Intrusion Detection System With Regulated Patrolling Robots For Apartments

Dr. Senthil Kumar[1], Mohamed Asheim[2], Nandha Gopal M[3], Nirmal Kumar[4]
[1]Professor, Dept of Computer Science
[2, 3, 4]Dept of Computer Science
[1, 2, 3, 4] Panimalar Engineering College Chennai, Tamilnadu, India

Abstract- *As people's concerns about security rise, more and more advanced intrusion detection systems are needed in residential structures. This study suggests a novel approach to bridge this gap: the use of controlled patrolling robots as a component of apartment-specific intrusion detection systems (IDS). The proposed IDS consists of an automated robot network capable of patrolling and conducting surveillance. These robots are placed intelligently throughout the apartment building to keep an eye out for any unwanted entry. The robots automatically cover the entire region by following pre-established courses. The system recognizes unusual movements or activities using a range of sensors, including webcams and motion detectors.*

When it detects an intruder, the patrolling robot records live footage and takes images of it. The collected data is processed using advanced picture recognition algorithms, which allow for the distinction between authorized and illegitimate users. Security risks are minimized as soon as the system detects an unauthorized entrance. These responses include activating alarms, alerting guards to approaching danger, and initiating the appropriate emergency protocols.

Security personnel and the controlled patrolling robots can communicate in real-time, which facilitates efficient coordination and response.

Keywords- computer vision, surveillance, anomaly detection, alerts, controlled patrolling robots, apartment security, intrusion detection system, real-time video streaming.

I. INTRODUCTION

Modern technologies have made cutting-edge protection options in the building security space more affordable and accessible. This design offers a comprehensive solution by deploying supervised autonomous platforms that can record and broadcast videos, avoid obstacles, identify intruders, and display anti-theft messaging. These platforms provide seamless control and monitoring of the whole security infrastructure because they are centrally administered from an integrated control station.

Conventional security methods typically rely significantly on human security officers, requiring continuous patrols and 24-hour attention. But there are problems with this strategy.

Difficulties include exhaustion, the requirement for downtime, and restrictions in inclement weather. The suggested solution addresses these issues by using security robots, often referred to as supervised autonomous platforms, which are able to continuously patrol a facility's grounds without growing weary or in need of a break.

Our proposed approach consists of mounting a single camera on top of a 360-degree mobile multifunctional robot. Because of this, the robot might adjust its orientation and location in order to take pictures from various angles. The ultrasonic sensor moves across the flat surface after determining the obstruction. This technique works well with surveillance systems and allows the camera to be used to monitor any type of living thing. All additional features, including sharing photos or videos that the robot captures and uploads and sound monitoring around the building, are made possible by the internet. The photographed images are stored in the database. The main part of our system for wide-area surveillance is the USB camera. An automated sensor system allows the robot to recognize sounds and movements in its environment. When that happens, we are promptly made aware of the presence of an unknown person on our property by an alert notice. Because it is a USB camera, it has the ability to send and record live video of the region where data may be kept. The security system can gain from transmitting video via Internet of Things technology.

Compared to human security guards, these security robots have a number of advantages. They are able to labor constantly in any weather condition, enduring the nighttime heat and cold without feeling uncomfortable. Through constant, round-the-clock activities, the system optimizes resource allocation and dramatically reduces security service provider expenses.

Even though autonomous platforms can perform regular patrols, the efficient use of human resources in emergency scenarios is made possible by the cooperation of mobile security guard robots and human security agents. Working together can cut down on the costs and effort involved in overseeing a large team of security officers during routine patrols, freeing officers to concentrate on handling unusual situations. The suggested system offers a comprehensive approach to apartment security by integrating message signaling, obstacle avoidance, video recording and streaming, and intruder detection. To protect the security and safety of the occupants, it enables proactive surveillance, real-time threat identification, and swift reaction to security breaches.

BACKGROUND

Security is a big worry since apartment complexes house a lot of people and valuable things. Sometimes real-time monitoring and efficient intrusion detection are limited by traditional security measures like CCTV cameras and security personnel. Apartments are therefore more susceptible to unlawful access and break-ins.

Security in apartment complexes is a big concern because they house a lot of people and valuable items. Real-time monitoring and efficient intrusion detection may occasionally be limited by conventional security measures like CCTV cameras and security personnel. Apartments are therefore more susceptible to break-ins and illegal entrances.

