JCBI
Journal of Computing & Biomedical Informatics Volume 05 Issue 01
ISSN: 2710 - 1606 2023
Research Article
https://doi.org/10.56979/501/2023

IOT Enabled Smart Ultrasonic Surveillance System Using IR Sensor

Muhammad Afzal[1], Muhammad Aoun[1*], Shafiq ur Rehman[2], Muhammad Aftab Kaleem[1], Muhammad Jamil[1], and Muhammad Taqi[1]

[1]Department of CS & IT, Ghazi University, Dera Ghazi Khan, 32200, Pakistan.
[2]Mir Chakar Khan Rind University of Technology, Deparnmnet of Computing and Information Technology, 32200, Pakistan.
[*]**Corresponding Author**: Muhammad Aoun. Email: muhammadaoun151@gmail.com

Received: January 28, 2023 **Accepted:** June 02, 2023 **Published:** June 05, 2023.

Abstract: The suggested system is an IoT-enabled auto surveillance and self-defence system made for interior security and self-defence against threats like robberies and target killings at residences, banks, and stores, among other places. The technique combines Face Detection, Infrared (IR), and Ultrasonic Sensors to find and follow possible threats in an interior setting. During the IR and Ultrasonic Sensors supply extra information like distance and position of prospective targets, the Face detection component enables the system to identify and monitor the adversary danger in that particular region. The system uses this information to automatically intercept, target, and fire a chemical dart at the detected threat. The procedure generally offers a precise and automatic reaction to possible security concerns in indoor settings. This study's primary purpose is to provide security and automatic defence to lives and property when interior employees find it challenging to monitor and intercept threats, especially in sensitive locations like banks, high-ranking officials' homes, shopping centres, and stores.

Keywords: Auto surevellance, Self defense , Facial detection, Potential threats, and Accurate response.

1. Introduction

People have traditionally placed a high value on the protection of their lives and their possessions, especially in confined settings like marketplaces, restaurants, and banks where the safety of customers and employees is essential. In recent years, it has become increasingly important to have automated systems that can rapidly and reliably identify potential security concerns [1]. Due to the nation's fast-shifting economic environment and inflation rate, street crimes have significantly grown. According to Pakistan's Yearly Crimes Reports, target killings at houses and marketplaces, robberies, and theft are the most frequent crimes, with a 3.4% rise since 2019. The recommended Automatic self-defence system is designed to provide an automatic response and defence to numerous potential security threats in indoor settings[2]. The system integrates face detection, IR, and ultrasonic sensors to find and monitor potential environmental dangers [3]. The system promptly targets and fires at any threats it detects to neutralise them [4]. The system's face identification component uses modern methods to identify and locate individuals in the interior environment region. It is trained to discriminate between known employees and potential dangers, and it can do this even in low light [5]. The IR sensors provide extra information on the location and range of potential targets by detecting body heat signatures [6]. The ultrasonic sensors are used to identify and follow the object's movement in the authorised area to provide more information about potential threats [7].

The device automatically targets and fires an authorised chemical through a Dart gun towards the detected item (person). It uses data from various sensors to determine its location and movement to protect against security hazards [8].

Ethical and legal concerns may need to be made while using such a system. Lethal force against potential threats should only be authorised after serious consideration [9]. Before usage, the system's accuracy and dependability would also be meticulously examined and validated [10] to prevent any unexpected

consequences. Since having a human-in-the-loop system to verify the threat before initiating the automated reaction is crucial, it is also essential to decrease the possibility of false positives, which prevents innocent individuals from being classified as potential threats [11].

It may be entirely ethically and legally questionable to use such a system. Lethal force in the face of potential threats must be authorised and carefully examined as a last resort [9]. Before usage, the system's reliability and correctness would be thoroughly examined and validated [10] to avoid any unexpected results. Another risk of false positives should be reduced, where innocent persons should not be identified as potential threats because it is imperative to have a human-in-the-loop system to verify the danger before initiating the automated reaction [11].

