IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Suspicious Person Detection Using Infrared Camera

Gaurav Thapliyal[1] , Mohit Titarmare[2] , Sanghdip Udrake[3], Yash Raut [4] , Gaurav Wankar[5], Prof. Anand Donald[6]

[12345]Students, CSE department , RCERT ,Chandrapur

[6]Faculty, CSE department , RCERT ,Chandrapur

Abstract: This project proposes a robust surveillance system for detecting suspicious individuals in low-light and challenging visibility conditions using infrared (IR) cameras and night vision technology. The system aims to enhance security by employing machine learning techniques to process and analyze thermal images captured by IR cameras. The approach involves image acquisition, pre-processing, feature extraction, and classification to identify individuals exhibiting unusual behavior or possessing suspicious attributes. The model is trained using a diverse dataset to improve accuracy and reliability in detection. The system's ability to function effectively under poor lighting conditions makes it highly suitable for nighttime monitoring, restricted access areas, and environments where conventional surveillance systems fail. This technology has potential applications in security systems, military surveillance, and critical infrastructure protection, contributing to improved public safety and crime prevention.

Keywords—Python,Surveillance, Systems, Suspicious Activity

1. INTRODUCTION

The detection of suspicious individuals is a critical aspect of modern security systems, particularly in areas with limited visibility, such as at night or in low-light conditions. Traditional surveillance systems, which rely on visible light cameras, often face significant challenges in these environments, making it difficult to monitor and detect potential threats in real time. Infra-red (IR) cameras and night vision technology provide powerful alternatives for enhancing surveillance capabilities in such scenarios. IR cameras capture thermal signatures rather than relying on ambient light, allowing for accurate detection of individuals based on their body heat. Meanwhile, night vision technology amplifies available light or utilizes near-infrared illumination to produce clearer visuals in dark environments.

This project aims to develop an intelligent suspicious person detection system using a combination of infra-red cameras and night vision technology to enhance security monitoring. By analyzing thermal images captured by IR cameras and enhanced visuals from night vision systems, the proposed system can identify heat patterns, anomalies, and physical movements that indicate the presence of individuals. Additionally, the system integrates machine learning techniques for object detection and behavior analysis, enabling it to differentiate between normal and suspicious activities. The use of IR and night vision technologies not only improves detection capabilities in low-visibility scenarios but also reduces the likelihood of false positives, ensuring more accurate threat identification. This project offers a robust solution for real-time monitoring in security-critical areas, contributing to safer environments through more reliable and efficient surveillance systems.

2. EASE OF USE

Suspicious Person Detection :

The use of Infra-red (IR) cameras and night vision technology provides a versatile approach to suspicious person detection. IR cameras are relatively easy to set up, with many modern models offering plug-and-play functionality and straightforward integration with processors such as Raspberrssy Pi or PC.

From a software perspective, IR cameras often provide SDKs or pre-built interfaces, while night vision systems are compatible with popular libraries like OpenCV for motion detection and image processing. Implementing detection algorithms requires knowledge of image processing and machine learning. While simpler methods like motion tracking and heat signature analysis can be effective,

integrating deep learning techniques offers better accuracy but demands higher technical expertise.

3. LITERATURE REVIEW

[International Journal of Creative Research Thoughts (IJCRT) www.ijcrt.org]- real time violence detection system using deep learning was developed to prevent the violence behavior of crowd or players in sports. In a spark environment, frames were extracted from real-time videos. If the system detects any violence in football, then alert the security people. To prevent the violence in advance, the system detects the video actions in real time and alerts the security forces. VID dataset was used and achieved an accuracy of 94.5% for detecting violence in football stadium [7]. The abnormal event detection consists of different modules for the processing of video data. Deep architectures were used to detect human behavior. The proposed CNN and LSTM based models used UT Interaction dataset. One of the drawbacks of the system was similar human behaviors like pointing or punching is difficult to identify [8]. Understanding crowd behavior.

[Deep Learning Approach for Suspicious Activity Detection from Surveillance Video Amrutha C.V, C.
Jyotsna, Amudha J. Dept. of Computer Science & Engineering] -Abnormal event detection includes different modules for processing video data. Deep architectures have been used to detect human behavior. The proposed models based on CNN and LSTM used the UT interaction dataset. One of the system's limitations is that it is difficult to identify similar human behaviors, such as pointing or hitting. Understanding crowd behavior using a deep space-time approach classifies videos into future pedestrian prediction, destination estimation, and overall crowd behavior into three other categories. together. Spatial information in the video image is extracted using a composite layer.