Increasingly, complex intrusion detection systems are being developed as a solution to this issue, particularly for apartment complexes. One potential tactic is to use remotely operated robots to patrol a certain region. These robots' inbuilt sensors allow them to autonomously explore complex areas, immediately alert security personnel to possible hazards, and identify intrusions.

PROBLEM STATEMENT

The problem originates from the fact that traditional apartment security systems, which mostly consist of cameras and alarms, are not accurate enough to detect and deter intruders. It is imperative to have an improved security system that uses robots under remote control to patrol. However, there are concerns over the robots' ability to navigate complicated housing complexes, identify intruders efficiently without raising false alarms,

OBJECTIVE

The objectives of using controlled patrolling robots as a component of an apartment building intrusion detection system are as follows:

Boost Security: The primary objective is to raise apartment security by employing robots to patrol buildings that are equipped with state-of-the-art sensors. These robots' effective intrusion detection and prevention will reduce the chance of theft, burglaries, and other security breaches.

Entire Coverage: Make sure that every employee in the apartment building is a construction robot with the ability to maneuver through intricate spaces, including hallways, rooms, and multiple store. Robots that can patrol the entire area will be deployed in order to minimize blind spots and provide complete coverage.

Precise Intrusion Detection: Create algorithms and include superior sensors to precisely identify trespassers. Reducing the number of false alarms while maintaining the system's ability to distinguish between routine operations and possible security concerns is the goal.

Integration with Existing Infrastructure: Establish a connection between the intrusion detection system and the CCTV cameras and access control that are already installed in the apartment. Developing an effective and well-coordinated security system that optimizes resource usage and boosts overall efficacy is the aim.

Scalability and Cost-Effectiveness: Provide a scalable and reasonably priced system that can be used in numerous housing complexes. The intention is to offer a workable solution that is economical without sacrificing effectiveness or efficiency.

CONTRIBUTION

By addressing the shortcomings in the current security systems installed in residential complexes, the suggested intrusion detection system with controlled patrolling robots significantly contributes. It offers a novel approach that makes use of advanced algorithms, robots, and sensors to Increase security.

The gaps left by more traditional security systems are filled by the system's extensive coverage, real-time monitoring, and quick response to security threats. The remotely controlled patrolling robots have built-in sensors that allow them to autonomously scan the premises, identify intruders, and notify security staff right away. This study aims to demonstrate that the recommended approach is feasible,

effective, and capable of significantly boosting apartment building security.

II. PROPOSED SYSTEM

SCOPE OF THE PROJECT: "The "Intrusion Detection System Using Regulated Patrolling Robots for Apartments" is responsible for the creation and deployment of a comprehensive security system designed especially for residential complexes. The concept seeks to meet the increasing demand for improved apartment complex surveillance and quick reactions to any security breaches.

The primary goal is to monitor the area surrounding the homes with remotely operated patrolling robots that are outfitted with cameras and sensors. Following predetermined routes, these robots will patrol the area, snapping pictures and looking for any indications of illegal access or infiltration.

The hardware, which consists of the patrolling robots, sensors, and cameras, as well as the design and integration of the necessary software systems, are all included in the project's scope. Using computer vision techniques, the system will scan and assess photos in order to detect any unusual or suspicious activity.

An intelligent system that precisely detects and categorizes intrusion incidents based on the processed photos will also be developed as part of this project. To allow for a prompt and efficient response, the system will broadcast live video, send out instant alerts to security staff, and send out rapid emails.

The project endeavors to establish a dependable and efficient intrusion detection system through the deployment of controlled patrolling robots, thereby enhancing security measures and reducing the likelihood of unauthorized access in residential units.

III. LITERATURE REVIEW

EXISTING APPROACHES TO INTRUSION DETECTION SYSTEMS

To address security concerns in several sectors, intrusion detection systems (IDS) have been the subject of substantial research and development. In residential contexts, static surveillance systems, such closed-circuit television (CCTV) cameras and motion sensors, are commonly used as components of traditional intrusion detection systems. These systems typically have coverage gaps and are sluggish to react to attacks, even if they can offer a certain level of protection. Smart home security systems and wireless sensor networks (WSNs) are examples of more sophisticated methods that have surfaced. WSNs use distributed sensor networks to keep an eye on their surroundings and identify security breaches. Smart home security systems use a range of sensors, cameras, and communication tools to enable remote monitoring and control. Real-time, scalability, and response coverage may still be limited for these systems.