Table 1. Weapons names, along with their frequency, weight, and size

Name	Frequency	Weight (unloaded)
Glock 17	3	25.06 oz (709 g)
Smith & Wesson M&P 9	3	24.7 oz (700 g)
SIG Sauer P226	2	34 oz (964 g)
Beretta M9	2	33.3 oz (943 g)
Colt Python	2	46 oz (1304 g)
Ruger GP100	2	36 oz (1021 g)
CZ Shadow 2	2	46.2 oz (1308 g)
Walther PPQ	1	24.5 oz (695 g)
1911	1	39 oz (1105.6 g)
Beretta 92FS	1	33.3 oz (943 g)
Smith & Wesson M&P 2.0 Compact	2	27 oz (765 g)
Glock 19	3	23.65 oz (669.6 g)
SIG Sauer P320 Compact	2	26 oz (737 g)
Smith & Wesson M&P Shield	3	19 oz (538.6 g)
Ruger LCP II	2	10.6 oz (300 g)
Walther PPK	1	20.1 oz (570 g)
FN Five-seveN	1	21.9 oz (621.4 g)
Desert Eagle	1	72 oz (2041.2 g)
CZ 75	1	35.2 oz (997.9 g)

Installing a metal detector in the suggested System necessitates its integration with the other system parts. The process will have the following steps.

1. **Choosing good metal detector:** Pick a metal detector that is system-compatible and capable of picking up weapons or metal items. The metal detector should produce a signal or data that the Arduino microcontroller can process.
2. **Connecting the metal detector to the Arduino:** The Most metal detectors offer a signal that may be utilised to output information on the identified metal items. These output signals must be connected to the corresponding Arduino input pins. To choose the proper wiring, input sensing, and output settings, it is crucial to read the metal detector's manual or datasheet thoroughly.
3. **Configuring the Arduino:** To enable the microcontroller to receive and handle signals from the metal detector, create an Arduino setup programme. When a weapon or other metal object is detected, this code should interpret the signals from the metal detector and activate the trigger in the Dart gun aiming mechanism. The needs of the metal detector and Dart gun systems will dictate the precise implementation characteristics.
4. **Testing and calibrating the detection system:** After the metal detector is placed into the Arduino board, the system is tested to ensure it accurately distinguishes firearms or other metal items. The sensitivity and threshold settings of the metal detector need to be calibrated to perform at their optimum.
5. **System components Integration:** Make that the output of the metal detector is correctly integrated

with the face detector, IR, and ultrasonic sensors in the system. The Dart gun targeting mechanism may be activated by precisely identifying any possible danger using the information received.

6. **Wireless connectivity and cloud integration:** To send information on intruder location and detection to the cloud, the NodeMCU module offers wireless connectivity. If a threat is identified, this might be utilised to trigger the Dart gun targeting system. Establish a Wi-Fi connection to allow the NodeMCU module to transfer the required data to the cloud for extra analysis.
7. **Ensuring the legal and ethical considerations:** When creating a system with weapons or the ability to hurt people, it is crucial to consider legal and ethical issues. Consult with legal professionals to ensure that the technology is utilised morally, in compliance with all applicable laws, and honestly.

1.1 IR Sensors

To provide details on the location and spacing of potential targets, the system integrates Infrared (IR) sensors with face recognition [16]. These sensors may recognise the body heat patterns that reveal where individuals are in the surroundings and how they are moving. The data acquired by the face detection components may be combined with the data gathered by the IR sensors to provide a more comprehensive picture of potential threats [17].

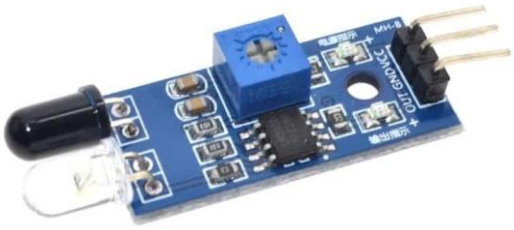

Figure 1. IR Sensor

1.2 Ultrasonic Sensors

The third component of the system, ultrasonic sensors, is utilised to recognise and track the movements of objects in their immediate environment. These sensors use the echoes of the high-frequency sound waves they produce to identify the locations and activities of nearby objects. Ultrasonic sensors may detect movement behind things or places without a clear line of sight, adding more details about potential threats [18].

