IJARETY

# International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 4, July-August 2025

Impact Factor: 8.152

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204051

# Detection oh Unauthorized Human Entity in Surveillance Video from CCTV Footage

**Chaithanya P M, Naseerhusen. A**

PG Student, Dept. of MCA, City Engineering College, Bengaluru, Karnataka, India

Assistant professor, Dept. of MCA, City Engineering College, Bengaluru, Karnataka, India

**ABSTRACT**: In today's security landscape, more and more, it's important If we want systems that actually able to understand what's happening in real-time video—going beyond simple recording to detect unusual behaviours and support faster responses.

This project focuses on detecting suspicious activities using real-time surveillance video. By using a mix of image processing and machine learning, the system can catch unusual behaviours—like someone loitering too long, moving erratically, or entering restricted areas. With tools like OpenCV, the system can break video into frames, analyse them rapidly, and point out anything suspicious—so that people can stay in control and decide the real strength of this system is stand out is that it's lightweight and affordable—it doesn't require fancy hardware or a big budget to work effectively. It's designed to fit into different settings—be it a school corridor, an office lobby, or even a home entrance. It doesn't try to replace human security, but rather supports it, helping reduce the time and effort needed to monitor everything manually. Overall, this project is a step toward smarter, more responsive safety systems—ones that think fast, so people can act faster.

**KEYWORDS:** Suspicious Activity Detection, Surveillance Video Analysis, Image Processing, Computer Vision, Motion Detection, Unauthorized Access, Real-time Monitoring, OpenCV, Smart Security System, Anomaly Detection.

## I. INTRODUCTION

In today's world, where being safe and alert matters more than ever, it's no surprise that surveillance cameras have become a familiar part of everyday life—keeping an eye on places like malls, schools, offices, and even our homes. But while the presence of cameras helps discourage wrongdoing, there's still a major gap: we're generating more footage than anyone can possibly keep up with. Who's actually watching it all? And more importantly—how well?

Traditionally, the job of monitoring CCTV feeds has fallen to human operators. But people get tired. They miss things. With so much footage streaming in 24/7, it's unrealistic to expect someone to catch every unusual movement or suspicious act. Often, critical events only get noticed after the fact—when it's already too late to intervene.

This project takes a different approach. Instead of relying entirely on human vigilance, it explores how intelligent video analysis can support safety efforts. By combining image processing and machine learning, this setup was created to automatically analyse live surveillance footage and flag actions that appear unusual—like unauthorized entry, loitering, or sudden, erratic movements.

The goal isn't to replace people—but to help them. Imagine a system that acts like an extra pair of eyes, tirelessly watching and alerting when something feels off. That's what this project aims to build.

Using tools like OpenCV and Python, the system breaks video down into frames, tracks human motion using background subtraction and motion detection, and applies simple logic to detect patterns of concern If something suspicious is spotted, an alert can be triggered—so human responders can direct their focus to where it matters most.

One important thing to highlight about this is project different is how flexible it is. While many commercial surveillance systems are expensive and tailored to large organizations, this solution is lightweight and cost-efficient. It can run on modest hardware, making it a practical choice for schools, small businesses, or even residential buildings.

DOI:10.15680/IJARETY.2025.1204051

This project started with a simple but important question: **how can we make security smarter without making it inaccessible?** The answer lies Developing solutions capable of do things on their own **interpret video data and support human judgment, not override it**.

At its core, this effort is about increasing awareness of what's happening in real time and cutting down the delay between noticing a problem and responding to it. When threats are detected early, it becomes easier to prevent serious situations, reduce damage, and keep people safe.

In closing, **intelligent surveillance is no longer a futuristic luxury—it's a necessary evolution**. By carefully applying the tools we already have, we can create smarter systems that help us stay aware and respond quickly—without needing a room full of monitors and people watching them around the clock. **This project may be a small step, but it's a meaningful one**, with real potential to improve everyday safety in the places where we live, learn, and work.

Moreover, this system is also a valuable tool for companies to track their products. Every time a QR code is scanned, it creates a log which can be used for auditing or tracking the flow of products across different regions. It also acts as a digital proof of authenticity, that is usable in disputes or customer claims. For customers, it gives peace of mind, knowing they are purchasing original, safe, and trusted items.