ROBOTS FOR SECURITY PURPOSES IN RESIDENTIAL SETTINGS

In recent years, the use of robots for security has increased. Robots can effectively cover large regions because of their mobility and versatility. Robotics can be used to improve security in residential settings by monitoring the property autonomously, spotting intrusions, and instantly raising alarms.

The employment of robots as home security has been the subject of numerous research. For instance, mobile robots outfitted with cameras and additional sensors have been utilized to patrol and observe residential areas. These robots are capable of autonomous movement as well as data collection from several sensors and transmission to a central control system. Nevertheless, the majority of these studies concentrate on general security applications and leave out some of the particular difficulties faced by apartment buildings.

Wireless sensor networks (WSNs) and smart home security systems are two instances of more advanced techniques that have emerged. WSNs monitor their environment and detect intrusions via a distributed sensor network. A range of sensors, cameras, and communication technologies are included in smart home security systems to enable remote monitoring and control. The real-time, scalability, and response coverage of these systems may still be limited.

PRIOR WORK ON REGULATED PATROLLINGROBOTS FOR INTRUSION DETECTION

While the use of robots for security has been studied, there hasn't been much research done in the past, particularly when it comes to using controlled patrolling robots to find breaches in residential buildings. Using controlled patrolling robots has several advantages, including frequent monitoring of a complex, which provides complete coverage and minimizes blind areas.

Numerous research publications state that robots have been deployed for security patrols in warehouses and other industrial settings. These studies often use To enable effective patrolling, navigation algorithms, obstacle avoidance, and path planning are used. Nevertheless, more investigation is required into the use of remotely operated patrolling robots made specifically for apartment complexes.
The suggested robot-controlled roving intrusion detection system for apartments fills the void left by current methods and the unique security requirements of apartment buildings. In an effort to offer broad coverage, real-time monitoring, and navigation, this system integrates sensors, communication systems, and navigational capabilities as well as a prompt reaction to any security risks. The literature study lays the groundwork for the suggested inquiry and emphasizes the necessity of a customized strategy for intrusion detection in apartment buildings.

IV. REQUIREMENT SPECIFICATIONS

FUNCTIONAL REQUIREMENTS

The Intrusion Detection System (IDS) of an apartment complex that employs controlled patrolling robots must meet the functional requirements listed below.

ROBOT PATROLLING:

The system should allow regulated robots to patrol in some areas of the apartment complex autonomously or semi-autonomously. The robots are expected to keep an eye on their surroundings, follow designated paths, and recognize any potential security threats.

SENSOR INTEGRATION:

Cameras, motion detectors, thermal imaging equipment, microphones, and other sensors should be installed on the controlled patrolling robots. To identify and evaluate any intrusions, the system ought to incorporate and make use of the information gathered from these sensors.

INTRUSION DETECTION:

The apartment building's IDS should analyze sensor data using algorithms and procedures to find aberrant activities or intrusions. It must be able to identify unauthorized access attempts, detect anomalous activity, and, in the event of a security breach, send out a warning.

REAL-TIME MONITORING:

The robot's cameras should provide live video feeds for security staff to view, and the intrusion detection system (IDS) should promptly notify them when an intrusion is detected. The robot's location and sensor data should be easy to observe using the monitoring interface.

Generation of Alert and Notification:

If the system detects an intrusion, it should promptly and accurately generate alerts. It should send out notifications via SMS, email, or mobile apps to renters, property managers, and security staff. Important details regarding the incursion, like the nature and extent of the threat, should be included in notifications.

CENTRAL CONTROL SYSTEM INTEGRATION: A central control system that functions as a command center should be interfaced with by the IDS in order to supervise the controlled patrolling robots and monitor security operations. The coordination, information sharing, and communication between the robots and the central control system should be made simple by the connection.

RECORDING AND LOGGING INCIDENTS

For every security incident that the IDS detects, the date, time, place, and kind of intrusion should be recorded. Future security improvements, forensic analysis, and system audits could benefit from this data.

The design of an IDS that employs controlled patrolling robots for residential areas is based on these functional aims. Depending on the scale, budget, and particular requirements of the apartment complex, the requirements could change.

