**Predictive Analytics Project**

**REPORT**

For

Computer Vision

Submitted By

**Specialization**  **SAP ID** **Name**

AIML 500105674 Vedanti Jauhari

Department of Informatics

School Of Computer Science

UNIVERSITY OF PETROLEUM & ENERGY STUDIES,

DEHRADUN- 248007. Uttarakhand

1. **Abstract**

This project presents the development of an intelligent Intruder Detection System that employs computer vision techniques and real-time communication to enhance security monitoring. The system utilizes OpenCV for image analysis and Twilio for instant alert messaging, offering a robust solution for intrusion detection. The system employs Background Subtraction and Contour Detection techniques to identify and track intruders within a given environment. By continuously analysing video feeds, it distinguishes ordinary movements from potential security threats, sending alerts only when necessary. This approach minimizes false alarms while ensuring swift responses to genuine security breaches. OpenCV, a powerful computer vision library, plays a pivotal role in creating an intelligent surveillance system that seamlessly handles video streams. Background Subtraction isolates moving objects from their surroundings, while Contour Detection further enhances object recognition. The integration of these techniques results in precise intruder detection. Twilio, a cloud communications platform, comes into play for real-time intruder alerts. The system dispatches SMS messages, allowing users to stay informed and respond promptly to security incidents, even when they are off-site.

The project's robustness against changing lighting conditions, noise, and false positives is achieved through a combination of techniques, including background modeling and contour filtering. Additionally, patience timers ensure that alerts are triggered only after sustained detections, significantly reducing the likelihood of false alarms. By combining computer vision with instant communication, Smart Intruder Detection System offers an effective and efficient solution for enhancing security in a variety of settings, including homes, offices, and public spaces. Its adaptability and flexibility make it a valuable tool for proactive security monitoring. Our project presents an intelligent surveillance system that harnesses the power of computer vision and instant communication to create a responsive and accurate Intruder Detection System, significantly advancing the field of smart security solutions.

1. **Introduction**

In an age where security is of utmost importance, technology continues to be a vital tool in safeguarding our surroundings. This project introduces the Smart Intruder Detection System, a fusion of computer vision and real-time communication technologies, designed to enhance security monitoring in various settings, from homes to offices and public spaces. This system's core strength lies in its ability to effectively detect and respond to potential intruders while minimizing false alarms. It achieves this through a combination of cutting-edge

techniques:

• Computer Vision with OpenCV: The system harnesses the robust capabilities of

OpenCV, including background subtraction and contour detection, to analyze real-time

video streams. By distinguishing ordinary movements from security threats, it

accurately identifies potential intruders.

• Patience-Based Intruder Detection: To eliminate transient disturbances and reduce false

positives, the system employs a patience mechanism. It requires consecutive intruder

detections before triggering an alert, ensuring reliability in varying environmental

conditions.

• Instant Alerting with Twilio: Real-time communication is facilitated through Twilio, a

cloud communications platform. When an intruder is detected, the system promptly

sends an SMS alert, enabling users to respond swiftly to security incidents, whether

they are on-site or remote.

• Adaptive Morphological Operations: Adaptive morphological operations are applied to

refine detected regions and enhance accuracy. These operations adapt to changing

lighting conditions and effectively reduce noise levels.

• Video Recording for Evidence: In the event of an intrusion, the system records video

footage, providing valuable evidence for reviewing security incidents and supporting

claims.

• Performance Monitoring: The system keeps users informed by displaying critical

performance metrics, such as frames per second (FPS) and current room occupancy

status. This data allows users to continuously assess the system's effectiveness.

1. **Literature Survey**

• Introduction to Video Surveillance-Based Intelligent Security Systems: Video

surveillance-based intelligent security systems play a crucial role in detecting potential

crimes early, allowing real-time notifications and preventive measures [1]. Intrusion

into sensitive areas necessitates simultaneous intrusion detection and visual observation

[2]. The affordability of general-purpose processors and video cameras gives video

based intrusion detection systems an advantage over alternatives like microwave

Doppler detectors and infrared detectors [3]. Despite various proposed variants, existing

systems often lack online performance, including high processing speed, low execution

memory, and high accuracy [1], [2], [4]–[7].