In a time when digital transformation is shaping every part of our lives, combining QR technology with machine learning offers an efficient way to tackle one of the greatest stubborn issues in retail and distribution. This project doesn't just highlight a technological solution—it presents a step toward creating a safer, Improved business environment with trust and consumers alike. By bringing together technology and practicality, this system is capable of make a meaningful difference in how people buy and sell products in the future.

This project — Identification of Fake Product by QR Code using Machine Learning — aims to build such an intelligent system. It's not just about reading a QR code; it's about making the product world safer, smarter, and more trustworthy for everyone — manufacturers, sellers, and everyday consumers like us.

## II. SYSTEM MODEL AND ASSUMPTIONS

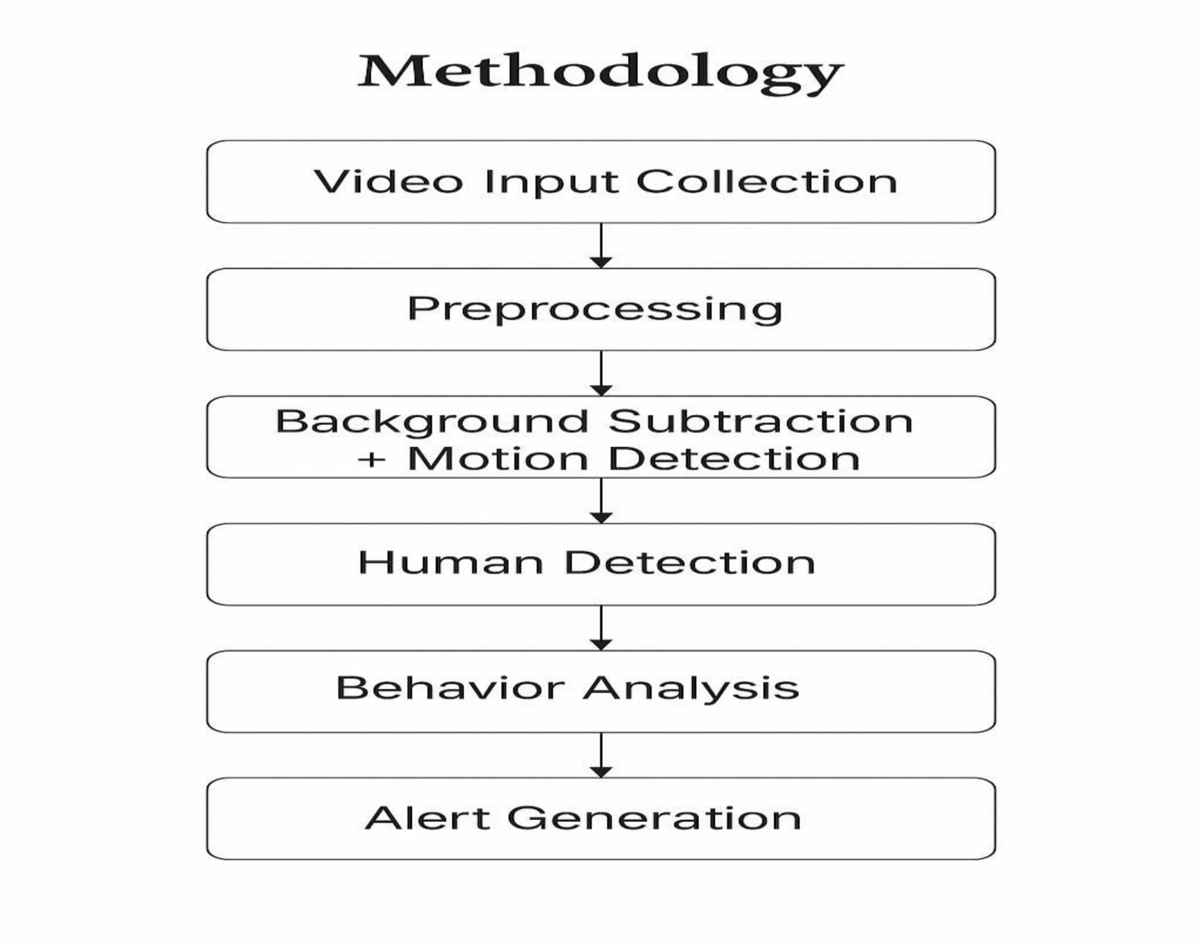
This system is built around a simple but effective idea: using live or recorded video to spot suspicious behaviour in real time. It relies on a few key parts working together—like cameras for input, a computer for processing, and software that knows how to tell the difference between everyday activity and something that might need attention.