HARDWARE REQUIREMENTS

RASPBERRY PI 3 MODEL B

Figure 1. Raspberry Pi 3b

The quad-core 1.2 GHz ARM Cortex-A53 CPU of the Raspberry Pi 3 Model B offers more performance than its predecessors. Thanks to its 1GB of LPDDR2 RAM, it can multitask and run apps more swiftly. The board has built-in Bluetooth 4.2 and Wi-Fi 802.11n, making wireless networking easier and eliminating the need for external adapters. networks and devices. It features four USB 2.0 ports in addition to a CSI camera connector for adding a Raspberry Pi camera module and other devices like keyboards, mice, and external hard drives. With its 40- pin General Purpose Input/Output (GPIO) header, you can combine the board with a wide range of electronic parts, sensors, and actuators to develop creative applications. A Raspberry Pi 3 Model B can be powered with a micro-USB power supply rated at 5 volts.

USB CAMERA FIGURE

Figure 2. USB Camera

Using a Raspberry Pi and an appropriate camera module is the simplest way to add visual input to a project. The figure has an external camera displayed. Because all you need to start using it is another compatible camera module, the regular Raspberry Pi camera module is a popular option. There are, however, a lot of alternative choices. A breakout board with an infrared LED and a night vision camera is one such substitute.

ULTRASONIC SENSOR

Figure 3. Ultrasonic Sensor

A device known as an ultrasonic sensor is one that, among other things, employs sound waves at frequencies higher than those that are audible to humans for object detection, navigation, and distance measurement. The transducer that powers the ultrasonic sensor generates ultrasonic waves, usually between 40.

SOUND SENSOR FIGURE

Figure 4. Sound Sensor

An electrical device that detects and measures sound waves in its immediate environment is called a sound sensor, sometimes referred to as a sound detector or sound module. It transforms acoustic energy into electrical impulses that other electronic devices or systems can process and examine. The primary component of a sound sensor is a microphone. It is made out of a diaphragm that, in reaction to sound waves, transforms electrical impulses into vibrations. The sensitivity of a microphone controls how well it captures sound waves and converts them into electrical impulses.

The range often includes the 20 kHz audible frequency spectrum, which is the range of frequencies that are perceptible to humans.

FIRE SENSOR

Figure 5. Fire Sensor

A fire sensor, also known as a smoke sensor or fire detector, is a crucial component of fire detection and alarm systems. Flame detectors are designed to detect the presence

of flames by sensing the characteristic ultraviolet (UV) or infrared (IR) light that flames emit.

Flamming detectors employ specialized sensors tuned to identify particular wavelengths of UV or infrared light emitted by flames. When the sensor detects the characteristic radiation, an alert is set off.

MOTOR DRIVER FIGURE

Figure 6. Motor Driver

A motor driver, also known as a motor controller, is an electrical device or circuit that controls the direction, speed, and functioning of an electric motor. It functions as an interface between the motor and a microcontroller or other control signals, transmitting the power and signals needed to run the motor safely and efficiently. Certain motor drivers can be used with a variety of motor types, including stepper, servo, DC, and BLDC motors. Motor drivers function as power amplifiers by accepting low- power control signals from a microcontroller or control system and raising the currents or voltages necessary to run the motor effectively.

SOFTWARE REQUIREMENTS

4.3.1. VISUAL STUDIO

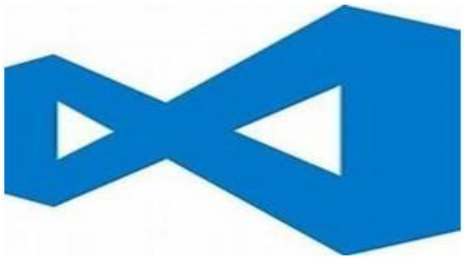

Figure 7. Visual Studio

An extensive integrated development environment (IDE) is Microsoft Visual Studio. Because it provides a wide range of tools and features for program creation, it is a popular choice among developers. Visual Studio's key feature is its support for many programming languages, like Python, C#, C++, and others. It offers extensive code editing and debugging features.

Features, enabling developers to build and debug programs more effectively. Furthermore, developers can easily improve and modify their code structure with Visual Studio's comprehensive toolkit for code refactoring.

4.3.2 OPERATING SYSTEM FIGURE

Figure 8. Raspberry Pi OS

Operating systems, such as Windows and Linux, are software packages that manage a computer's hardware and software resources to provide users with a dependable and user-friendly environment for running programs. It serves as a conduit for dialogue and interaction between the computer's hardware and its user. Raspberry Pi OS, formerly known as Raspbian, is a distribution designed specifically for the ARM architecture of the Raspberry Pi, and it is based on Debian Linux. It comes with a range of pre-installed apps, utilities, and tools made especially for Raspberry Pi devices, in addition to an intuitive UI.