• Challenges in Video-Based Intrusion Detection: Video-based intrusion detection

involves object detection, target tracking, and the implementation of intrusion rules.

Object detection in complex environments using real-time video streams is challenging.

Traditional methods like Gaussian Mixture Model (GMM), morphological operations,

background subtraction, and frame difference may lack the robustness required for real

time applications [8]–[10]. Deep learning-based object detection techniques, such as

those leveraging OpenCV, offer potential improvements in accuracy and performance

[11].

• Integration of Intrusion Detection and Facial Recognition in IoT: Prakash's work [11]

proposes an innovative approach to enhance IoT security by integrating intrusion

detection and facial recognition in CCTV systems. Face detection algorithms,

particularly with OpenCV, are seamlessly integrated to transform traditional CCTV

systems into advanced security tools.

• Low-Cost IoT-Based Intruder Detection System with Face Recognition: Rao and

colleagues [12] introduce a groundbreaking approach to home security through a low

cost IoT-based intruder detection system using face recognition. The system employs a

PIR sensor, a USB camera, and a Raspberry Pi for efficient processing. The

combination of machine learning algorithms and OpenCV facilitates real-time face

detection and recognition, achieving a processing rate of 28 images per second. The

system distinguishes between authorized and unauthorized access attempts and,

importantly, enables remote authentication via the IoT. Upon intrusion detection, the

system promptly sends email notifications, allowing homeowners to take immediate

action, even when physically absent.

1. **Existing System**

Currently, the landscape of security systems is diverse, with various approaches addressing the imperative need for intrusion detection and intelligent security monitoring. Traditional security systems typically rely on physical barriers and alarms, complemented by surveillance cameras. However, these systems may lack the adaptability and advanced features required to effectively respond to modern security challenges.

Video-based intrusion detection systems have emerged as a significant advancement, harnessing the power of surveillance cameras and sophisticated algorithms. These systems focus on real-time video analysis to identify potential intruders. Nevertheless, challenges persist in achieving high processing speed, minimizing execution memory usage, and ensuring accuracy in dynamic and complex environments.

The integration of Internet of Things (IoT) devices has led to innovative security solutions. These systems incorporate sensors, cameras, and communication devices that work cohesively to detect and respond to security threats. By leveraging the IoT, these systems enable remote monitoring and control, offering users real-time alerts and the ability to take immediate action. Face recognition systems represent another facet of security technology, contributing to access control and identification. Utilizing machine learning algorithms and frameworks like OpenCV, these systems efficiently detect and recognize faces, adding an additional layer of authentication to security setups. Acknowledging the challenges posed by dynamic environments, some existing systems incorporate adaptive operations. These operations, including background subtraction morphological operations, and frame difference methods, refine object detection and reduce false positives, enhancing overall system accuracy.

1. **Proposed System**

The Smart Intruder Detection System is poised to revolutionize security monitoring by integrating state-of-the-art technologies to create a robust and responsive solution. In an era where security is paramount, this proposed system aims to address the limitations observed in existing security systems while introducing novel features to enhance intrusion detection and real-time response. At its core, the Smart Intruder Detection System leverages the capabilities of computer vision, specifically employing OpenCV for sophisticated real-time video stream analysis. This technology facilitates the accurate identification of potential intruders by employing techniques like background subtraction and contour detection, distinguishing ordinary movements from security threats. A distinctive feature of the proposed system is the incorporation of a patience-based intruder detection mechanism. By requiring consecutive intruder detections before triggering an alert, this mechanism minimizes false alarms, enhancing reliability across varying environmental conditions. This innovation seeks to eliminate transient disturbances and enhance the system's effectiveness. Real-time communication is a cornerstone of the Smart Intruder Detection System, achieved through the integration of Twilio, a cloud communications platform. Upon detecting an intruder, the system promptly sends an SMS alert, ensuring instant notification to users, whether they are on-site or remote. This real-time alerting mechanism empowers users to respond swiftly to security incidents, contributing to a proactive security posture. Adaptive morphological operations further distinguish the proposed system. These operations refine detected regions, adapting to changing lighting conditions and effectively reducing noise levels. This adaptability ensures the system's accuracy in dynamic environments, overcoming challenges faced by traditional methods.