Figure 2. Ultrasonic Sensors

1.3 Overall System Design:

The suggested system uses face recognition, IR, and ultrasonic sensors to provide an autonomous defensive response to potential security threats in interior environments. The system examines the data obtained by the multiple sensors to find hazards and determine where they are and how they are moving. The device then automatically aims and fires a chemical through a Dart gun to neutralise the detected threat [19].

1.4 Need and Significance of the study

Section 96 of the Pakistan Penal Code states that everyone has the right to defend their body and property against any offence that causes reasonable apprehension of death or grievous bodily harm. As a result, the primary purpose of this study is to ensure security against crimes that threaten life, such as robbery, theft, and target killing in indoor systems.

1.5 Component Required

1.5.1 Radiation Detector

Any intrusion would produce heat and be in motion. To ascertain the existence of an intruder, an electronic IR sensor called an "Infrared Sensor" has been added to the system. Its infrared wavelength range is 850nm [21].

Figure 3. Radiation Detector

1.5.2 Node MCU

NodeMCU is used in wireless communication setup to transmit and receive information about the presence of intruders in border zones and is connected to the microcontroller. The Arduino UNO microcontroller provides wireless connection and is an open-source, budget-friendly IoT platform. Formally speaking, "NodeMCU" denotes the firmware as opposed to the associated development kits [22].

Figure 4. Node MCU

1.5.3 Ultrasonic Sensor

The ultrasonic sensor works with reflected signals, much like radar and sonar equipment. It calculates the item's distance by utilising the time difference between sending a message and getting an echo. Consequently, by using the application, the inside system will be able to detect the presence of an intruder [23].

Figure 5. Ultrasonic Sensor

1.5.4 LCD

An LCD alerts the administration and extra security soldiers to the existence of any dangerous objects, allowing them to take the necessary action. It will also demonstrate that it is feasible to fire chemical darts

from a dart gun at an intruder while simultaneously detecting their face [24].

1.5.5 Microcontroller development board Arduino-Uno R3

This microcontroller handles the multiple sensor inputs. It is then interfaced with Python to distinguish human faces, updating the control station through the cloud of intrusions. An ATMEGA 328 microprocessor is built inside this development board [25].

Figure 6. Arduino-Uno R3

1.5.6 Adafruit IO

A cloud application takes advantage of Adafruit IO. It is mainly concerned with sending data collected from sensors to the cloud. Additionally, it incorporates feed sharing and has honed privacy controls, which permit and limit data access [26].

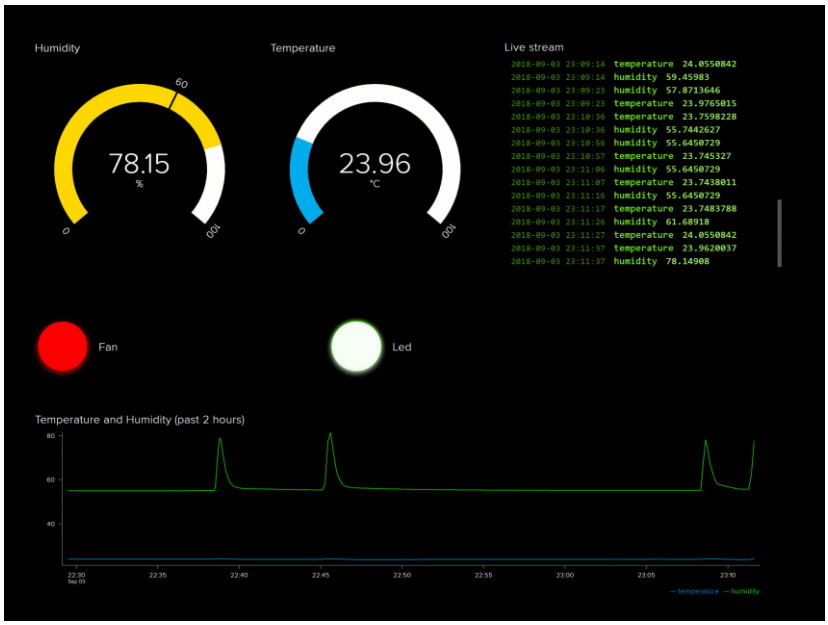

Figure 7. Adafruit IO

2. Face Detection

2.1 Algorithm for Haar Cascade Classifier

Haar Wavelet technique, based on which this classifier splits the resulting image into squares depending on the function for pixels analysis. It has four crucial components that make it perfect for face recognition while cameras are streaming live: selection of Haar features, creation of a primary image from the live streaming, application of Adaboost training, and cascade classifiers [27]. The Haar feature selection broadly distinguishes between the features unique to a human face and other elements of images. By determining positives from negatives, one AdaBoost training strategy produces superior outcomes for

picking only the essential characteristics. Finally, cascade classifiers shorten computation time and speed up identification.