4.2.5 LANGUAGE SPECIFICATION

Figure 9. Python Programming Language

Python is a high-level programming language with an interpreted execution architecture and an object- oriented philosophy. It is suggested for integration, scripting, and rapid application development because to its dynamic semantics. The key advantages of Python are its built-in high-level data structures, binding techniques, and dynamic typing. The grammar of the language is simple, readable, and easy to learn, all of which contribute to lower program maintenance costs.

.

Python promotes modularity and Reusing code is made easier by its support for packages and modules. Furthermore, both the extensive standard library and the Python interpreter are freely distributable in source and binary formats across major platforms, and they are both open source.

4.1.1OpenCV

Figure 10. open cv

A set of freely available techniques for computer vision and image processing known as Open CV is used in numerous domains, including augmented reality, robotics, object recognition, and video analysis. It provides a large selection of tools and algorithms for the analysis and editing of images and videos.

The library has many features, including input/output (I/O) for images and videos, object tracking, feature extraction and detection, camera calibration, machine learning algorithms for computer vision tasks, and image processing operations (filtering, transformations, and morphological operations). One of OpenCV's notable features is its ability to handle real-time computer vision applications by utilizing GPU capacity for high-performance processing.

V. METHODOLOGY

5.1 BLOCK DIAGRAM

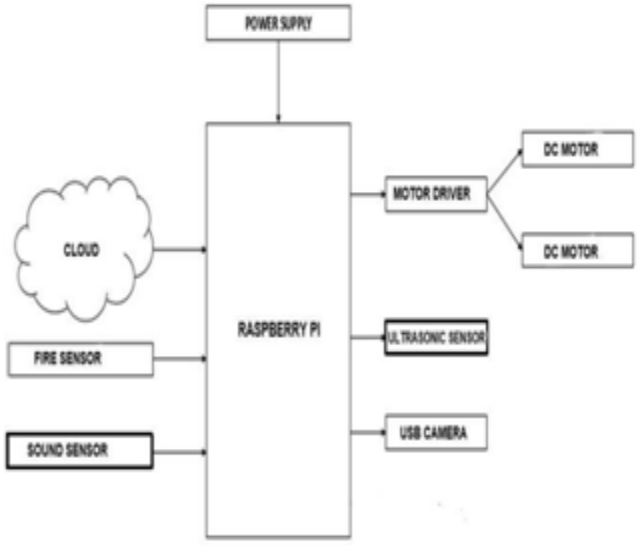

Figure 11. Modules Block Diagram

Our creation is a surveillance robot designed to keep an eye on the residential complex around-the-clock. The robot moves along a predefined course when it navigates. Our robot has an ultrasonic sensor and a USB camera mounted on its neck, which allow it to snap photos from various angles. The robot can recognize people or living things thanks to a sound sensor. The ultrasonic sensor enables obstacle identification and avoidance on flat surfaces. Using its sound sensors, the robot recognizes movement and sounds and responds accordingly. It detects obstacles using an ultrasonic sensor as well. Additionally, the robot uses its camera to snap pictures, which it then uploads to a database for later examination and analysis.

The photos that were taken will be forwarded for image processing. It makes use of the Haar Cascade Algorithm.Three pieces make up the entire system:Creating a database: Pictures of the apartment residents are gathered via the camera. tagging each person's photo with their user ID. Once the image has been converted to grayscale, locate the face. To make it accessible to you later, save it in the database.

The LBPH face recognizer, the load Haar classifier, and trained data from XML or YML files are utilized in the testing process. To take a picture, use the camera. Transform the picture to grayscale. Search within for the face. To predict a face, use the recognizer above.

If there is a discrepancy in the facial recognition data, the system will alert us, suggesting that someone else may have accessed our property. When the robot notices movement, sound, or an obstruction, it will process images. It will send an alert notification suggesting that an unknown individual is on our property if the faces don't match.

