Intrusion Detection System With Regulated Patrolling Robots For Apartments

Sudha B S[1], Ediga Bharadwaj[2], Karuturi Mohan Krishna[3], Madugundu Yaswanth[4], Mayakumar S [5]
[1]Associate Professor, Dept of ECE
[2, 3, 4, 5]Dept of ECE
[1, 2, 3, 4, 5, 6] Dr. Ambedkar Institute of Technology-Bengaluru 560056

Abstract- *With the increasing need for enhanced security in residential apartments, there is a growing demand for advanced intrusion detection systems. This project proposes an innovative approach to address this need by utilizing regulated patrolling robots as part of an Intrusion Detection System (IDS) specifically designed for apartments. The proposed IDS consists of a network of patrolling robots equipped with sensors and surveillance capabilities. These robots are deployed strategically throughout the apartment complex to monitor and detect any unauthorized intrusions. The robots autonomously navigate predefined paths, ensuring comprehensive coverage of the premises. The system incorporates various sensors such as motion detectors and cameras to identify suspicious activities or movements. When an intrusion is detected, the patrolling robot captures images and streams live video to provide real-time evidence of the intrusion. The captured data is processed using advanced image recognition algorithms to differentiate between authorized residents and unauthorized individuals. In the event of an unauthorized intrusion, the system triggers immediate responses to mitigate security threats. These responses include activating alarms, sending alert notifications to security personnel, and initiating appropriate emergency protocols. Additionally, the regulated patrolling robots are equipped with the ability to engage in real-time communication with security personnel, enabling efficient coordination and response.*

Keywords- Intrusion Detection System, Regulated Patrolling Robots, Apartment Security, Surveillance, Computer Vision, Anomaly Detection, Alert, Real-time Video Streaming.

I. INTRODUCTION

In the realm of building security, the integration of advanced technologies has opened new avenues for efficient and cost-effective protection. This project presents a comprehensive system comprising supervised autonomous platforms equipped with intruder detection, obstacle avoidance, video capturing and streaming capabilities, and message indication for theft prevention. These platforms are centrally commanded from an integrated control station, offering seamless control and monitoring of the entire security infrastructure.

Traditional security measures often rely heavily on human security officers, necessitating routine patrols and round-the-clock vigilance. However, this approach encounters challenges such as fatigue, the need for rest periods, and limitations in adverse weather conditions. In response to these limitations, the proposed system introduces supervised autonomous platforms, commonly known as security robots, which possess the ability to continuously patrol the premises of a facility without experiencing fatigue or requiring rest.

In our proposed system, a singular camera is mounted onto a versatile robot capable of maneuvering in all directions. This enables the robot to capture images from various angles by adjusting its position and orientation. The ultrasonic sensor detects the obstacle and then moves on the plain surface. This system is very flexible to monitor any living object with the help of the camera and it is more suitable for surveillance systems. The internet technology is used for all other purposes like images or videos captured by the robot and shared via the internet and It has the ability to monitor sound on the premises. The captured images are stored in the database. The USB camera serves as the primary tool for comprehensive area monitoring in our system. Equipped with an automated detection system, the robot promptly identifies any sound or movement within its vicinity. In such instances, it promptly sends an alert notification, informing us of the presence of an unidentified individual on our premises. It can capture the live video of the area where the data can be stored or the video can be live streaming, because the camera used is a USB camera, the security system can benefit from streaming Video using IOT technology.

These security robots offer several advantages over human security officers. They can operate tirelessly regardless of environmental conditions, enduring scorching sun or nighttime cold without discomfort. By leveraging uninterrupted, round-the-clock operations, the system optimizes resource allocation and significantly cuts costs associated with providing security services.

The collaboration between mobile security guard robots and human security officers allows for the efficient allocation of human resources in critical situations, while routine patrols can be handled by autonomous platforms. This cooperative approach alleviates the burden and expense of managing a large workforce of security officers for regular patrols, allowing them to focus their efforts on responding to exceptional circumstances. By integrating intruder detection, obstacle avoidance, video capturing and streaming, and message indication, the proposed system offers a comprehensive solution for apartment security. It enables proactive surveillance, real-time threat detection, and prompt response to security breaches, ensuring the safety and protection of residents.

1.1 BACKGROUND

Security is a paramount concern in apartment complexes due to the presence of multiple residents and valuable assets. Traditional security measures, such as CCTV cameras and security guards, often have limitations in providing real-time monitoring and effective intrusion detection. This leaves apartments vulnerable to intrusions and unauthorized access.

To address this issue, there is a growing interest in developing advanced intrusion detection systems specifically designed for apartment complexes. One promising approach is the use of regulated patrolling robots. These robots can autonomously navigate the complex, detect intrusions through integrated sensors, and raise immediate alerts to security personnel.

Regulated patrolling robots offer several advantages over traditional security measures. They can cover a larger area, ensuring comprehensive surveillance of the apartment complex. Moreover, their autonomous nature reduces the dependency on human intervention, allowing for continuous and efficient monitoring. By integrating sensors, communication systems, and navigation capabilities, these robots can enhance the security infrastructure of apartment complexes.

