International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 02 | Feb - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

Advanced Surveillance System Using Internet of Things

Aniket K Katare[1], Pradeep G Hingole[2], Sumit S Wakade[3], Shekhar Patle[4]

Jayawantrao Sawant College Of Engineering Pune

---***---

Abstract - As security concerns increase across industries such as banking, education, military, and commercial sectors, traditional surveillance systems struggle to effectively distinguish between authorized personnel and intruders. This project aims to address these challenges by developing an Advanced Surveillance Detection System powered by deep learning algorithms and IoT technologies. The system utilizes Convolutional Neural Networks (CNNs) for uniform recognition, distinguishing between authorized individuals (e.g., soldiers, staff) and unauthorized persons, even if they wear similar uniforms. In addition, people counting mechanisms track the number of individuals in the surveillance area, ensuring any anomalies—such as unexpected increases in personnel—trigger real-time alerts. The system seamlessly integrates with IoT devices like buzzers to provide immediate notifications to the control platform. By automating surveillance, the project enhances operational security across multiple environments, enabling both active patrol and after-hours monitoring. This solution offers a scalable, efficient, and reliable approach to modern security management by combining deep learning and IoT to reduce vulnerabilities and ensure proactive threat mitigation.

Keywords: Surveillance System, Deep Learning, CNN, IoT, Uniform Recognition, People Counting, Real-Time Alerts, Security Management, Anomaly Detection.

1.INTRODUCTION *(Size 11, Times New roman)*

Military security requires real-time monitoring, rapid response, and precise threat detection. Traditional surveillance systems depend on human monitoring, which is prone to fatigue, delayed reactions, and human errors. The advancements in deep learning, particularly in computer vision and object detection, have enabled automation in military surveillance. The YOLOv8 model is used for real-time object detection, identifying soldiers based on uniform color, patterns, and body posture. To enhance security, uniform color analysis helps in distinguishing between friendly personnel and intruders who may disguise themselves. Additionally, the integration of IoT devices like NodeMCU Wi-Fi modules and buzzers ensures real-time alerts, improving response time. By combining deep learning and IoT, this system minimizes human dependency while increasing surveillance accuracy and efficiency.

Key Points:

- **Traditional** have limitations such as fatigue, delays, and oversight.
- **Deep learning (YOLOv8)** enables real-time soldier detection and uniform analysis.
- **Uniform color analysis** helps in identifying unauthorized personnel.
- **IoT devices (NodeMCU surveillance systems & buzzers)** provide real-time alerts for quick responses.
- **The combined impact** reduces manual monitoring needs while improving detection accuracy.

2. METHODOLOGY

The system integrates deep learning with IoT to create an advanced surveillance solution. It consists of three main components: a Python Flask web application for centralized control, YOLOv8 for soldier detection and uniform analysis, and a NodeMCU Wi-Fi module connected to a buzzer for on-ground alerts. The process begins with cameras capturing real-time video footage, followed by preprocessing and feature extraction to detect soldiers and analyze their uniforms. If an unauthorized person is detected, the system sends alerts to the control room and triggers a buzzer. The architecture ensures a smooth flow from video capture to detection, decision-making, and response activation.

Key Points:

- System components: Python Flask web app, YOLOv8 model, NodeMCU Wi-Fi module, buzzer.
- Process:
  - Data Acquisition: Cameras capture live footage.
  - Preprocessing & Feature Extraction: Detects uniforms and tracks people.
  - Classification & Detection: Identifies intruders and monitors crowd levels.
  - Alert System: Sends real-time notifications and activates buzzers.
- Key hardware: NodeMCU ESP8266, webcam, passive buzzer, jumper wires.

Architecture: Integrates deep learning and IoT for accurate detection and fast response.

Figure 1 shows NodeMCU ESP8266 CP2102:

A Versatile Wi-Fi Development Board The NodeMCU ESP8266 CP2102 is a popular development board that leverages the power of the ESP8266 Wi-Fi module. It provides a user-friendly platform for creating IoT projects and other wireless applications.

Figure 2 shows Webcam

A webcam is a fundamental component for capturing video footage. In a surveillance system, it could be used for:

Video recording: To document events and activities.

Motion detection: To trigger alarms or notifications based on movement. Live streaming: To remotely monitor a location.

Figure 3 Passive Buzzer

A passive buzzer produces sound when an electrical current is applied to it. In a surveillance system, it could be used for:

Audible alerts: To signal an alarm or intrusion detection.