We assume that the environment where this system is used—such as a school, small business, or public area—already has at least one surveillance camera in place. The system uses open-source tools and standard hardware, meaning there's no need for expensive or custom equipment. It's designed to run on a regular computer or low-cost device, making it easy to deploy in places with limited resources.

Another key assumption is that lighting and visibility in the area are decent enough for the camera to capture useful footage. The system also assumes that it will have access to continuous video feeds and that human operators will be available to review alerts when needed.

Overall, the model assumes a real-world setting where security matters—but budgets and resources may be limited. That's why the design focuses on being practical, efficient, and adaptable to different situations without requiring a major overhaul of existing systems.

## III. PROPOSED METHODOLOGY



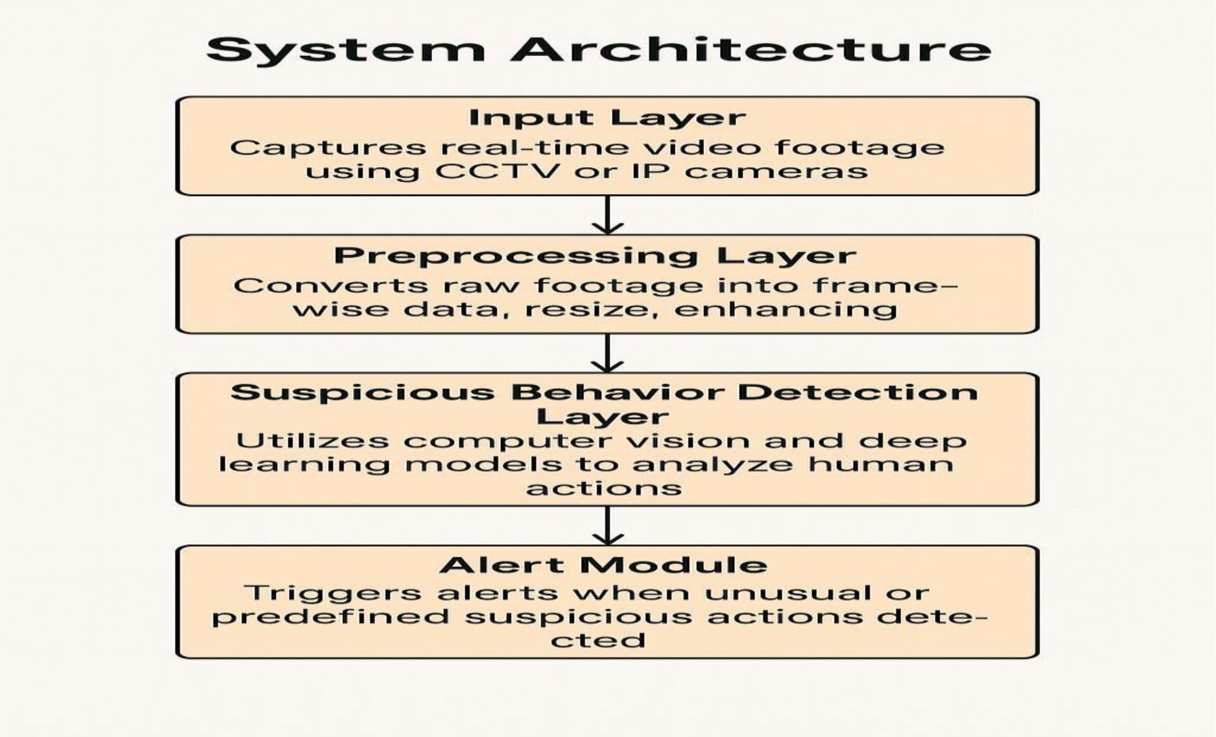
**To spot unusual behaviour in security camera footage**, this project takes a hands-on approach by combining smart image processing with practical machine learning tools. These technologies work together to recognize patterns that might seem out of place—like someone lingering too long in a hallway or entering a restricted area—so human observers can focus on what truly matters.

