Aqua Farm Theft Control System using IoT and Telegram

J. Saivikas[1], N. Veena Madhuri[2], K. Pothu Raju[3], K. Nitin[4], R. Anil Srinivas[5], V. Sateesh[6]
Department of Electronics and Communication Engineering
Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, India.
saivikasjami2000@gmail.com[1]

Abstract- The device's objective is to protect fishermen's gear. Raspberry Pi processors are used as both the station and the controller for the warehouse's intrusion detection system (IDS). This involves the use of face recognition technologies and telegraph alerts. A USB cord connects the PIR sensor, camera processing, and buzzer processing to the Raspberry Pi. The notification system communicates with bots using Telegram's API. When a person is recognised, the camera records a video and saves it to the SD card. This is compared using the database's information. It sends a video to the owner's telegram account as a notification/alert to the owner that there is an intruder in the Aqua Farm, and a buzzer is used as an alarm to notify the nearby residents when the unknown intruder is noticed on camera. pond ecosystems employ the planned project for fishing activities..

Keywords- Alert, Face recognition, Intrusion Detection System (IDS), Raspberry pi, Telegram.

I. INTRODUCTION

The thefts at the aquafarm have become a major source of worry in modern times. There are now a few surveillance options on the market, but they have various limitations, including high costs, low transmission distances, reliance on PCs, and a high need for storage space [1] [2]. To address the shortcomings of current monitoring systems, this research proposes an intrusion detection system that is both frugal and energy efficient and is cheap to aquaculture [3]. Some of the components of the Intrusion Detection System that ensure security include facial recognition, telegram alerting, and motion detection [4]. One of the most appropriate approaches for assisting aquafarm owners in remotely monitoring the aquafarms is to utilise IoT (Internet of Things) [5].

The PIR sensor is utilised in Aqua Farm to detect intruder movements. It activates the camera, and footage of the invader begins to be taken. If the data of the person entering the farm (owner or worker) is available in the database, no alarm is issued to the owner by telegram; otherwise, the owner is notified and locals are warned through a buzzer. Telegram is used for notifications instead of other apps because it allows you to share many photos and videos (up to 1.5 GB) and has more security, speed, and no advertising or additional premium content. It has no subscription fees, and it is easily accessible on Android and iOS devices, whereas others, such as G-Mail and Twitter, are very time-consuming to use [6]. The major goal of this article is to build and deploy a cost-effective and secure aqua theft monitoring system.

The literature review has also been completed. The suggested item is IoT and telegram-based theft control system for aqua farmers has the benefit of notifying not just one but a large number of people when they are joined to the group. Because the face recognition system utilised is dynamic and can be trained to learn new faces instantly, it addresses some of the issues identified in previous research. This technology is so adaptable and user-friendly that even inexperienced users can use it. It employs a motion sensor and only activates when motion is sensed, using less electricity and promoting its widespread use. This system was designed with aqua farmers in mind, but its adaptability allows it to be applied to a broad range of applications based on facial recognition and alerting systems. Introduction, methodology, results & discussion, and conclusion are the four sections of the study.

II. METHODOLOGY

For this product, a Raspberry Pi is utilised to build an intrusion detection system, which needs hardware and software cooperation. In the hardware implementation of this project, the Raspberry Pi, controller board, camera module, passive infrared sensor, and buzzer are all used. Raspbian Buster is the operating system, and Python is used to develop programmes for the board. Python libraries such as OpenCV and Imutils, as well as Dlib's face recognition components, are used to process photos. The user utilises Telegram messenger to connect with the system and get intrusion detection warnings. [7]

Hardware Requirements:

1. Raspberry pi 3B+ (BCM2837): A credit card-sized computer that acts as the core of the proposed system [8]. The Raspberry Pi 3B+ from Broadcom exceeds its predecessors in terms of performance. On this 64-bit quad-core SOC, the A53 CPU (ARM Cortex) operates at 1.4GHz.
2. The recommended model can record video at 720p with 30fps using the Logitech C270 HD Webcam, which features an automatic light adjustment capability for higher image processing output [9].
3. This kind of passive infrared sensor (PIR) determines whether or not an object is moving by monitoring the infrared radiation it produces (Model HC-SR501). Unlike Active Infrared sensors, which produce an infrared beam, this kind of motion sensor only receives infrared waves. A PIR sensor can detect people, animals, and other things. Pyroelectric sensors detect infrared light and are used in infrared sensors such as the PIR. The detector does not generate energy; rather, it receives it passively.
4. When an electrical signal is sent through a buzzer, it creates a different beep sound depending on the kind of signal. The sound source may produce sound for many seconds. When an intruder is detected, the buzzer in the recommended device sounds.