4. PROBLEM STATEMENT

Traditional security systems that rely on visible light cameras are limited by poor lighting conditions, such as nighttime or low- visibility environments. The challenge is to develop an automated system capable of detecting suspicious persons in such conditions using a combination of infrared (IR) cameras and night vision technology to enhance detection capabilities.
The goal of this project is to design and implement a suspicious person detection system using infrared thermal imaging, night vision technology, and machine learning (ML) techniques. The system will automatically analyze thermal and low-light visual data in real- time to identify human figures, detect unusual behaviors (e.g., loitering, unauthorized entry), and issue alerts for further action by security personnel. The primary challenge is to accurately detect and classify potential threats in diverse environmental conditions while minimizing false positives and ensuring real-time performance.

5. WORKING

1. Image/Video Capture:

To address the challenges of low visibility, the system utilizes **infrared (IR)** or **night vision cameras** capable of capturing high- contrast video footage in dark environments. These cameras detect **thermal radiation** emitted by objects, particularly human bodies, enabling reliable detection even in total darkness. The captured video serves as the primary input for subsequent processing stages.

2. Preprocessing :

Each video stream is processed frame-by-frame to enhance detection reliability and computational efficiency:

- **Grayscale or Thermal Image Conversion**: Frames are converted to grayscale or thermal formats, depending on the sensor input, to simplify analysis and reduce computational complexity.
- **Noise Reduction**: A **Gaussian Blur** is applied to suppress high-frequency noise.
- **Feature Enhancement**: Techniques such as **Histogram Equalization** or **Contrast Limited Adaptive Histogram Equalization (CLAHE)** are used to enhance image contrast and bring out significant features critical for object detection.

3. Object Detection and Tracking :

After preprocessing, frames are passed to the object detection module:

- **Detection**: Using **Convolutional Neural Networks (CNNs)** or lightweight alternatives (e.g., MobileNet, YOLO- tiny for embedded systems), human figures are detected in each frame.

4. Suspicious Behavior Detection :

The behavior analysis module is responsible for identifying potentially suspicious activities based on motion patterns:

- **Motion Tracking**: Movement vectors are computed for each detected person across a temporal window.
- **Pattern Analysis**: The system flags anomalies using both rule-based logic and basic machine learning classifiers such as:
  - **Support Vector Machines (SVM)**
  - **Decision Trees**

5. Alert Generation :

When suspicious behavior is detected, the system initiates the following actions:

- **Visual/Audio Alerts**: A buzzer or visual pop-up is triggered to notify nearby personnel.
- **Data Logging**:

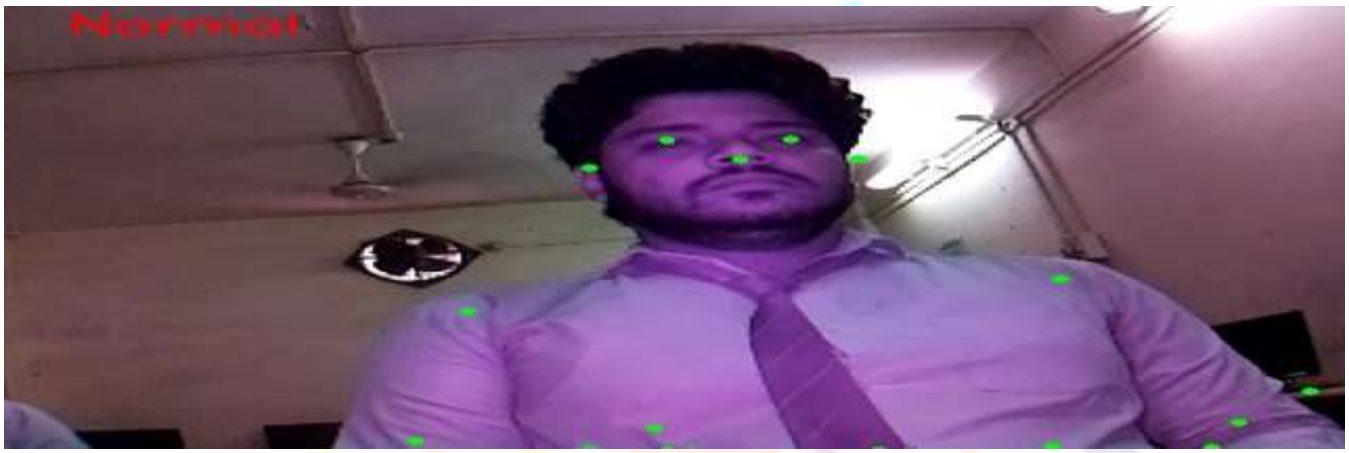
- Saves the frame in which suspicious behavior was detected.
- Stores metadata such as **timestamp**, **location**, and **person ID** in a local database or filesystem.