IMAGE PROCESSING

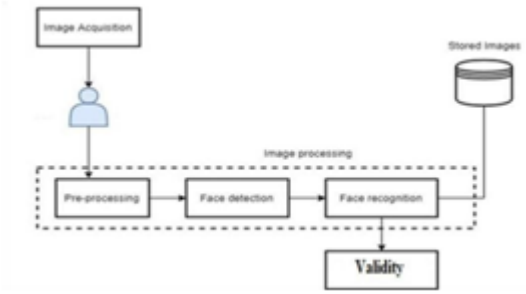

IMAGE PRE-PROCESSING

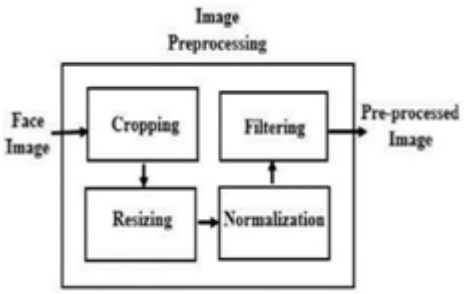

Figure 13. Image Preprocessing

"Image preprocessing" is the term used to describe a group of methods used on a picture prior to additional processing or analysis. Improving an image's quality, legibility, or ability to extract pertinent information from it is the aim of image preprocessing.

Among the Preprocessing Methods Are:

Image scaling is the process of changing an image's dimensions to a standard or compatible size.

Image cropping: excessive backdrop or chunk removal from an image to bring attention to the focus.

Reducing noise or other undesirable interference that may be present in an image due to a number of circumstances, such as sensor limits or environmental impacts, is the process of picture denoising.

Image enhancement: Methods that enhance the visual quality of an image and highlight key details include brightness adjustment, contrast alteration, and histogram equalization.
To facilitate further processing or comparison, picture normalization entails bringing an image's pixel values into a standard scale or range.

Image smoothing is the process of reducing sharp edges and high-frequency noise in an image by using filters or smoothing techniques like median or Gaussian filtering.

Enhancing the edge definition or sharpness of a picture to facilitate feature extraction or boost visual clarity is known as image sharpening.

The process of altering a color's hue, saturation, or balance to improve color accuracy or take lighting fluctuations into account is known as image color correction.

Image registration is the process of aligning several images to a single coordinate system for fusion, analysis, or comparison.

Use attributes like color, texture, or intensity to segment an image into relevant areas or objects for additional analysis or object detection.

These preprocessing techniques improve the quality, usability, and interpretability of images, which facilitates more effective processing or additional analysis.

5.1.1IDENTIFICATION OF PERSON

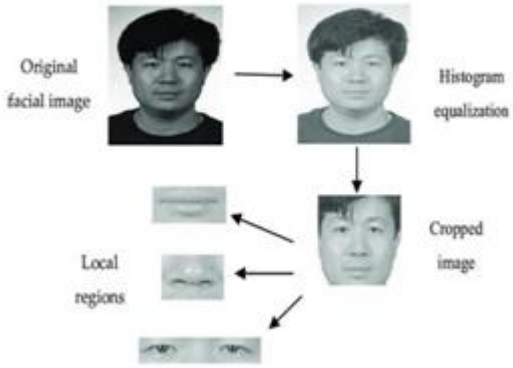

Figure 14. Face Detection

Face detection is the process of finding and identifying human faces inside an image or video frame. This fundamental problem in computer vision finds applications in biometrics, facial identification, augmented reality, emotion detection, and surveillance. Face identification aims to identify faces in photos or videos that are owned by individuals. The following steps are often involved in the process: An image or video's input frame: The system is fed an input image or video frame that includes one or more human faces. Before being processed: Preprocessing techniques, including noise reduction, scaling, and normalizing, can be applied to enhance the image quality.

Feature extraction: A range of visual characteristics, such as color, texture, or shape, are extracted from the image to identify potential face regions. Face region localization: Following facial recognition, the positions of the faces in the picture are typically depicted as bounding boxes or contours encircling the identified face regions.

Post-processing: To improve the results of face detection, eliminate false positives, and raise the accuracy of detections, more post-processing methods could be used.

5.1.1 FACE REDEEMING

5.2.3(1) CLASSIFIER FOR HAAR CASCADE

Figure 15. Haar-Feature Extraction

By utilizing the Haar Wavelet technique to analyze the pixels, the Haar Cascade classifier partitions the pixels of an image into square segments based on their respective functions. The concept of "integral images" is used in this method to identify the features that have been found. Haar Cascades employ the Ada-boost learning technique to give classifiers an effective output. Afterwards, faces in images are recognized using cascade approaches. These are some illustrations of Haar-Features.