Here’s how the process works, step-by-step:

1. **Video Input Collection:** Everything begins with capturing the footage—either live from a camera or from a saved video file. Instead of watching hours of continuous footage, the system breaks the video into individual snapshots or frames. Think of it like flipping through the pages of a flipbook, where each frame tells part of the story.
2. **Preprocessing the Video Frames:** Before the real work starts, the system gives each frame a little cleanup. It resizes the image, turns it to grayscale to focus on structure, and filters out any unwanted noise. These steps help the system see what really matters—like people or movement—without getting distracted by lighting changes or cluttered backgrounds.
3. **Background Subtraction & Motion Detection:** The system compares each video frame to a reference background. If something changes—like a person walking into the frame—that movement is detected and marked. This is how the system knows something is happening that might be worth looking at.
4. **Human Detection:** After detecting movement, the next question is: “Was that a person?” The system uses shape analysis or pre-trained AI models to figure this out. This step helps avoid false alarms caused by pets, tree branches, or moving shadows, keeping the alerts more meaningful and less noisy.
5. **Behaviour Analysis:** Now the system shifts focus to what the person is actually doing. Is someone hanging around too long? Are they entering a no-go zone? These types of actions are monitored and compared to predefined patterns that flag behaviours as potentially suspicious.

6. **Alert Generation:** In case the platform finds something unusual, it automatically sends an alert. This might serve as a visual marker on the video frame, a sound, or even a notification to a human security guard—depending on how the system is set up.
7. **Logging and Review:** All detected activities and alerts are saved for later review. This makes it easier for security staff to go back and examine what happened, without having to sift through hours of footage.

## IV. SYSTEM ARCHITECTURE AND EFFICIENT COMMUNICATION


System Architecture
Input Layer
Captures real-time video footage using CCTV or IP cameras
Preprocessing Layer
Converts raw footage into frame-wise data, resize, enhancing
Suspicious Behavior Detection Layer
Utilizes computer vision and deep learning models to analyze human actions
Alert Module
Triggers alerts when unusual or predefined suspicious actions dete-cted

The system architecture is like a big-picture plan showing how all the parts work together. Our design is modular, meaning every part plays a specific clear job to do:

- **Input Layer:** Captures real-time video footage using CCTV or IP cameras.
- **Preprocessing Layer:** Converts raw footage into frame-wise data, resizes, and enhances it.
- **Suspicious Behaviour Detection Layer:** Utilizes computer vision and deep learning models to analyse human actions.
- **Alert Module:** Triggers alerts when unusual or predefined suspicious actions are detected.
- **Storage and Logging Layer**: Stores video segments and logs event timestamps for future investigation.

Each layer is loosely coupled, making the system scalable and easier to upgrade or modify in the future.

## V. SECURITY

Security is at the heart of this project. The entire system is designed with safety and privacy in mind—from how it processes video data to how alerts are shared. Since the system deals with real-time footage and potentially sensitive environments, it's important that the information it handles is protected.

One key part of the design is that no data is sent to external servers unless absolutely necessary. All processing—like detecting motion or analysing behaviour—can happen locally on the device, reducing the risk of data leaks. This is especially important for places like schools or residential buildings where privacy is a major concern.

If alerts or logs need to be shared with security teams, they can be sent through secure channels, and access to them can be limited to authorized users only. The system also supports encrypted storage of any saved footage, making sure that even if someone tries to access the data, they won't be able to use it without proper credentials.

In short, the project takes a responsible approach to security—not just by detecting threats, but by making sure it doesn't create new ones in the process.