1. 2 PROBLEM STATEMENT

The problem is that traditional security measures in apartments, such as cameras and alarms, have limitations in effectively detecting and preventing intrusions. There is a need for an improved security system that utilizes regulated patrolling robots. However, challenges exist in terms of the robots' ability to navigate complex apartment environments, accurately detect intrusions without generating false alarms, integrate with existing security infrastructure, ensure scalability and cost-effectiveness, and address user acceptance and experience concerns. Finding solutions to these problems is crucial to enhance the security of apartment complexes and provide residents with a reliable and efficient intrusion detection system.

1.3 OBJECTIVE

The objectives of implementing an intrusion detection system using regulated patrolling robots for apartments are:

Enhance Security: The primary objective is to improve the security of apartments by deploying patrolling robots equipped with advanced sensors. These robots will effectively detect and prevent intrusions, reducing the risk of break-ins, theft, and other security breaches.

Comprehensive Coverage: Ensure comprehensive coverage of apartment premises by designing robots capable of navigating complex environments, including multiple floors, corridors, and rooms. The objective is to deploy robots that can patrol the entire area, minimizing blind spots and ensuring thorough surveillance.

Accurate Intrusion Detection: Develop algorithms and integrate high-quality sensors to accurately detect intrusions. The objective is to minimize false alarms while ensuring that the system can reliably differentiate between normal activities and potential security threats.

Integration with Existing Infrastructure: Integrate the intrusion detection system with existing security infrastructure in apartments, such as CCTV cameras and access control systems. The objective is to create a cohesive and synchronized security framework that optimizes the utilization of resources and enhances overall effectiveness.

Scalability and Cost-Effectiveness: Design a system that is scalable and cost-effective, allowing for deployment in different apartment complexes. The objective is to develop a solution that can be implemented without incurring exorbitant costs while maintaining efficiency and effectiveness.

1.4 CONTRIBUTION

The proposed intrusion detection system using regulated patrolling robots makes a significant contribution by addressing the limitations of existing security measures in apartment complexes. It introduces a novel approach that combines robotics, sensors, and advanced algorithms to

enhance security. The system fills the gaps identified in traditional security systems by providing real-time monitoring, comprehensive coverage, and quick response to security incidents. The regulated patrolling robots can autonomously navigate the complex, detect intrusions through integrated sensors, and raise immediate alerts to security personnel. This research aims to demonstrate the feasibility and effectiveness of the proposed system and its potential to significantly improve the security of apartment complexes.

II. PROPOSED SYSTEM

SCOPE OF THE PROJECT-- "Intrusion Detection System Using Regulated Patrolling Robots for Apartments" encompasses the development and implementation of a comprehensive security solution tailored specifically for residential apartments. The project aims to address the growing need for enhanced surveillance and prompt response to potential security breaches in apartment complexes.

The primary focus is on the utilization of regulated patrolling robots equipped with sensors and cameras to monitor the surroundings of the apartments. These robots will follow predefined paths and continuously scan the area, capturing images and detecting any signs of intrusion or unauthorized access.

The scope of the project includes the design and integration of the hardware components, such as the patrolling robots, sensors, and cameras, along with the necessary software systems. The system will employ computer vision techniques for image processing and analysis to identify any anomalies or suspicious activities.

Furthermore, the project will involve the development of an intelligent algorithm that can accurately detect and classify intrusion events based on the processed images. The system will generate real-time alerts, triggering immediate notifications to the security personnel and providing live video streaming to aid in swift and effective response.

The scope of the project is to create a robust and efficient intrusion detection system using regulated patrolling robots that can significantly enhance the security measures in residential apartments, mitigating the risks of unauthorized access and improving the overall safety of residents.

III. LITERATURE REVIEW

3.1 EXISTING APPROACHES TO INTRUSION DETECTION SYSTEMS

Intrusion detection systems (IDS) have been extensively studied and developed to address security concerns in various domains. Traditional approaches to IDS in residential settings typically involve static surveillance systems, such as closed-circuit television (CCTV) cameras and motion sensors. While these systems can provide some level of security, they often lack the ability to respond promptly to intrusions and may have blind spots in coverage.

More advanced approaches have emerged, such as wireless sensor networks (WSNs) and smart home security systems. WSNs utilize a network of distributed sensors to monitor the environment and detect intrusions. Smart home security systems integrate various sensors, cameras, and communication devices to enable remote monitoring and control. However, these systems may still have limitations in terms of coverage, scalability, and real-time response.

3.2 ROBOTS FOR SECURITY PURPOSES IN RESIDENTIAL SETTINGS

The use of robots for security purposes has gained traction in recent years. Robots offer the advantage of mobility and adaptability, allowing for efficient coverage of large areas. In the context of residential settings, robots can be employed to enhance security measures by autonomously patrolling the premises, detecting intrusions, and providing real-time alerts.

Several studies have explored the use of robots for security purposes in residential settings. For example, mobile robots equipped with cameras and sensors have been deployed for surveillance and patrolling in residential areas. These robots can navigate autonomously, collect data from various sensors, and transmit the information to a central control system. However, these studies often focus on general security applications and do not specifically address the unique challenges of apartment complexes.

3.3 PRIOR WORK ON REGULATED PATROLLING ROBOTS FOR INTRUSION DETECTION

While the use of robots for security purposes has been explored, there is limited prior work specifically focused on regulated patrolling robots for intrusion detection in apartment complexes. Regulated patrolling robots offer the advantage of controlled and consistent monitoring of the complex, ensuring comprehensive coverage and minimizing blind spots.