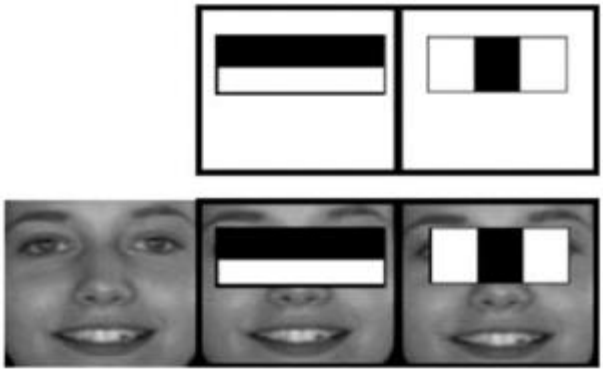

Figure 16 illustrates the Haar-like characteristic.

It is made up of two parts: lines and edges. The grayscale image's pixels nearest to the light source are shown as a white bar. To obtain this assessment, the Haar value is computed. The algorithm for determining pixel value is (Total Dark Pixels / Total Dark Pixels) - (Total Light Pixels/ Total Light Pixels). The Haar cascade Classifier is one way to detect things. The image will go through feature extraction to facilitate object identification and recognition. The equation that was previously mentioned can be used to determine the value of the Haar pixel.

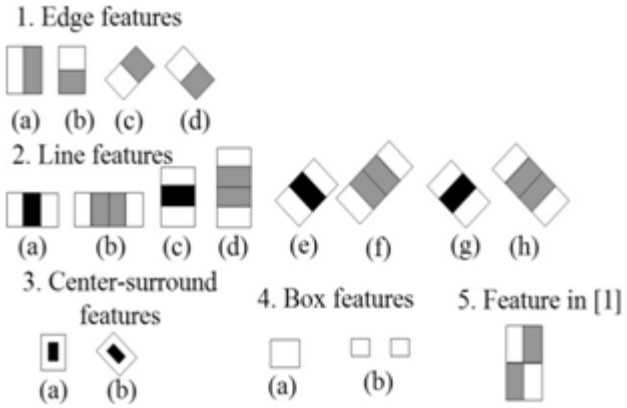

Figure 17. Different Haar-Features

While face recognition can be started with Haar cascades, face recognition is a separate process with its own set of algorithms and methods. Typically, face recognition entails the following actions: Face recognition: First, face areas from an image or video frame are detected and retrieved using a face detection approach such as the Haar cascade. Face alignment: In order to align and normalize the orientation and scale of the various components of a face, landmarks or prominent spots on the face are recognized after faces have been detected.

This stage uses continual feature extraction to ensure accurate recognition. To extract discriminative features from the aligned face areas, many approaches can be employed. Eigenfaces, Local Binary Patterns (LBP), and Convolutional Neural Networks (CNNs) are examples of deep learning approaches

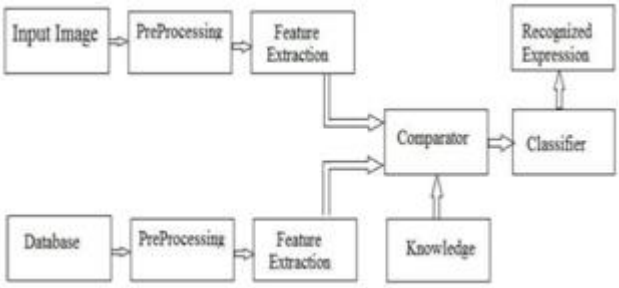

Figure 18. The Haar Cascade Algorithm Flow Diagram

The goal of these features is to record unique facial traits that facilitate person identification. Comparing and matching with features: The retrieved facial features are cross-referenced with a database of acknowledged identities during the recognition step. Numerous methods, including the Euclidean and Mahalanobis distances and similarity metrics like correlation or cosine similarity, can be used to compare the two. Choice about acknowledgment: The person's identity is established based on the measurements of distance or likeness. The face can be categorized as belonging to a

particular identity or as an unknown face by applying a threshold or classification algorithm.