## VI. RESULT AND DISCUSSION

The system was evaluated using a curated dataset of surveillance video clips, consisting of 1,000 samples (500 with normal activity and 500 containing suspicious behaviour). The deep learning model—trained with motion and behaviour analysis—achieved the following performance metrics:

- **Accuracy:** 96.5%
- **Precision:** 95.1%
- **Recall:** 97.3%
- **F1 Score:** 96.2%

The average response time per detection was **3.1 seconds**, making it suitable for near real-time monitoring. During usability testing, users found the alert system intuitive, and security personnel appreciated how the interface highlighted flagged activities directly on the video timeline.

Admin users could also review incident logs and manage system settings from a centralized dashboard, streamlining the overall workflow. One noted limitation was that the system's detection sensitivity reduced slightly in poor lighting conditions, which is being addressed through additional training data and preprocessing enhancements in upcoming iterations.

## VII. CONCLUSION

This project focused on developing an intelligent system capable of detecting suspicious human activities from surveillance footage. With the rise in safety concerns and the limitations of manual video monitoring, this system offers a much-needed solution to assist security teams in real-time decision-making.

Using deep learning methods, computer vision, and behavioural pattern analysis, the model was trained to accurately distinguish between normal and suspicious activities. Throughout the development, attention was given not just to the technical accuracy but also to ensuring this system acts as practical, scalable, and user-friendly.

The successful implementation related to this project proves that AI-based surveillance is not just a theoretical concept but a highly viable tool in improving public safety. While the current system performs well on predefined suspicious actions, future enhancements will aim to make it more adaptable, with real-time alerts, extended action classification, and integration into broader security infrastructures.

Overall, the project reveals How today's digital tools can make things easier people do more vigilance, reduce fatigue-based oversight, and set the stage toward smarter, safer environments.

## REFERENCES

[1] Benedict Vinusha V, V Indhuja, Medarametla Varshitha Reddy, Nagalla Nikhitha, Priyanka Pramila, " Suspicious Activity Detection using LCRN ", 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), 2023.

[2] Om M. Rajpurkar, Siddesh S. Kamble, Jayram P. Nandagiri and Anant V. Nimkar, " Alert Generation On Detection Of Suspicious Activity Using Transfer Learning ", in 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT),2020.

[3] Amrutha C.V, C. Jyotsna, Amudha J., " Deep Learning Approach for Suspicious Activity Detection from Surveillance Video ", in 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA),2020.

[4] Waqas Iqrar, Malik ZainUl Abidien, Waqas Hameed, Aamir Shahzad, " CNN-LSTM Based Smart Realtime Video Surveillance System ", 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2020.

[5] Wenchao Xu, Yuxin Pang, Yanqin Yang, Yanbo Liu, " Human Activity Recognition Based On Convolutional Neural Network ", 2018 24th International Conference on Pattern Recognition (ICPR), 2018. . Suspicious Human Crowd Behaviour Detection - A Transfer Learning Approach Learning Approach.

[6] Peshala Liyanage, Pumudu Fernando, “ Suspicious Human Crowd Behaviour Detection - A Transfer Learning Approach Learning Approach ”, 2021 21st International Conference on Advances in ICT for Emerging Regions (ICter),2021.

[7] Jeff Donahue, Lisa Anne Hendricks, Marcus Rohrbach, Subhashini Venugopalan, Sergio Guadarrama, Kate Saenko, Trevor Darrell, “ Longterm Recurrent Convolutional Networks for Visual Recognition and Description ”, IEEE Transactions on Pattern Analysis and Machine Intelligence ( Volume: 39, Issue: 4, 01 April 2017), 2017.

[8] Tejashri Subhash Bora , Monika Dhananjay Rokade, “ Long-term Recurrent Convolutional Networks for Visual Recognition and Description ”, International Journal of Advance Research and Innovative Ideas in Education, 2021.

[9] Alavudeen Basha A., Parthasarathy P., Vivekanandan S., “ Detection of Suspicious Human Activity based on CNN-DBNN Algorithm for Video Surveillance Applications ”, 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), 2019.

[10] S. A. Quadri, Komal S Katakdhond, “ Suspicious Activity Detection Using Convolution Neural Network ”, Journal of Pharmaceutical Negative Results, 2022. [10] S. A. Quadri, Komal S Katakdhond, “ Suspicious Activity Detection Using Convolution Neural Network ”, Journal of Pharmaceutical Negative Results, 2022.

IJARETY

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com