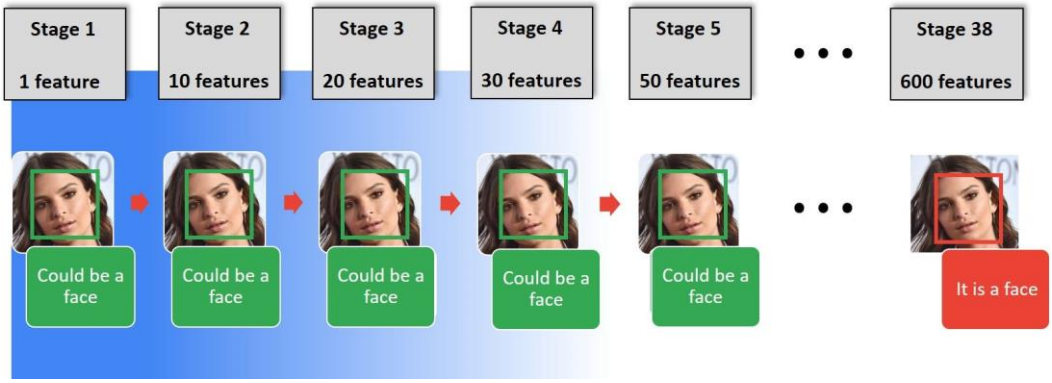

Figure 8. Haar Cascade Classifier

2.2 Pseudocode

The camera uses PYTHON and real-time Adafruit IO data to detect human activity in the targeted area. Adafruit IO files are supplied in addition to MIME (Multipurpose Internet Mail Extensions) components OpenCV, OS, SMTPlib, SSL, and email packages. After that, SMTPlib sends the email from the source to the destination over a server. We store the variables ADAFRUIT IO KEY and USERNAME after a string variable's declaration and before invoking them in a function to enable cloud in the code [28]. Next, the open cv function is used to capture the video while the Haar cascade classifier, a core method for face detection, is loaded. Then, we create a process for sending emails. Before including the image, we spell out all the requirements for the email that will be posted. An exception of error is sent to indicate that the email cannot be delivered if there is no internet connectivity. When the camera detects a face after the image has been converted to grayscale, the look is then highlighted by a circle. The statement "face detected" on the Python output shell is then emailed with the face image. The first formed variable is sent to the cloud function, which then sends the data there.

2.3 Hardware Pseudocode

Pins are then assigned to various sensors and other components after the header files for the LCD and I2C have been included. A trigPin and an LED serve as the function's outputs, and an IR sensor and an ultrasonic sensor's echoing serve as inputs. When Arduino is powered up, the LCDs are "BORDER AREA." Then, a function is developed for an ultrasonic sensor's functioning that includes a formula the sensor may use to calculate the object's distance from it [29]. These calculations will be displayed on the serial monitor in the Arduino IDE. If the item is within 20 units of the sensor, the LED will illuminate and print "GUN FIRING" on the LCD; otherwise, it will remain off. At the same time, a function for the IR sensor is specified; if it is low, the LCD will display "GUN FIRING", and the LED will turn on; if not, it will remain off. A face detection function has been built, and when it reads a byte from an I2C serial connection, the LCD will display "INTRUDER DETECTED," and the LED will either turn on or remain off [30].

2.3.1 Abbreviations and Acronyms

LCD: Liquid Crystal Display.

LED: Light Emitting Diode.

I2C: IC inter. This bus supports many masters, and any linked chips have the ability to act as a mas- ter by starting a transfer.

MIME: Multipurpose Internet Mail Extensions.