Software Requirements:

1. The Raspberry Pi Buster is a Debian-based eco-friendly operating system for the Raspberry Pi. Debian 10 is being worked on by the Raspbian Buster developers. Other Raspbian OS versions with minor differences include Stretch, Jessie, and Bullseye. Buster's security has been strengthened between OS versions.
2. The Python programming language In this section, we'll use Python to teach the Raspberry Pi the objects in our model [11]. programming language for machine learning and application interfaces. It includes a number of functions, modules, and libraries that the user may access. Open-source software teaches the Raspberry Pi and connects it to apps such as Telegram and WhatsApp [12].
3. The Telegram app is available for free on both Android and iOS. This tool encrypts media files from beginning to finish and may be used on both PCs and mobile devices. A group may share material by using a telegraph server. To trade media, the suggested option makes use of a Telegram bot. A telegram bot may send media without using phone numbers.

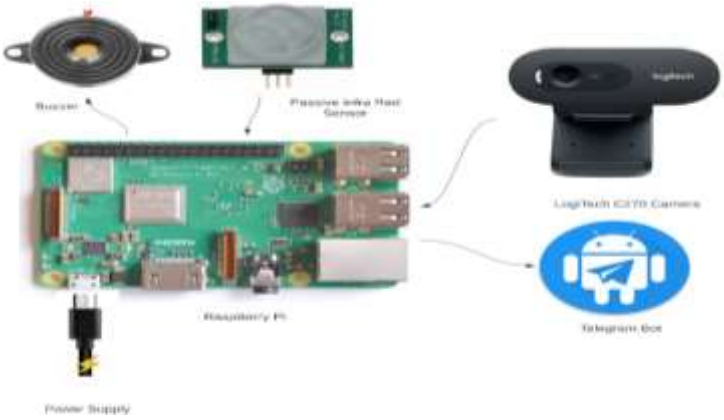

Fig. 1. Connections of raspberry pi

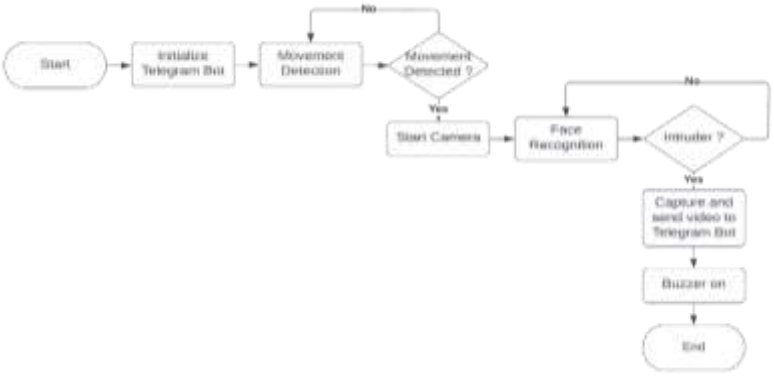

Fig. 2. Flow Chart

Pond ecosystem aquaculture producers use the methodology we propose to increase production by providing an intrusion detection system to reduce thefts in their facilities [13]. Fig. 1 depicts the precise linkages between all suggested components. Figure 2 depicts the proposed model's flow chart. In the suggested system, a PIR sensor is used to identify people or animals based on their body temperature. If the PIR sensor detects any human motion, it will send a signal to the Raspberry Pi via GPIO pins, which will activate the face recognition system by turning on the camera module. The camera will record the scene, which will then be transferred to the Raspberry Pi for face recognition [14]. The Raspberry Pi employs the Histogram of Oriented Gradients (HOG) [15] for face recognition [16][17].

Following face recognition, the computer will categorise the individual in the frame as the owner or an unknown person [18][19]. If there is an unknown person, the raspberry pi will record a brief video and transmit it to the owner's telegram bot using the Bot API key and chat id. This is possible thanks to the Telegram library, which is installed in Python and offers a pure Python interface to the Telegram Bot API[18][19]. The Telegram bot may be created by searching for @botfather, selecting the bot, and then entering /newbot to create a new one. Select a name and user id for the bot, and it will return the bot API key [20][21]. The conversation id of the owner's Telegram account must be supplied in the Python code. By using certain methods in the library, the model will be linked to the Telegram bot so that it can send alerts and video messages[22][23].

