, the MediaPipe Pose estimation method exhibits a more stable performance, achieving an average accuracy of 94% under well-lit conditions and 89% in low-light environments. The system consistently detects suspicious movements across various distances and delivers real-time notifications with minimal response time.

In summary, this AI-driven laboratory security system has demonstrated efficacy, adaptability, and responsiveness in identifying both individuals and suspicious activities within the laboratory setting. The integration of Face Recognition and MediaPipe Pose Estimation significantly enhances computer vision-based security in research environments.

References

[1] S. Yao *et al.*, "From Lab to Field: Real-World Evaluation of an AI-Driven Smart Video Solution to Enhance Community Safety," Aug. 2023, doi: 10.1016/j.iot.2025.101716.

[2] L. Ali, F. Alnajjar, M. M. A. Parambil, M. I. Younes, Z. I. Abdelhalim, and H. Aljassmi, "Development of YOLOv5-Based Real-Time Smart Monitoring System for Increasing Lab Safety Awareness in Educational Institutions," *Sensors*, vol. 22, no. 22, Nov. 2022, doi: 10.3390/s22228820.

[3] M. Janapati, L. P. Allamsetty, T. T. Potluri, and K. V. Mogili, "Gait-Driven Pose Tracking and Movement Captioning Using OpenCV and MediaPipe Machine Learning Framework," *Engineering Proceedings*, vol. 82, no. 1, 2024, doi: 10.3390/ecsa-11-20470.

[4] W. Zhang *et al.*, "Combined MediaPipe and YOLOv5 range of motion assessment system for spinal diseases and frozen shoulder," *Sci Rep*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-66221-8.

[5] A. S. Dileep, S. S. Nabilah, S. Sreeju, K. Farhana, and S. Surumy, "Suspicious Human Activity Recognition using 2D Pose Estimation and Convolutional Neural Network," in *2022 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 19–23. doi: 10.1109/WiSPNET54241.2022.9767152.

[6] C. W. Wahome, G. Ling, and L. Ma, "Multi-modal fall detection using improved YOLOv5 and mediapipe," in *ASIG 2024 - Proceedings of the 2nd Asia Symposium on Image and Graphics*, Association for Computing Machinery, Inc, Apr. 2025, pp. 29–35. doi: 10.1145/3718441.3718446.

[7] V. P. Kothari and P. S. Chakurkar, "Towards safer environments: A YOLO and MediaPipe-based human fall detection system with alert automation," *MethodsX*, vol. 15, Dec. 2025, doi: 10.1016/j.mex.2025.103623.

[8] S. Malaikrisanachalee, N. Wongwai, and E. Kowcharoen, "ESPCN-YOLO: A High-Accuracy Framework for Personal Protective Equipment Detection Under Low-Light and Small Object Conditions," *Buildings*, vol. 15, no. 10, May 2025, doi: 10.3390/buildings15101609.

[9] B. R. Ardabili *et al.*, "Understanding Policy and Technical Aspects of AI-enabled Smart Video Surveillance to Address Public Safety," *Computational Urban Science*, vol. 3, no. 1, Dec. 2023, doi: 10.1007/s43762-023-00097-8.

[10] Y. M. Manu, S. V. Shashikala, N. Darshan, A. P. Dheeraj, N. J. Hemanth, and N. B. Gowda, "Smart Surveillance Camera Using AI," in *2nd IEEE International Conference on Advances in Information Technology, ICAIT 2024 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ICAIT61638.2024.10690287.

[11] M. Sujkowski, J. Kozuba, P. Uchronski, A. Banas, P. Pulit, and L. Gryzewska, "Artificial Intelligence Systems for Supporting Video Surveillance Operators at International Airport," in *Transportation Research Procedia*, Elsevier B.V., 2023, pp. 1284–1291. doi: 10.1016/j.trpro.2023.11.273.

[12] O. E. Putra, R. Devita, and N. Wahyudi, "Safe Security System Using Face Recognition Based on IoT," *SinkrOn*, vol. 8, no. 2, pp. 1021–1030, 2023, doi: 10.33395/sinkron.v8i2.12231.

[13] N. Afiyat and G. Mubtadi, "Rancang Bangun Sistem Keamanan Laboratorium Menggunakan Face Recognition Berbasis Internet of Thing (IoT)," *QOMARUNA Journal of Multidisciplinary Studies*, vol. 2024, no. 01, pp. 20–41, 2024.

[14] Noel Ipe Johnson, Jereena John, and Dalbina Dalan, "Artificial Intelligence in Surveillance Camera," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 28–32, Jun. 2022, doi: 10.48175/ijarsct-4904.

[15] H. Sabit, "Artifical Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications," *Electronics (Switzerland)*, vol. 14, no. 3, Feb. 2025, doi: 10.3390/electronics14030608.

[16] S. Dill *et al.*, "Accuracy Evaluation of 3D Pose Reconstruction Algorithms Through Stereo Camera Information Fusion for Physical Exercises with MediaPipe Pose," *Sensors*, vol. 24, no. 23, pp. 1–18, 2024, doi: 10.3390/s24237772.

[17] M. K. Ganesh, "Shoplifting Detection System Using YOLOv5, MediaPipe Pose Estimation, and Machine Learning-Based Behavior Analysis," *International Journal of Advance Research in Multidisciplinary*, vol. 3, no. 2, 2025, doi: 10.5281/zenodo.15590304.