In the event of an intrusion, the proposed system goes beyond mere detection by incorporating video recording capabilities. This feature provides valuable evidence for reviewing security incidents and supporting claims, enhancing the system's utility beyond real-time monitoring. Additionally, the Smart Intruder Detection System prioritizes performance monitoring, offering users critical metrics such as frames per second (FPS) and current room occupancy status. This data empowers users to continuously assess the system's effectiveness and make informed decisions regarding security measures. Hereby, our proposed Smart Intruder Detection System combines computer vision, patience based detection, real-time communication through Twilio, adaptive morphological operations, video recording, and performance monitoring. This amalgamation aims to create a cutting-edge security solution that not only identifies potential security threats but also enables rapid response, real-time communication, and continuous assessment of security effectiveness. The proposed system stands as a testament to the evolution of intelligent security solutions in the face of modern challenges.

**6. Methodology**

1. Problem Definition:

• Clearly define the problem and objectives of the intruder detection system.

• Identify the need for real-time detection and timely alerts.

2. Hardware and Software Setup:

• Set up the necessary hardware components, including cameras or sensors for

capturing video streams.

• Configure the software environment, including computer vision libraries like

OpenCV and Twilio for real-time communication.

3. Data Collection:

• Capture video streams from the cameras or sensors placed in the surveillance area.

• Ensure consistent and high-quality data acquisition for accurate analysis.

4. Preprocessing:

• Apply preprocessing techniques to improve the quality of video data.

• Techniques may include noise reduction, image stabilization, and frame rate

adjustment.

5. Computer Vision Analysis:

• Utilize computer vision techniques for intruder detection.

• Implement background subtraction and contour detection algorithms to identify

moving objects.

• Employ adaptive morphological operations to refine detected regions and reduce

noise.

6. Patience-Based Detection:

• Implement a patience mechanism to eliminate transient disturbances and reduce

false positives.

• Require consecutive intruder detections before triggering an alert, ensuring

reliability in varying environmental conditions.

7. Alerting System with Twilio:

• Integrate Twilio, a cloud communications platform, for real-time alerting.

• Configure Twilio to send SMS alerts when an intruder is detected.

• Include information like the location and timestamp in the alert message.

8. Video Recording:

• Implement video recording capabilities for evidence collection.

• Record video footage when an intrusion is detected, ensuring a visual record of

security incidents.

9. Performance Monitoring:

• Develop a user interface or dashboard to display critical performance metrics.

• Metrics may include frames per second (FPS), current room occupancy status, and

alert history.

• Allow users to continuously assess the system's effectiveness.

10. Testing and Evaluation:

• Thoroughly test the system in real-world scenarios to evaluate its accuracy and

reliability.

• Use various intrusion scenarios, including different lighting conditions and object

sizes, to assess system performance.

11. Deployment:

• Deploy the system in the target environment, such as homes, offices, or public spaces.

• Ensure proper installation and integration with existing security infrastructure.

12. Maintenance and Updates:

• Establish a maintenance schedule for hardware and software components.

• Continuously update and improve the system based on user feedback and emerging

technologies.

13. User Training:

• Provide user training to ensure that individuals or organizations can effectively use

the system and respond to alerts.

14. Documentation:

• Create comprehensive documentation, including user manuals and troubleshooting

guides, for system users and administrators.

15. Monitoring and Support:

• Offer ongoing monitoring and support to address any issues, provide software

updates, and ensure the system's long-term functionality.

1. **Results**

The Smart Intruder Detection System, incorporating advanced computer vision with OpenCV, demonstrates remarkable accuracy in distinguishing potential security threats from normal movements in real-time video streams. A unique patience-based mechanism minimizes false positives by requiring consecutive intruder detections before triggering alerts. Leveraging Twilio for instant SMS alerts ensures swift response to security incidents, whether on-site or remotely monitored. Adaptive morphological operations refine detected regions, adapting to changing lighting conditions and reducing noise. The system's video recording feature provides valuable evidence for incident reviews. With a user-friendly interface displaying key metrics and real-time performance monitoring, this system creates a safer environment by combining cutting-edge technologies for effective intrusion detection and rapid response.