OS: Operating System

SMTPlib: Simple Mail Transfer Protocol manages email transmission and distribution across mail servers. The SMTPlib module is provided by Python, and it specifies an SMTP client session object [31].

SSL: Layers of secure sockets. It is a networking protocol intended for protecting online interactions between web clients and web servers.

2.3.2 OpenCV

Open Source Library for Computer Vision. Real-time computer vision functions are cov- ered by a programming function library [32].

3. Configuration

Pin Configuration

Table 2. Arduino Pin Configuration

COMPONENT	PIN NUMBER
ULTRASONIC SEN-SOR	TRIGGER PIN - 6 ECHO PIN - 5
IR SENSOR	4
LED	7
LCD	RESET - 13 ENABLE – 12 D4 - 11 D5 - 10 D6 - 9
Node MCU	GPIO1(SDA)- A4

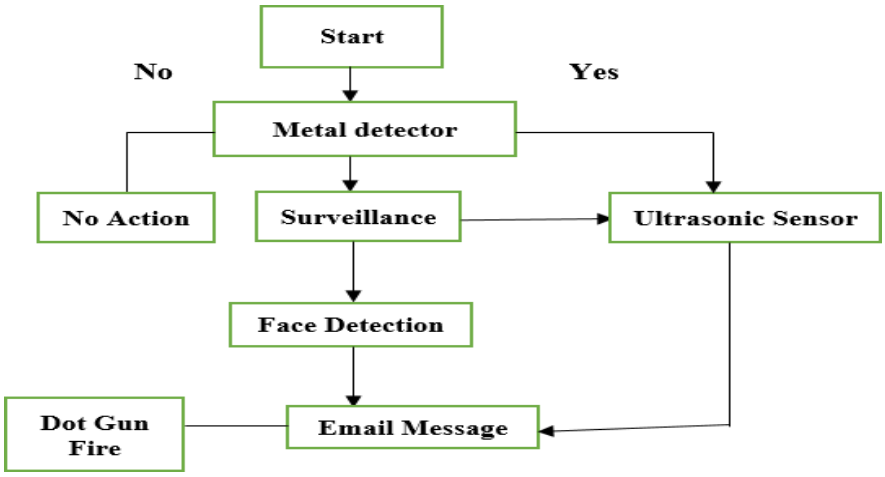

Figure 9. Working Flowchart

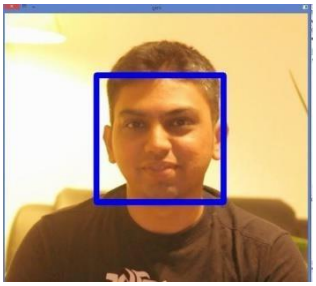

Figure 10a. Detected Face 1

Figure 10b. Detected face 2

4. OBSERVATION

4.1 Cloud

Adafruit IO, a real-time application cloud, monitors the camera. Thanks to it, the user may define various devices to be linked. The POONCH cloud server, shown in Figure 11, displays data such as the date and time and the notification that an intrusion has been found. According to the requirements of the coverage area, several servers may be defined [33].

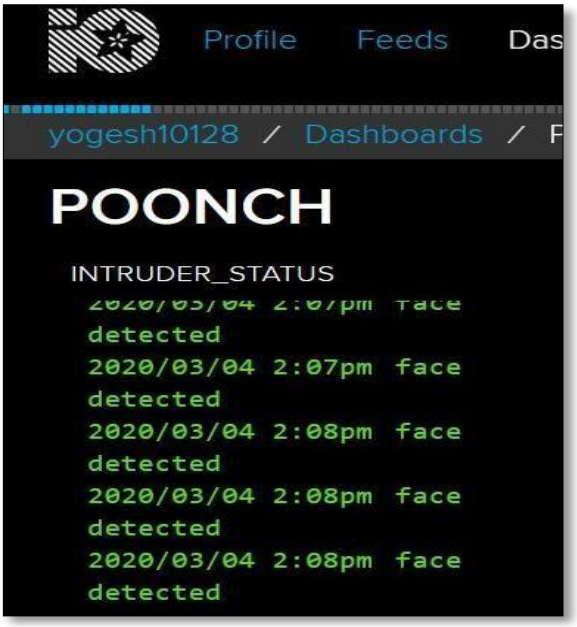

Figure 11. Adafruit cloud output

4.2 LCD

In Figure 12, the LCD has been turned on and initialised. While the LCD was being initialised, the BORDER_AREA message was shown. If an intruder is discovered or any sensor responds favourably, Figure 6 displays an INTRUDER_DETECTED message [34].