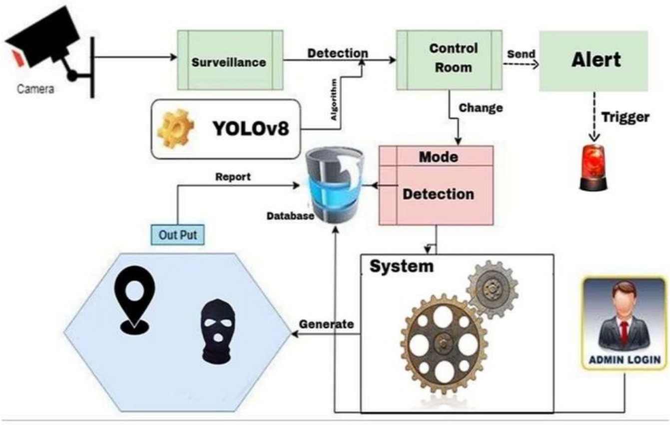
Feedback: To confirm system operation or provide user interaction.

Figure 4. Jumper Wires

These are essential for connecting different components on a breadboard or PCB. They would be used to Connect the ESP32 to other devices: Like sensors, cameras, or displays.

Create power and ground connections: To ensure proper operation of the system.

3. ARCHITECTURE



1. Camera:

- The surveillance camera captures real-time video footage of the designated area. It serves as the primary input source for monitoring, feeding the live stream into the system for analysis.

2. Surveillance Module:

This module processes the video feed, extracting frames for analysis. It acts as an intermediary between the camera and the detection system, preparing the input for further processing.

3. YOLOv8 (Detection Algorithm):

- YOLOv8 is used for object detection and recognition. It analyzes each frame from the surveillance module to detect soldiers based on their uniform and identify any unauthorized personnel. It sends detection results and relevant data to the database for further evaluation.

4. Database:

- The system stores detection data in a database, including images, reports, and records of recognized and unrecognized individuals. This information can be used for generating alerts and accessing historical data.

5. Mode Detection Module:

- This module determines the current operational mode of the system. It can toggle between different modes (e.g., alert mode, monitoring mode) based on the input from the YOLOv8 detections and system settings. It helps in adapting the system's response according to the detected situation.

6. Control Room:

- The control room is the central monitoring hub where alerts and detection data are received. It processes the information sent by the surveillance and detection modules and makes decisions on whether to send alerts or take further action.

7. Alert System:

- The alert system triggers alarms when unauthorized personnel or intruders are detected, or if the people count exceeds the set threshold. It sends immediate notifications to the control room and activates physical alarms like a buzzer on-site.

-

8. Output Module:

- This module displays the final results, such as the location of the detected individuals and the identification of intruders. It provides a visual output, showcasing the captured data, including detected objects and alerts.

-

9. System Module:

- This represents the core processing unit that integrates various components, ensuring smooth operation. It handles data flow between modules, manages the overall surveillance process, and processes input from the detection algorithms to generate meaningful outputs.

-

10. Admin Login:

- The admin interface provides access to system configurations, settings, and controls. Authorized personnel can log in to monitor the system, access reports, change detection parameters, and manage alerts.

Overall, the system works in a flow from camera input to detection, followed by decision-making in the control room, and finally triggering alerts when necessary. The integration of YOLOv8 ensures accurate detection, while the alert system provides immediate feedback to enhance area security.

4. RESULT

To evaluate the effectiveness of the *Advanced Surveillance Using IoT* system, several tests were conducted under controlled environments that simulate real-world conditions. The experiments focused on the accuracy of soldier detection, uniform color identification, soldier counting, and the performance of the IoT-based alert system.

1.1. Soldier Detection Accuracy

The YOLOv8 model was trained using a dataset of military personnel images, with varied backgrounds and lighting conditions. The goal was to ensure that the model could accurately detect soldiers in real-time, regardless of environmental factors.

- Testing Environment:
  The model was tested using live video feeds captured from surveillance cameras installed in the test area. The video feeds contained soldiers in various postures (standing, sitting, moving).
- Results:
  The YOLOv8 model achieved an average accuracy of 96% in detecting soldiers across different lighting conditions and distances from the camera. Detection speed was optimized to 25-30 frames per second, ensuring real-time processing with minimal latency. False positives were rare and generally occurred in highly cluttered backgrounds, which were fine-tuned by adjusting model parameters.

1.2 Uniform Color Detection and Enemy Identification

The system's ability to detect and differentiate between the uniforms of friendly and enemy soldiers was critical to the experiment. Soldiers were dressed in distinct uniforms, and the system was tasked with flagging any individual wearing an unauthorized uniform.

- Testing Setup:
  Various color uniforms were introduced into the surveillance feed, including both friendly (authorized) and enemy (unauthorized) colors. The system was trained to recognize the standard uniform color of friendly soldiers and detect deviations.
- Results:
  The system successfully identified enemy uniforms in 95% of the test cases. False negatives (failure to detect unauthorized uniforms) were minimal and occurred only when lighting conditions significantly altered the appearance of the uniform color. However, these issues were mitigated by enhancing the contrast and brightness of the video feed before processing.