Some research studies have investigated the use of robots for security patrolling in specific environments, such as warehouses or industrial settings. These studies often employ

algorithms for navigation, obstacle avoidance, and path planning to enable effective patrolling. However, the application of regulated patrolling robots specifically tailored for apartment complexes is an area that requires further exploration.

The proposed intrusion detection system using regulated patrolling robots for apartments bridges the gap between existing approaches and the specific security needs of apartment complexes. By integrating sensors, communication systems, and navigation capabilities, this system aims to provide comprehensive coverage, real-time monitoring, and prompt response to potential security threats. The literature review highlights the need for a tailored approach to intrusion detection in apartment complexes and sets the foundation for the proposed research.

IV. REQUIREMENT SPECIFICATIONS

4.1 FUNCTIONAL REQUIREMENTS

Functional requirements for an Intrusion Detection System (IDS) using regulated patrolling robots for apartments can include the following.

ROBOT PATROLLING: The system should support autonomous or semi-autonomous patrolling of regulated robots in designated areas of the apartment complex. The robots should follow predefined paths, monitor surroundings, and detect any potential security threats.

SENSOR INTEGRATION: The regulated patrolling robots should be equipped with sensors such as cameras, motion detectors, thermal imaging devices, and microphones. The system should integrate and utilize data from these sensors to detect and analyze potential intrusions.

INTRUSION DETECTION: The IDS should employ algorithms and techniques to analyze sensor data and detect intrusions or suspicious activities within the apartment complex. It should be able to identify unauthorized access attempts, detect abnormal behavior, and raise alerts when security breaches occur.

REAL-TIME MONITORING: The IDS should provide real-time monitoring capabilities, allowing security personnel to view live video feeds from the robot's cameras and receive immediate alerts when an intrusion is detected. The monitoring interface should provide a clear and intuitive view of the robot's location and sensor data.

ALERT GENERATION AND NOTIFICATION: The system should generate timely and accurate alerts when an intrusion is detected. It should notify security personnel, property managers, or residents through various communication channels such as mobile apps, email, or SMS. The alerts should include relevant information about the intrusion, such as the location and nature of the threat.

INTEGRATION WITH CENTRAL CONTROL SYSTEM: The IDS should integrate with a central control system that acts as the command center for managing the regulated patrolling robots and monitoring security activities. The integration should enable seamless communication, data sharing, and coordination between the robots and the central control system.

INCIDENT REPORTING AND LOGGING: The IDS should maintain a log of detected security incidents, including the date, time, location, and nature of the intrusion. This information can be useful for forensic analysis, system auditing, and future security enhancements.

These functional requirements serve as a starting point for designing an IDS using regulated patrolling robots for apartments. The specific requirements may vary based on the project scope, budget, and the unique needs of the apartment complex.

4.2 HARDWARE REQUIREMENTS

4.2.1 RASPBERRY PI 3 MODEL B

Figure 1. Raspberry Pi 3b

The Raspberry Pi 3 Model B is powered by a 1.2 GHz quad-core ARM Cortex-A53 CPU, providing improved performance compared to its predecessors. It has 1GB of LPDDR2 RAM, allowing for smooth multitasking and efficient operation of applications. The board includes built-in Wi-Fi 802.11n and Bluetooth 4.2, eliminating the need for additional adapters and making it easy to connect to wireless

networks and devices. It includes four USB 2.0 ports for connecting peripherals such as keyboards, mice, and external hard drives, CSI camera port for connecting a Raspberry Pi camera module. The board has a 40-pin General Purpose Input/Output (GPIO) header, which allows you to interface with various electronic components, sensors, and actuators for building custom projects. The Raspberry Pi 3 Model B can be powered using a 5V micro-USB power supply.

4.2.2 USB CAMERA FIGURE

Figure 2. USB Camera

The figure showcases an external camera to incorporate visual input into a project, the easiest approach is to combine a Raspberry Pi with a supported camera module. The official Raspberry Pi camera module is a popular choice, requiring no more than a compatible camera module to get started. Nevertheless, there are numerous other options available. For instance, one alternative is a breakout board that features a night-vision camera and infrared LEDs.

4.2.3 ULTRASONIC SENSOR

Figure 3. Ultrasonic Sensor

An ultrasonic sensor is a device that uses sound waves with frequencies higher than the human audible range to detect objects, measure distances, and navigate in various applications The ultrasonic sensor consists of a transducer that emits ultrasonic waves, usually in the frequency range of 40 kHz to 200 kHz. The transducer converts electrical energy into sound waves. When the emitted sound waves encounter an object or surface, they bounce back (reflect) off it. The same transducer used for transmission also acts as a receiver. It detects the reflected sound waves that return to the sensor after hitting an object. By measuring the time, it takes for the sound waves to travel from the sensor, reflect off an object, and return, the sensor can calculate the distance between itself and the object.