Figure 12. LCD intruder detected via Face DetectionAlgorithm

Figure 13. LCD on Intruder D Serial Monitor

In Figure 13, the LCD has been turned on and initialised. While the LCD was being initialised, the BORDER_AREA message was shown. If an intruder is discovered or any sensor responds favourably, Figure 6 displays an INTRUDER_DETECTED message [34]

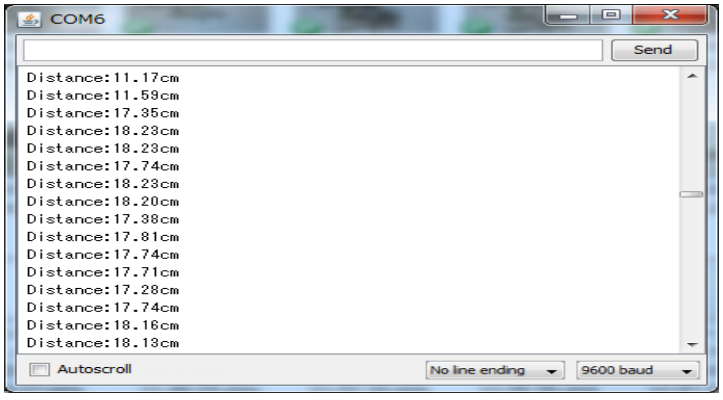

Figure 14. Serial Monitor

4.3 E-mail Output

Figure 15, illustrates an email warning the cloud sent to identify the intruder. The camera captures a photo of the intruder, examines it on the cloud, and then emails a copy of the result.

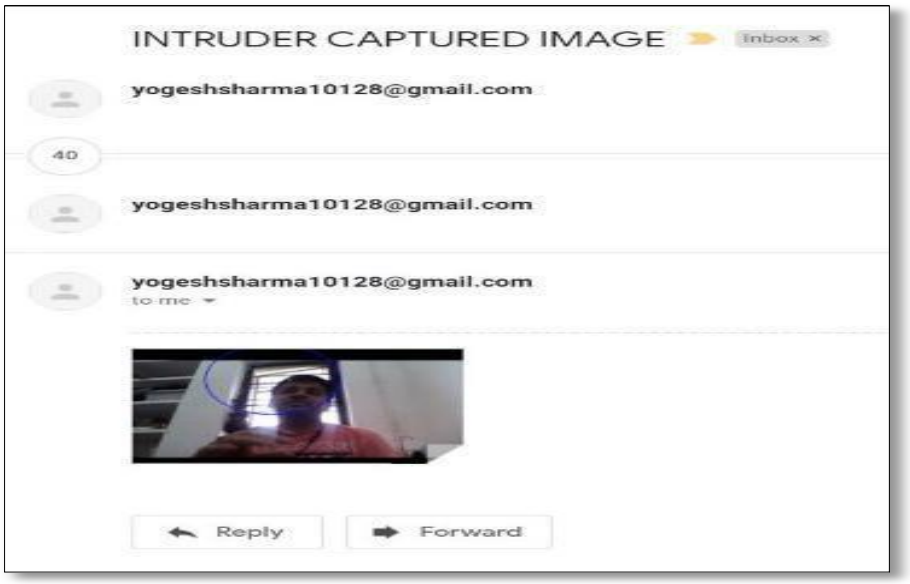

Figure 15. E-mail received

5. Result & Discussion

Using an automatic handgun aiming system with facial detection yields accurate information. The image of the intruder, as recorded by the camera, is sent to email, making it easy to identify the person. The project gains access to the IR and Ultrasonic Sensors, two more sensors. These sensors offer additional security by acting as a backup in case a camera fails. If the thief can escape the camera, these sensors help nearby for his identification. Haar Cascade's facial recognition method enables the simultaneous detection of several faces. As long as it saw a look, the camera gun would keep firing while simultaneously sending an email with the intruder's picture. The Adafruit IO cloud determines which gun has been triggered and when. We could utilize this cloud to locate any invasion detected by hardware. It is possible to see any weapon remotely and from a distance. When the intruder triggers the IR sensor, their world is reduced to a single LED blink, signifying the firing of a single shot. Any interior object, including homes, banks, and stores, can trigger an IR sensor; as a result, the microcontroller instructs a single image to be fired. When the ultrasonic sensor detects an intruder, the LED flashes for extended periods, signaling several shots have been fired.