VI. RESULTS

6.1 COMPLETED MODEL

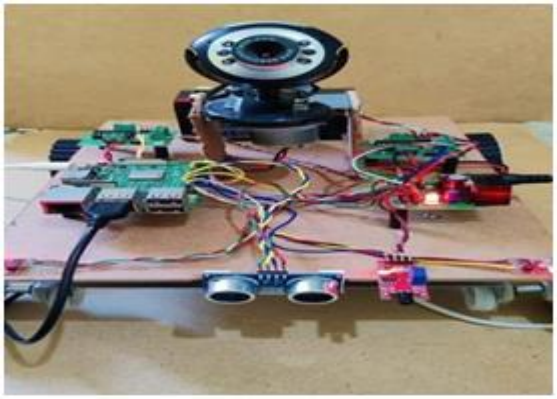

Figure 19. completed model picture

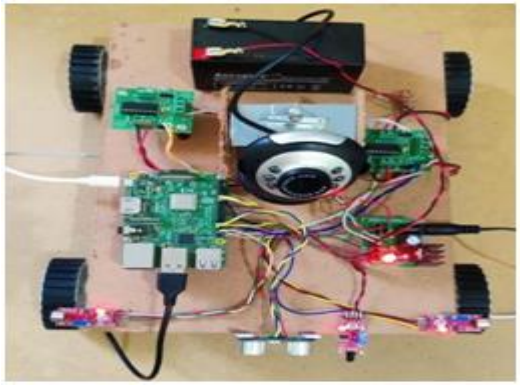

Figure 20. Completed model picture

The Python IDE will display the sound or obstacle detected in the robot's surroundings, as illustrated in figure 21 below.

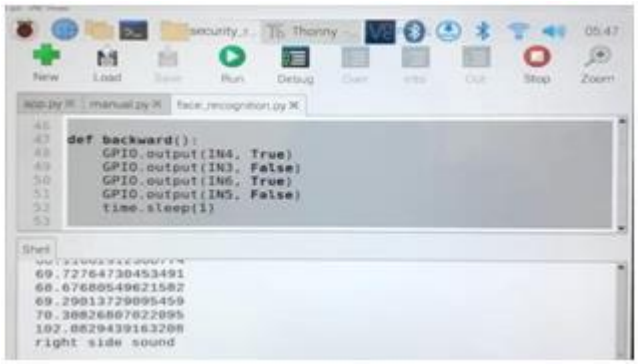

Figure 21. Status of sound detected

The robot will use its USB camera to record the scene and check to see if the person matches the predefined dataset after detecting any sound or impediment. If not, the Python IDE will display the UNKNOWN status, as shown in figure 22 below.

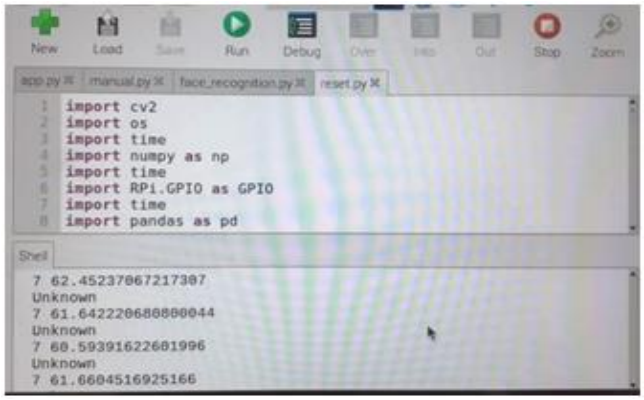

Figure 22. Status of face recognition

As seen in figures 23 and 24, when it determines that the individual is unknown, it notifies the authorities by sending a picture of that person along with an alert.

figure 23: Status of the named individual

Figure 24: The unidentified person's status and alert message

VII. CONCLUSION

An intriguing approach to bolstering security and safety procedures is to incorporate remotely operated patrolling robots into the intrusion detection system of an apartment complex. Modern monitoring and detection systems, along with robotic technology, offer an efficient and preventive means of thwarting these kinds of attacks. Robots that patrol apartments under supervision and are outfitted with sophisticated sensors and surveillance equipment can help provide dependable, 24-hour apartment security. These mobile robots can rapidly identify any unlawful access or abnormal activities by patrolling the region. Early detection of incursions enables prompt response and intervention, which lowers the risk of property damage or resident injury.

The goal of the project was to develop and deploy a security robot that can perform a variety of functions, such as real-time threat identification and alerting. Self-governing robots have the potential to be more trustworthy and effective security agents than people or most current security systems. To determine whether or not the apartment's occupants were meant to be there, sound sensors were consequently added to a particular user robot. If not, it will display the live video stream and notify the official.

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 inIntrusion 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 IntrusionDetection 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. Lien hart, 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/S266685X21000728
[10] https://towardsdatascience.com/face-detection-with-haar-cascade-727f68dafd08