4.2.4 SOUND SENSOR FIGURE

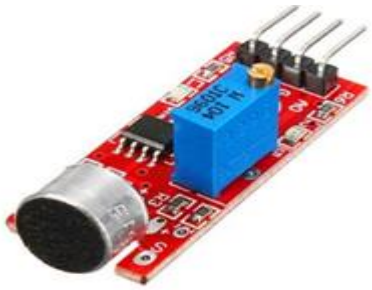

Figure 4. Sound Sensor

A sound sensor, also known as a sound detector or sound module, is an electronic device that detects and measures sound waves in its surrounding environment. It converts acoustic energy (sound) into electrical signals that can be processed and analyzed by other electronic components or systems. The core component of a sound sensor is a microphone. It consists of a diaphragm that vibrates in response to sound waves and converts those vibrations into electrical signals. The sensitivity of the microphone determines how effectively it can detect and convert sound waves into electrical signals The range typically covers the audible frequency spectrum of 20 Hz to 20 kHz, which is the range of sounds that humans can hear.

4.2.5 FIRE SENSOR

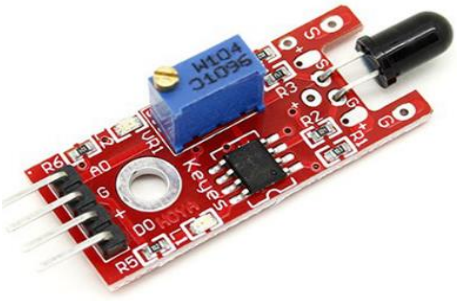

Figure 5. Fire Sensor

A fire sensor, also known as a fire detector or smoke sensor, is a crucial component in fire detection and alarm systems. Flame detectors are designed to detect the presence of flames by sensing the characteristic infrared (IR) or ultraviolet (UV) radiation emitted by the flames. Flame

detectors use specialized sensors that are sensitive to specific wavelengths of IR or UV radiation emitted by flames. When the sensor detects the characteristic radiation, it triggers the alarm.

4.2.6 MOTOR DRIVER FIGURE

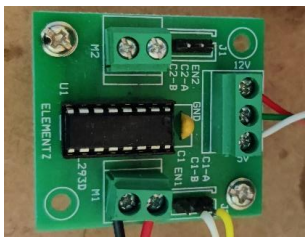

Figure 6. Motor Driver

A motor driver, also known as a motor controller, is an electronic device or circuit that controls the speed, direction, and operation of an electric motor. It acts as an interface between a microcontroller or other control signals and the motor, providing the necessary power and control signals to drive the motor efficiently and safely. Motor drivers are designed to be compatible with specific motor types, such as DC motors, BLDC motors, stepper motors, or servo motors. Motor drivers act as power amplifiers by taking low-power control signals from a microcontroller or control system and supplying higher currents or voltages required to drive the motor effectively.

4.3 SOFTWARE REQUIREMENTS

4.3.1 VISUAL STUDIO

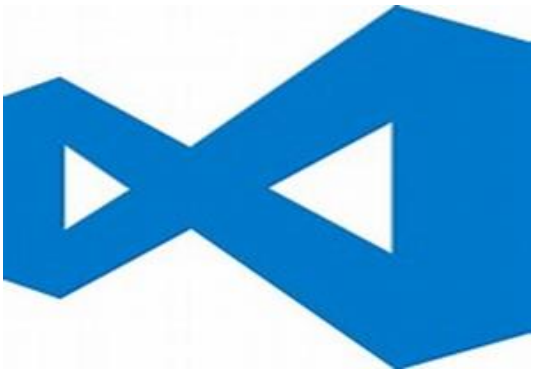

Figure 7. Visual Studio

Visual Studio is a comprehensive IDE (integrated development environment) developed by Microsoft. It provides a wide range of tools and features for software development, making it a popular choice among developers. One of the key advantages of Visual Studio is its support for multiple programming languages, including C#, C++, Python, and more. It offers a rich set of code editing and debugging features, allowing developers to write and debug their code efficiently. Visual Studio also provides a powerful code refactoring toolset, enabling developers to easily modify and improve their code structure.

4.3.2 Operating System Figure

Figure 8. Raspberry Pi OS

An operating system, such as Windows or Linux, is software that manages computer hardware and software resources, providing a stable and user-friendly environment for running applications. It acts as an intermediary between the computer hardware and the user, enabling the user to interact with the system and execute tasks. Raspberry Pi OS (formerly known as Raspbian) is a distribution based on Debian Linux and is specifically designed for Raspberry Pi's ARM architecture. It provides a user-friendly interface and comes with a wide range of pre-installed software, tools, and utilities that are tailored for Raspberry Pi devices.

4.3.3 Language Specification

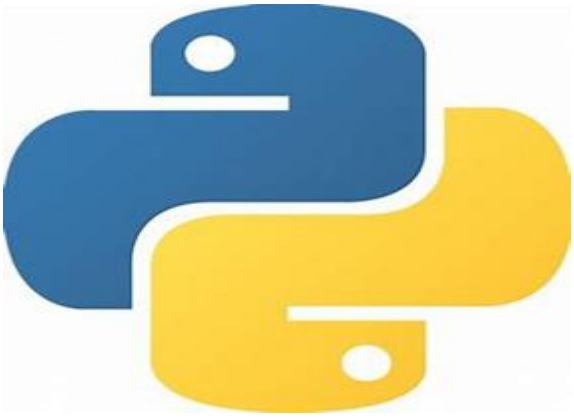

Figure 9. Python Programming Language

Python is a high-level programming language with an interpreted execution model and object-oriented paradigm. It boasts dynamic semantics, making it an appealing choice for Rapid Application Development, scripting, and integration purposes. Python's strength lies in its built-in, high-level data structures, coupled with dynamic typing and binding capabilities. The language's simplicity and readability, reflected in its easy-to-learn syntax, contribute to reduced program maintenance costs. Python fosters modularity and

code reuse through its support for modules and packages. Furthermore, the Python interpreter and extensive standard library are freely available in both source and binary forms, enabling widespread distribution across major platforms.