6. Conclusion

The idea uses three different technologies: infrared technology, an ultrasonic sensor, and face detection. An email message with an image of the intruder is sent to the user's mail address, in this instance, the person in charge of the control station, upon face detection. When a human face is detected, the gun will continue to fire. When the IR sensor registers a reading, continuous firing starts, and an LCD panel shows the gunshot. The LCD and one shot are fired when the ultrasonic sensor detects movement. A live report on the Adafruit cloud is obtained using the face the camera recognizes. It would be difficult to spy inside due to the defense mechanism's traits, which all worked to keep remote locations under continual observation. An intruder will be simpler and easier to locate and target. This will result in an overall enhancement in security around interior spaces, including homes, banks, and businesses. The logistics of regulating our increasing indoor spaces, the allocation of resources, and other costs will all be much enhanced. With

the help of efficiency improvement, the indoor can deploy resources in other vital areas, saving money and defense personnel. As a result, the created approach effectively achieves the primary objectives of our research.

7. Future Scope

The project will be improved using a state-of-the-art, high-resolution camera that supports night or thermal vision. Examining targets in the air may also be done using this method. The probe will focus more on chasing fast-moving objects, such as aero planes. More research may be conducted to develop a system monitoring several targets. The survey may be extended further so that the system can track many targets with different goal criteria. The project may be advanced by integrating with a complex microprocessor rather than using a simple microcontroller like arduino.

Funding: No funding was received.