6. Real-Time Monitoring and User Interface

The final component is the real-time interface for operators:

- **Platform**: Runs on standard PCs or embedded systems (e.g., Raspberry Pi 4 with sufficient processing capabilities).
- **Graphical User Interface (GUI)**:
  - Displays the **live video feed** with bounding boxes and annotations.
  - Maintains a **log panel** showing:

.



Here , It represent the person is shows the activity is normal.

Here , It represent the person is shows the activity is suspicious

6. FUTURE SCOPE

The proposed system for suspicious person detection using infrared (night vision) cameras offers considerable potential for future development and real-world applications. As security concerns continue to grow, especially in low-light or nighttime environments, this technology can serve as a critical component in advanced surveillance systems. Future work can focus on integrating deep learning techniques such as convolutional neural networks (CNNs) and real-time object detection models (e.g., YOLO, SSD) to enhance the system's accuracy, speed, and ability to detect abnormal behavior patterns.

Furthermore, the system can be extended for use in high-security areas such as defense zones, border surveillance, airports, and railway

stations, where 24/7 monitoring is essential. By combining infrared imaging with facial recognition, motion analysis, and biometric data, the system could provide more reliable identification of suspicious individuals even in complete darkness.

The integration of Internet of Things (IoT) devices and cloud-based analytics platforms would enable real-time data transmission, remote monitoring, and centralized control. Additionally, future versions of the system could be implemented on mobile surveillance units such as drones or autonomous robots for wider area coverage.

Beyond security, the technology also shows promise in fields like disaster management and search-and-rescue operations, where locating individuals in smoke-filled, foggy, or dark environments is critical. With ongoing advancements in thermal imaging sensors and intelligent video processing, the system can evolve into a comprehensive tool for smart and proactive surveillance

7. SYSTEM REQUIREMENTS

Hardware Requirements:

- Infra-red Camera: High-resolution (640x480 or better),
- 30+ fps, wide field of view.
- Processing Unit: High-performance CPU/GPU (Intel i5 or NVIDIA Jetson), 8 GB RAM, SSD storage (100 GB+).
- Peripheral Devices: Monitor, keyboard, mouse, alert system.
- Network: Internet/Wi-Fi for cloud integration and remote monitoring.

Software Requirements:

- Languages: Python, C++ for image processing.
- Libraries: TensorFlow/PyTorch (for deep learning), OpenCV (for computer vision), scikit-learn (for anomaly detection).
- Real-Time Processing: Flask/Django for web monitoring, MQTT/WebSocket for alerts.
- Database: MySQL/PostgreSQL for storing logs (optional).

8. CONCLUSION

This study demonstrates the practical implementation of a suspicious person detection system using infrared night vision technology for enhanced surveillance in low-light environments. By leveraging thermal imaging, the system effectively detects human presence and movement irrespective of lighting conditions. The integration of image processing techniques and motion analysis allows for the identification of potentially suspicious behavior based on predefined parameters such as prolonged presence, unusual movement patterns, and unauthorized access zones. It is lightweight, portable, and easily customizable for detecting various other poses or behaviors.
Overall, this solution combines machine learning, computer vision, and embedded systems to enhance real-time human activity monitoring.

9. REFERENCE

[1] Brown, T. B., et al. "Language Models are Few-Shot Learners." Advances in Neural Information Processing Systems, 2020.

[2] Karras, T., Laine, S., and Aila, T. "A Style-Based Generator Architecture for Generative Adversarial Networks." IEEE Transactions on Pattern Analysis and Machine Intelligence, 2019.

[3] Radford, A., et al. "DALL·E: Creating Images from Text." OpenAI, 2021.

[4] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." Cryptography Mailing list, 2008.

[5] Protocol Labs. "InterPlanetary File System (IPFS)." 2020.

[6] Chen, X., et al. "MoCoGAN: Decomposing Motion and Content for Video Generation." IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

[7] G. Sreenu and M. A. Saleem Durai “Intelligent video surveillance: a review through deep learning techniques for crowd analysis” , Journal Big Data ,2019