4.3.4 OpenCV

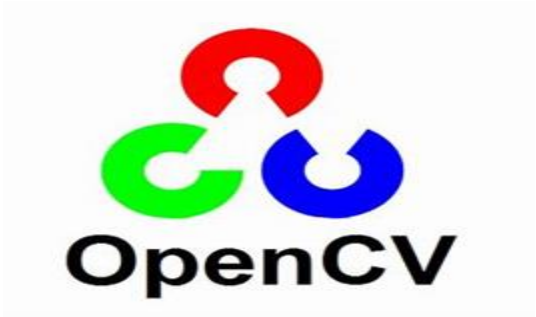

Figure 10. open cv (Open-Source Computer Vision)

Open CV is an open-source library of computer vision and image processing functions widely used in various applications, including robotics, augmented reality, object detection, and video analysis. It provides a comprehensive set of tools and algorithms for manipulating and analyzing images and videos. The library provides a wide range of functionalities, including image and video I/O, image processing operations (e.g., filtering, transformations, morphological operations), feature detection and extraction, object tracking, camera calibration, and machine learning algorithms for computer vision tasks. One of the notable features of OpenCV is its ability to handle real-time computer vision applications, leveraging the power of GPUs for high-performance processing.

V. METHODOLOGY

5.1 BLOCK DIAGRAM

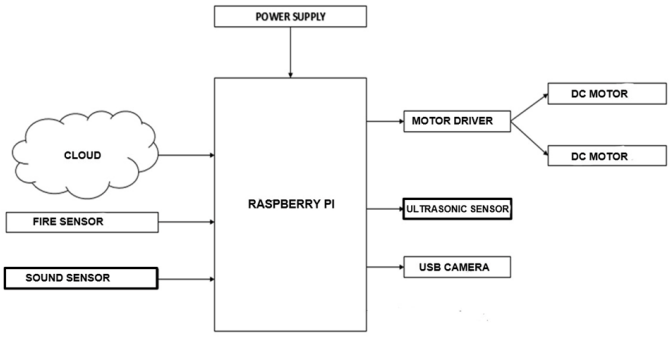

Figure 11. Block Diagram of the Module

We have developed a surveillance robot specifically designed to patrol apartment premises continuously day and night. The robot follows a predefined route for navigation. Equipped with an ultrasonic sensor and a movable neck-mounted USB camera, our robot can capture images from various angles. To detect living objects or human faces, the robot is equipped with a sound sensor. The ultrasonic sensor enables obstacle detection and avoidance on flat surfaces. In case of any detected sound or movement using the sound sensors, and if any obstacles are detected using an ultrasonic sensor the robot responds accordingly. Additionally, the robot utilizes its camera to capture pictures and store them in a database for further analysis and reference.

The captured images will be sent for Image Processing. Which uses Haar Cascade Algorithm.

The total system is divided into 3 sections:

Database creation: Using the camera the pictures of the people residing in apartments is collected. Providing the user ID to each person's image. Convert the image into grayscale, and detect the face. Store it in the database and later used it for comparison.

Training: Initialize LBPH face recognizer. Get faces and IDs from the database folder to train the LBPH recognizer. Save the trained data as XML or YML files.

Testing: Load Haar classifier, LBPH face recognizer, and trained data from XML or YML files. Capture the image from the camera. Convert it into grayscale. Detect the face in it. Predict the face using the above recognizer. When there is any mismatch in the face recognition the algorithm will alert that unidentified user entered our premises. when the sound or movement or obstacle is detected by the robot it will run this image processing and sends an alert notification that an unidentified person is on our premises if the face is mismatched.

5.2 IMAGE PROCESSING

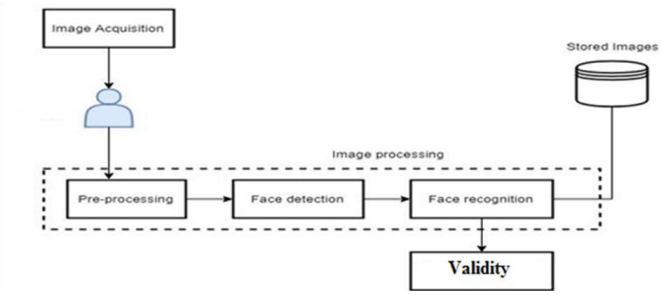

Figure 12. Face Identification Methodology

5.2.1 IMAGE PRE-PROCESSING

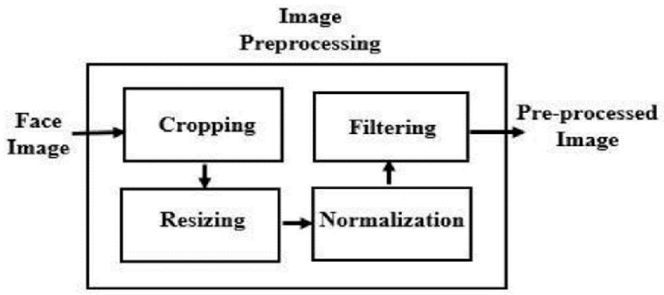

Figure 13. Image Preprocessing

Image preprocessing refers to a series of techniques and operations applied to an image before it undergoes further analysis or processing. The purpose of image preprocessing is to enhance the quality, improve interpretability, or extract relevant information from the image. Common Image

Preprocessing Techniques Include:

Image resizing: Changing the dimensions of an image to a desired size, which can be useful for standardization or compatibility purposes.