Data Availability Statement: The authors declare that all data supporting the findings of this study are available within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. N. Djelal, N. Mechat, and S. Nadia, "Target tracking by visual servoing," in Systems, Signals and Devices (SSD), 2011 8th International Multi-Conference on. IEEE, 2011, pp. 1–6.
2. N. Djelal, N. Saadia, and A. Ramdane-Cherif, "Target tracking based on surf and image based visual servoing," in Communications, Computing and Control Applications (CCCA), 2012 2nd International Conference on. IEEE, 2012, pp. 1–5.
3. E. Iflachah, D. Purnomo, and I. A. Sulistijono, "Coil gun turret controlusing a camera," EEPIS Final Project, 2011.
4. A. M. Idris, K. Hudha, Z. A. Kadir, and N. H. Amer, "Development oftarget tracking control of gun-turret system," in Control Conference (ASCC), 2015 10th Asian. IEEE, 2015, pp. 1–5.
5. J. D. S. Munadi and M. F. Luthfa, "Fuzzy logic control application for the prototype of gun-turret system (arsu 57-mm) using matlab," 2014.
6. T. M. Nasyir, B. Pramujati, H. Nurhadi, and E. Pitowarno, "Control simulation of an automatic turret gun based on force control method," in Intelligent Autonomous Agents, Networks and Systems (INAGENTSYS), 2014 IEEE International Conference on. IEEE, 2014,pp. 13–18.
7. G. Ferreira, "Stereo vision-based target tracking for a gun turret utilizing low performance components," Ph.D. dissertation, Universityof Johannesburg, 2006.
8. H. D. B. Brauer, "Real-time target tracking for a gun-turret using low cost visual servoing," Master's thesis,University of Johannesburg, 2006. [Online].
9. Ö. Gümü¸say, "Intelligent stabilization control of turret subsystems under disturbances from unstructured terrain," Ph.D. dissertation, Middle East Technical University, 2006.
10. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.
11. A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classificationwith deep convolutional neural networks," in Advances in neuralinformation processing systems, 2012, pp. 1097–1105.
12. K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," arXiv preprint arXiv:1409.1556, 2014.
13. C. Farabet, C. Couprie, L. Najman, and Y. LeCun,"Learning hierarchical features for scene labeling," IEEE transactions on patternanalysis and machine intelligence, vol. 35, no. 8, pp. 1915–1929, 2013.
14. A. Graves, M. Liwicki, S. Fernández, R. Bertolami, H. Bunke, and J. Schmidhuber, "A novel connectionist system for unconstrained handwriting recognition,"IEEE transactions on pattern analysis and machine intelligence, vol. 31, no. 5, pp. 855–868, 2009.
15. A.-r. Mohamed, G. E. Dahl, and G. Hinton, "Acoustic modeling usingdeep belief networks," IEEE Transactions on Audio, Speech, and Language Processing, vol. 20, no. 1, pp. 14–22, 2012.
16. R. Girshick, "Fast r-cnn," in Proceedings of the IEEE International Conference on Computer Vision, 2015, pp. 1440–1448.
17. Benet, Gines, et al. "Using infrared sensors for distance measurement in mobile robots." Robotics and autonomous systems 40.4 (2002): 255-266.
18. Magori, Valentin. "Ultrasonic sensors in air." 1994 Proceedings of IEEE ultrasonics symposium. Vol. 1. IEEE, 1994.
19. Kundur, Prabhashankar, et al. "Application of power system stabilizers for enhancement of overall system stability." IEEE Transactions on power systems 4.2 (1989): 614-626.
20. Jardine, Cynthia G., and Angela James. "Youth researching youth: Benefits, limitations and ethical considerations within a participatory research process." International Journal of Circumpolar Health 71.1 (2012): 18415.
21. Milbrath, Brian D., et al. "Radiation detector materials: An overview." Journal of Materials Research 23.10 (2008): 2561-2581.
22. Parihar, Yogendra Singh. "Internet of things and nodemcu." journal of emerging technologies and innovative research 6.6 (2019): 1085.
23. Carullo, Alessio, and Marco Parvis. "An ultrasonic sensor for distance measurement in automotive applications." IEEE Sensors journal 1.2 (2001): 143.
24. Silveira, A. V. M., et al. "Recovery of indium from LCD screens of discarded cell phones." Waste management 45 (2015): 334-342.
25. Bereziuk, V., et al. "Means for measuring relative humidity of municipal solid wastes based on the microcontroller Arduino UNO R3." Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics
26. Shrivastava, Anurag, et al. "IoT Based RFID Attendance Monitoring System of Students using Arduino ESP8266 & Adafruit. io on Defined Area." Cybernetics and Systems (2023): 1-12.
27. Cuimei, Li, et al. "Human face detection algorithm via Haar cascade classifier combined with three additional classifiers." 2017 13th IEEE International Conference on Electronic Measurement & Instruments (ICEMI). IEEE, 2017.
28. Oda, Yusuke, et al. "Learning to generate pseudo-code from source code using statistical machine translation." 2015 30th IEEE/ACM International Conference on Automated Software Engineering (ASE). IEEE, 2015.
29. Bonelli, Nicola, et al. "On multi–gigabit packet capturing with multi–core commodity hardware." Passive and Active Measurement: 13th International Conference, PAM 2012, Vienna, Austria, March 12-14th, 2012. Proceedings 13. Springer Berlin Heidelberg, 2012.
30. Charan, Ram, Dennis Carey, and Michael Useem. Boards that lead: When to take charge, when to partner, and when to stay out of the way. Harvard Business Review Press, 2013.

31. Goerzen, John, and John Goerzen. "Simple message transport protocol." Foundations of Python Network Programming (2004): 197-210.
32. Bradski, Gary, and Adrian Kaehler. "OpenCV." Dr. Dobb's journal of software tools 3.2 (2000).
33. Dillon, Tharam, Chen Wu, and Elizabeth Chang. "Cloud computing: issues and challenges." 2010 24th IEEE international conference on advanced information networking and applications. Ieee, 2010.
34. Silveira, A. V. M., et al. "Recovery of indium from LCD screens of discarded cell phones." Waste management 45 (2015): 334-342.
35. Iwasaki, Y., et al. "Occasional infection of hepatitis C virus occurring in haemodialysis units identified by serial monitoring of the virus infection." Journal of Hospital Infection 45.1 (2000): 54-61.