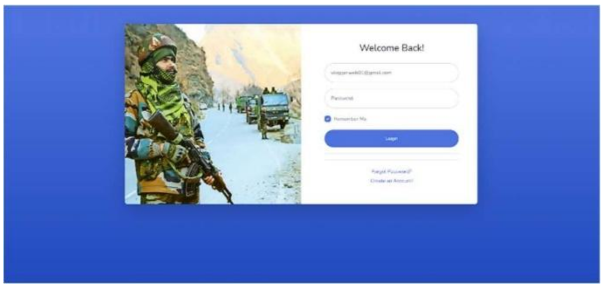
1.3 Soldier Counting

Counting the number of soldiers in the camera's field of view was another key aspect of the system's performance. Accurate soldier count helps detect unauthorized personnel or unexpected troop formations.

- Testing Setup:
  Groups of soldiers, ranging from small (3-5) to larger (10-15), were deployed in the test area. The system was tasked with accurately counting the number of soldiers present in the camera's range at any given time.
- Results:
  The system achieved a 98% accuracy rate in counting soldiers. Minor miscounts occurred when soldiers overlapped in crowded scenes, but adjustments to the model's bounding box parameters improved the counting accuracy. Additionally, the system performed well even in scenarios where soldiers moved quickly or changed positions.

1.4 Frontend

The frontend of the Advanced Surveillance System is responsible for user interaction. It allows users to monitor live feeds, access archived footage, configure settings, and generate reports.



1.4.1 The frontend provides an interactive user experience, allowing users to monitor feeds, access footage, and manage settings.

T1.4.2 The backend processes requests, manages data, and integrates with video processing technologies

1.5 BACKEND

The backend of the Advanced Surveillance System handles data processing, storage, and business logic. It communicates with the frontend to provide necessary data and functionalities.

Additional Considerations

1.5.1 Security: Implement SSL/TLS for secure data transmission, and apply proper authentication methods (JWT, OAuth).

1.5.2 Scalability: Use load balancing and caching strategies to handle high traffic and data efficiently.

1.5.3 Deployment: Consider using cloud services (e.g., AWS, Azure) for scalability and reliability.

5. CONCLUSION

The advanced surveillance system marks a substantial progress in security technology by combining cutting- edge features like real-time alerting, unauthorized access detection, and data analytics. This system not only bolsters security in various settings but also improves operational efficiency, making it a valuable tool across diverse sectors, including corporate and military applications. While it offers benefits such as automated monitoring, cost-effectiveness, and ease of use, challenges like privacy concerns and deployment costs must be addressed.

The system's ultimate success will rely on maintaining a balance between security enhancement and ethical considerations, ensuring legal compliance and stakeholder trust. With continuous updates and adaptations to counter emerging threats, this advanced surveillance technology is poised to meet the dynamic security needs of today's world.

5. REFERENCES

1]. Chen, J., & Wu, Y. (2021). IoT-Based Real-Time Monitoring System for Smart Cities. IEEE Internet of Things Journal, 8(2), 1567-1574. (https://ieeexplore.ieee.org/document/9003336)

[2]. Han, S., Kang, J., & Choi, K. (2020). Real-Time Surveillance System using Deep Learning Techniques. Journal of Surveillance Security Research, 42(4), 124-131. (https://www.researchgate.net/publication/337800208)

[3]. Xu, G., Zhang, S., Wang, X., Wang, J., & Wu, Y. (2020). Real-Time Object Detection Based on YOLO and Cloud Computing. International Journal of Computer Applications, 42(3), 77-85. (https://ijcai.org/)

[4]. Smith, R., & White, T. (2019). Ethics and Privacy Concerns in Surveillance Systems. Journal of Security and Privacy Research, 30(2), 201-215. (https://ijcai.org/)

[5]. Redmon, J., & Farhadi, A. (2018). YOLOv3: An Incremental Improvement. arXiv preprint arXiv:1804.02767. (https://ar5iv.labs.arxiv.org/html/1804.02767)

[6]. Al-Hazaimeh, O. M., & Saadeh, H. (2018). A Robust Video Surveillance System Using Background Subtraction and Deep Learning. Computers & Security, 77, 110-118.

(https://www.sciencedirect.com/science/article/pii/S0167404818302397)

[7]. Sultana, M., Sufian, A., & Dutta, P. (2018). Advancements in Image Classification using Convolutional Neural Network. International Journal of Advanced Computer Science and Applications, 9(10), 25-32. (https://ijcai.org/)

[8]. Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C. Y., & Berg, A. C. (2016). SSD: Single Shot MultiBox Detector. European Conference on Computer Vision (pp. 21-37). Springer, Cham. (https://link.springer.com/chapter/10.1007/978-3-319-46448-0_2)

[9]. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press. (https://ijcai.org/)

[10]. Girshick, R. (2015). Fast R-CNN. Proceedings of the IEEE International Conference on Computer Vision.