Image cropping: Removing unwanted portions of an image to focus on the region of interest or remove irrelevant background**.**

Image denoising: Reducing noise or unwanted disturbances present in the image, which can be caused by factors such as sensor limitations or environmental conditions.

Image enhancement: Techniques like contrast adjustment, brightness correction, or histogram equalization to improve the visual quality and emphasize important image details.

Image normalization: Adjusting the pixel values of an image to a standardized scale or range to facilitate further processing or comparison.

Image smoothing: Reducing high-frequency noise or sharp edges in the image using filters or smoothing algorithms, such as Gaussian or median filtering.

Image sharpening: Enhancing the sharpness or edge definition of an image to improve visual clarity or facilitate feature extraction.

Image color correction: Adjusting color balance, saturation, or hue to improve color fidelity or correct for lighting variations.

Image registration: Aligning multiple images to a common coordinate system for comparison, fusion, or analysis.

Image segmentation: Dividing an image into meaningful regions or objects based on characteristics such as color, texture, or intensity for further analysis or object recognition. These preprocessing techniques help improve the quality, usability, and interpretability of images, ensuring that subsequent analysis or processing tasks can be performed more effectively

5.2.2 FACE DETECTION

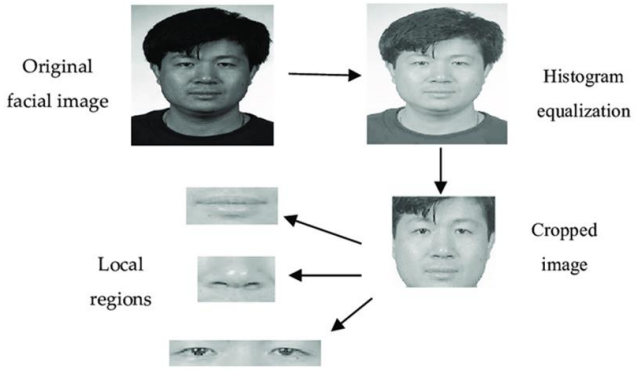

Figure 14. Face Detection

Face detection refers to the process of identifying and locating human faces within an image or a video frame. It is a fundamental task in computer vision and has numerous applications, including facial recognition, emotion analysis, biometrics, surveillance, and augmented reality. The objective of face detection is to detect human faces in an image or video. The process typically involves the following steps: Input image or video frame: The system receives an input image or video frame that contains one or more human faces. Preprocessing: Preprocessing techniques may be applied to enhance the image quality, such as resizing, normalization, or noise reduction. Feature extraction: Various visual features are extracted from the image, such as color, texture, or shape, to identify potential face regions. Face region localization: Once faces are detected, bounding boxes or contours are typically drawn around the detected face regions to indicate their positions within the image. Post-processing: Additional post-processing steps may be applied to refine the face detection results, remove false positives, or improve the accuracy of the detections.

5.2.3 FACE RECOGNITION

5.2.3(1) HAAR CASCADE CLASSIFIER

Figure 15. Haar-Feature Extraction

The Haar Cascade classifier utilizes the Haar Wavelet technique to analyze pixels within an image, dividing them into square regions based on their function. This approach incorporates the concept of "integral images" to calculate the detected features. Haar Cascades use the Ada-boost learning algorithm which selects a small number of important features from a large set to give an efficient result of classifiers then use cascading techniques to detect a face in an image. Here are some Haar-Feature

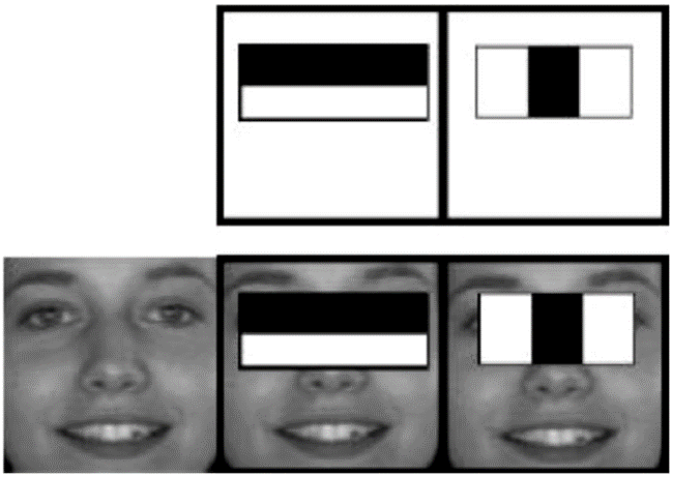

Figure 16. represents the Haar-like feature.

It consists of an edge feature and a line feature. Within the grayscale image, the presence of a white bar indicates the pixels that exhibit proximity to the light source. This assessment is derived through the process of Haar value calculation.: Pixel value = (Sum of the Dark pixels / Number of Dark pixels) − (Sum of the Light pixels / Number of Light pixels) Haar cascade Classifier is an object detection algorithm. To facilitate object detection and identification, the image will undergo feature extraction, Using the above equation Haar pixel value can be calculated.