**8. Conclusion and Future Scope**

**Conclusion**

The Smart Intruder Detection System represents a significant stride in the realm of intelligent security solutions, leveraging cutting-edge technologies to address the complexities associated with intrusion detection. Through the fusion of computer vision, patience-based detection, real time communication via Twilio, adaptive morphological operations, and video recording capabilities, the system demonstrates a holistic approach to security monitoring. The results of the evaluations highlight the system's prowess in accurately identifying potential security threats while minimizing false alarms, thanks to the patience-based intruder detection mechanism. The integration of Twilio ensures swift and reliable real-time communication, allowing users to respond promptly to security incidents, irrespective of their physical location. The adaptive morphological operations contribute to the system's resilience in dynamic environments, adapting to varying lighting conditions and effectively reducing noise levels. Moreover, the video recording feature not only enhances the system's evidentiary value but also extends its utility beyond real-time monitoring, providing a comprehensive security solution. Performance monitoring metrics offer users insights into the system's effectiveness, allowing for continuous assessment and informed decision-making. Despite these achievements, it is crucial to acknowledge certain limitations and areas for improvement. Ongoing refinements to enhance processing speed, user interface intuitiveness, and scalability considerations will be imperative for the sustained success of the Smart Intruder Detection System.

**Future Scope**

The project lays the foundation for future advancements and refinements in intelligent security

systems. The following avenues present promising directions for future research and

development:

• Multi-Sensor Fusion: Consider incorporating data from multiple sensors, such as

infrared and acoustic sensors, to create a more comprehensive and robust intrusion

detection system.

• User-Centric Interface Design: Focus on refining the user interface to enhance user

experience, ensuring that security personnel can efficiently interact with and manage

the system.

• Scalability and Integration with Smart Home Systems: Explore the scalability of the

system for deployment in larger settings and investigate seamless integration with

existing smart home systems for broader applicability.

**9. References**

[1] Tahir, S. M., Shen, O. P., Yang, L. C., & Karuppiah, E. K. (2013). Implementation of

intrusion detection system in CUDA for real-time multinode streaming. In Proceedings of the

IEEE Conference on Systems, Process & Control (ICSPC) (pp. 97–102). [2]. Keisham, K., &

Dixit, S. (2016). Recognition of Handwritten English Text U Minimisation. Advances in

Intelligent Systems and Computing, 607–614.

[2] Hariprakash, R., Ananthi, S., & Padmanabhan, K. (2011). An economical wireless network

monitored scheme for camera-based intrusion detection at unattended sites. In Proceedings of the IEEE International Conference on Computer Applications and Industrial Electronics

(ICCAIE) (pp. 150–155).

[3] Zhang, Y.-L., Zhang, Z.-Q., Xiao, G., Wang, R.-D., & He, X. (2015). Perimeter intrusion

detection based on intelligent video analysis. In Proceedings of the IEEE 15th International

Conference on Control, Automation and Systems (ICCAS) (pp. 1199–1204).

[4] Schutte, J., & Scholz, S. (2009). Guideway intrusion detection. IEEE Vehicular Technology

Magazine, 4(3), 76–81.

[5] Kaneda, K., Nakamae, E., Takahashi, E., & Yazawa, K. (1990). An unmanned watching

system using video cameras. IEEE Computer Applications in Power, 3(2), 20–24.

[6] ALshukri, D., Sumesh, E., Krishnan, P., et al. (2019). Intelligent border security intrusion

detection using IoT and embedded systems. In Proceedings of the IEEE 4th MEC International

Conference on Big Data and Smart City (ICBDSC) (pp. 1–3).

[7] Deshmukh, R., Kamdi, S., Pingle, M., Rajebhosale, S., & Bhosale, A. (2018). Intelligent

surveillance system using energy-efficient intrusion detection and tracking techniques. In

Proceedings of the IEEE 2nd International Conference on Electronics, Communication and

Aerospace Technology (ICECA) (pp. 1214–1218).

[8] Chen, H., Chen, D., & Wang, X. (2016). Intrusion detection of a specific area based on

video. In Proceedings of the IEEE 9th International Congress on Image and Signal Processing,

Biomedical Engineering and Informatics (CISP-BMEI) (pp. 23–29).

[9] Kongurgsa, N., Chumuang, N., & Ketcham, M. (2017). Real-time intrusion detecting and

alert system by image processing techniques. In Proceedings of the IEEE 10th International

Conference on Ubi-media Computing and Workshops (UbiMedia) (pp. 1–6).