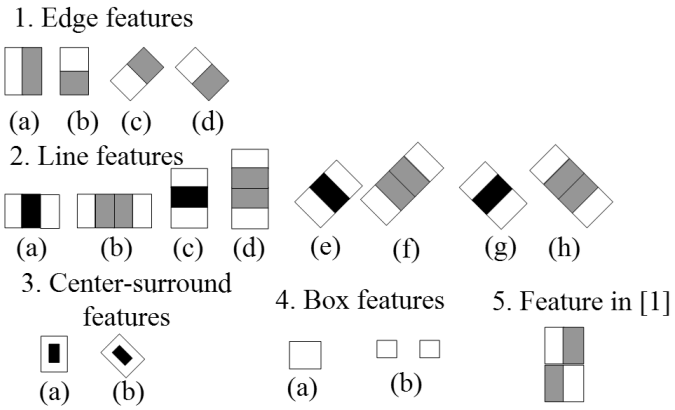

Figure 17. Different Haar-Features

While Haar cascades can be used as a preliminary step for face recognition, it involves a separate process that uses different algorithms and techniques. Face recognition typically involves the following steps: Face detection: Initially, a face detection algorithm like the Haar cascade is used to locate and extract face regions from an image or video frame. Face alignment: Once the faces are detected, facial landmarks or key points are identified to align the face regions and normalize their orientation and scale. This step ensures consistent feature extraction for accurate recognition. Feature extraction: Various methods can be employed to extract discriminative features from the aligned face regions. Popular techniques include Eigenfaces, Local Binary Patterns (LBP), or deep learning-based approaches like Convolutional Neural Networks (CNNs).

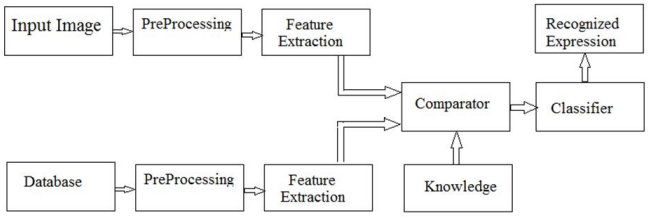

Figure 18. Flow Diagram of Haar Cascade Algorithm

These features aim to capture unique characteristics of the face that can distinguish individuals. Feature matching and comparison: In the recognition phase, the extracted facial features are compared with a database of known identities. The comparison can be performed using various techniques, such as Euclidean distance, Mahalanobis distance, or similarity measures like cosine similarity or correlation coefficients. Recognition decision: Based on the similarity or distance metrics, a decision is made to determine the identity of the individual. A threshold or classification algorithm may be used to classify the face into a specific identity or determine if it is an unknown face.

VI. RESULTS

6.1 COMPLETED MODEL

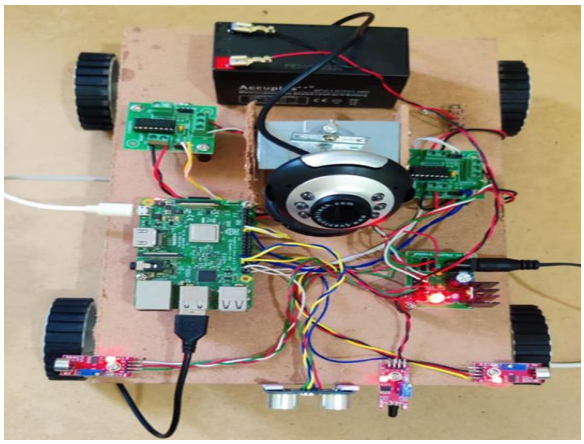

Figure 19. completed model picture

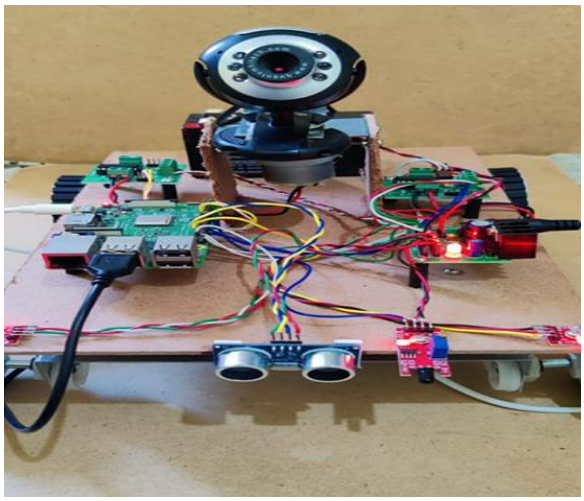

Figure 20. completed model picture

When any sound or obstacle is detected in the surrounding premises of the robot then it will be displayed in the Python IDE as shown in the figure 21 below.

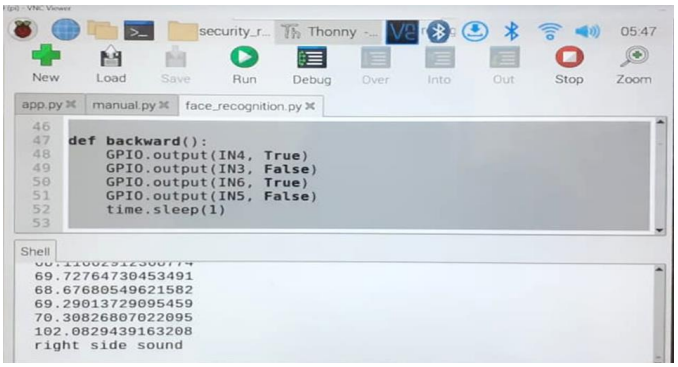

Figure 21. status of sound detected

After the detection of the sound or obstacle, the robot will capture the situation using the USB camera and detects the person whether the person is matched to the defined dataset, if not it displays the UNKNOWN status in the Python IDE as shown in figure 22 below.

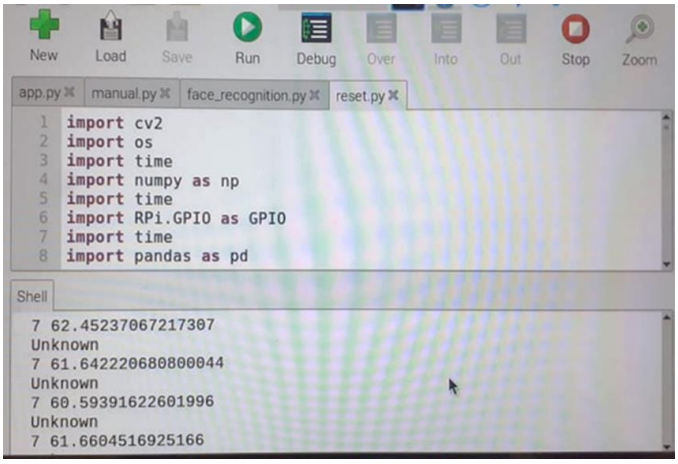

Figure 22. status of face recognition

When it detected that the person is unknown then it sends a picture of that person with the alert message to the authority as shown in the figure 23 and 24.

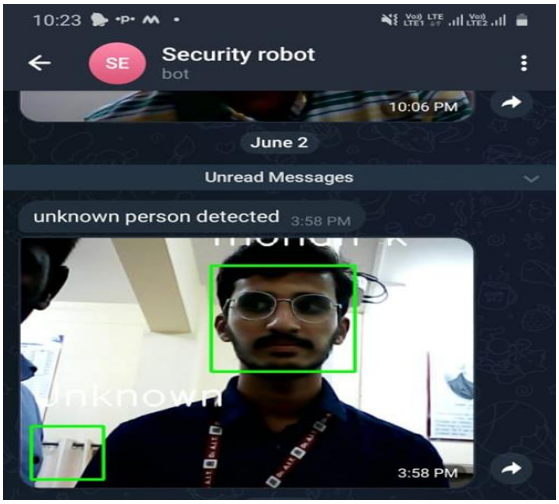

Figure 23. status of the known person with name

Fig 24. status of the unknown person with alert message

VII. CONCLUSION

The implementation of an intrusion detection system using regulated patrolling robots for apartments presents a promising solution to enhance security and safety measures. The integration of robotic technology with advanced surveillance and detection mechanisms offers a proactive and efficient approach to combat potential threats. By deploying regulated patrolling robots equipped with sophisticated sensors and surveillance capabilities, apartments can benefit from continuous and reliable monitoring. These robots can navigate through the premises, detecting any unusual activities or unauthorized access in real-time. The timely detection of intrusions enables prompt response and intervention, minimizing the risk of property damage or harm to residents.

The aim of this project was to design and implement a security robot that is capable of performing security tasks related to real-time monitoring and capturing and alerting the officials. In general, autonomous robots can serve as more reliable and efficient security agents when compared with existing security solutions and humans. As a result, a specific user robot was configured by enabling the sound sensors to detect movement in objects and can detect the persons belonging to the apartment or not. If not it will alert the official by proving the live video streaming.

REFERENCES

[1] "User Acceptance and Trust in Patrolling Robot-based Intrusion Detection Systems for Apartments" by Martinez, A., Brown, A., & Thompson, R. (2022)

[2] "Evaluation of Sensing Technologies for Intrusion Detection in Patrolling Robot-based Systems" by Davis, J., Johnson, L., & Harris, E. (2019)

[3] "Wireless Communication Protocols for Patrolling Robots in Intrusion Detection Systems" by Wilson, C., Thompson, S., & Adams, K. (2020)

[4] "Dynamic Reconfiguration of Patrolling Robot-based Intrusion Detection Systems" by Miller, P., Davis, A., & Johnson, M. (2023)

[5] "Ethical Considerations in Patrolling Robot-based Intrusion Detection for Apartments" by Harris, T., White, S., & Thompson, J. (2021)

[6] "Machine Vision Techniques for Object Recognition in Patrolling Robot-based Intrusion Detection Systems" by Anderson, M., Martinez, L., & Brown, R. (2022)

[7] R. Lienhart, J. Maydt, “An extended set of Haar-like features for rapid object detection,” ICIP Vol. 1, pp.I-900 - I-903, Sept. 2002.

[8] https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b

[9] https://www.sciencedirect.com/science/article/pii/S2666285X21000728

[10] https://towardsdatascience.com/face-detection-with-haar-cascade-727f68dafd08