III. RESULTS AND DISCUSSIONS

The previous work compares facial recognition and telegram alerting. However, the older work has the limitation of simply sending photographs to the owner as evidence [24]. This recommended effort improves evidence and enables speedy action against theft by delivering the video via a telegram bot and a group message to both the owner and his staff. Face recognition algorithms like HOG and SVM are

utilised to identify the intruder and the home's owner. The completed model will resemble the one shown in Figure 3.

Fig. 3. Complete model image

The below block diagram depicted in Fig. 4 represents the model's programmed method:

Fig. 4. Programmatic Approach

The Fig.4 depicts the sample collection, Training model, Face recognition, and Telegram Alerting.

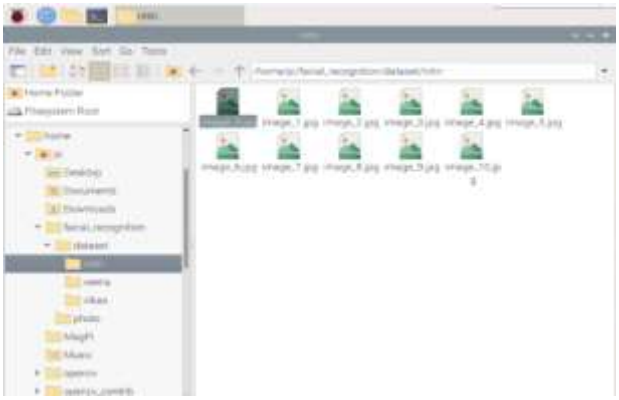

Fig. 5. Collecting Samples-1

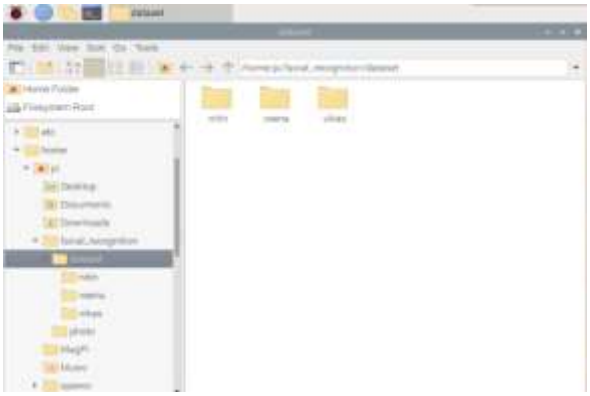

Fig. 6. Collecting Samples-2

Some processes must be undertaken before installing the proposed model on the field since it includes some measures for face recognition, which are listed below:

Step 1: Gather images of the owner and servants in order to identify them. The number of images gathered for each individual might vary from 10–100. The photos are saved in the folders seen in Figs. 5 and 6.

Step 2: After gathering the photographs, this data must be trained on the Raspberry Pi by extracting the characteristics of faces using Histogram of Oriented Gradients (HOG) and saved in a format that can be accessed by a face recognition tool.

Step 3: After gathering the essential characteristics for detection, the model is ready for identification.

Step 4: The device will also transmit a video to the owner's Telegram App as a backup. Figures 7 and 8 show the face recognition results:

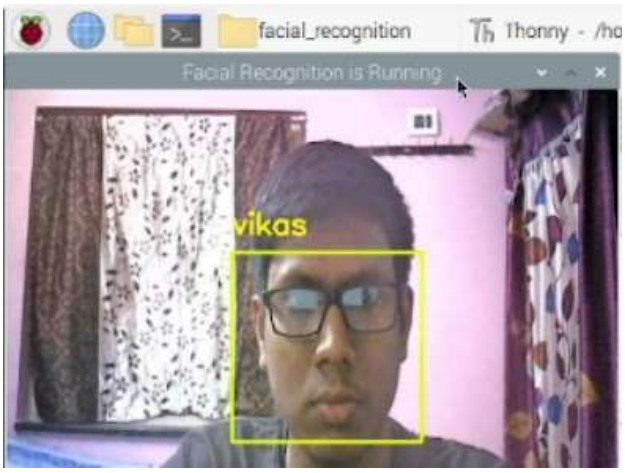

Fig. 7. Authorized person detection

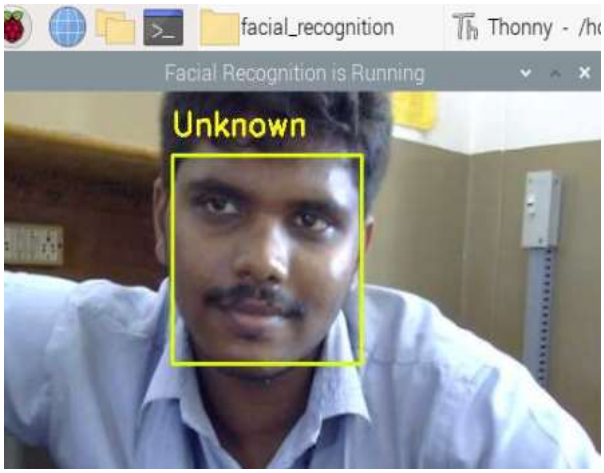

Fig. 8. Unauthorized person detection

Fig. 9.1. Telegram alert only to the owner

Fig. 9.2. Telegram alert via group

Fig. 9.1 and Fig. 9.2 depicts a telegram warning from an unnamed individual. An unnamed person has created a telegram group for the owner and his or her staff to share a theft control system. In addition to

assisting the owner in locating the thief, this telegram video message employs a buzzer to alert the surrounding community to take action[25].

IV. CONCLUSION

The proposed IoT-based theft control system for aqua farmers utilising Telegram has successfully completed the test cases relating to face recognition and Telegram integration. In addition, the suggested model has incorporated intruder detection using the PIR sensor, and the video message of the intruder surveillance is communicated to the corresponding owner through the Telegram app. In comparison to prior efforts, the face recognition in this study was effective when it was taught using machine learning methods. At the moment, the suggested model is for farmers' requirements, individuals who work in the pond for fishing, and those who run fish markets to safeguard their products and services. Furthermore, the suggested model may be expanded by integrating with other sensors such as temperature, pH sensors, humidity sensors, and rain sensors that are relevant in their surroundings, and these sensor values are communicated to the respective owners through the Telegram app. Furthermore, the suggested model may be expanded by incorporating this intruder monitoring data into the cloud system of the appropriate police station.

V. REFERENCES

1. Adarsh Prabhakar Chantar, Charan G Bhaktha, Manjunath S G, Manojkumar H M. “Home Surveillance System using Raspberry Pi. 2016 175 – 188.

2. D Abhilash, Chandrashekar Chandrashekar, and S Shalini. 2017. Economical, energy efficient and portable home security system based on Raspberry Pi 3 using the concepts of OpenCV and MIME. In 2017 International Conference on Circuits, Controls, and Communications (CCUBE). IEEE, 60–64.

3. Mfundo Zuma, Pius A Owolawi, Vusi Malele, Kehinde Odeyemi, Gbolahan Aiyetoro, Joseph S. Ojo, “Intrusion Detection System using Raspberry Pi and Telegram Integration”. icARTi ’21, December 9–10, 2021, Virtual Event, Mauritius https://doi.org/10.1145/3487923.3487928

4. D. Sri Sai Mahesh, T.Maneesh Reddy, A.Sai Yaswanth, Dr. C Joshitha, and S. Sudarshan Reddy, “Facial Detection and Recognition System on Raspberry pi with Enhanced Security”. 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)

5. Neha Patil, Shrikant Ambatkar and Sandeep Kakde “IoT Based Smart Surveillance Security System using Raspberry Pi” in Proc. International Conference on Communication and Signal Processing, April 6-8, 2017, India.

6. N. Hema and Juli Yadav, "Secure Home Entry Using Raspberry Pi with Notification via Telegram". IEEE 2020 6th International Conference on Signal Processing and Communication (ICSC)

7. Gagandeep Singh Nagpal, Gagandeep Singh, Jappreet Singh, Nishant Yadav "Facial Detection and Recognition using OpenCV on Raspberry Pi Zero" in Proc. International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018).

8. Raspberry pi - https://www.raspberrypi.com/documentation/

9. G. Senthikumar, K. Gopalakrishnan and V.S. Kumar, "Embedded Image Capturing System using Raspberry Pi System," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 3(2), pp. 3, 2017.

10. Irina Mazwin Hazri, Mus'ab Sahrim, Wan Zakiah Wan Ismail, Irneza Ismail, Shahnurriman Abdul Rahman, Filzah Syairah Hussin, "Automated Motion Detection Security System Notifier using Raspberry Pi with Telegram".

11. python- https://www.python.org/doc/

12. Wilson Feipeng Abaya, Jimmy Basa, Michael Sy, Alexander C. Abad and Elmer P. Dadios, "Low Cost Smart Security Camera with Night Vision Capability Using Raspberry Pi and OpenCV". 7th IEEE International Conference Humanoid, Nanotechnology, Information Technology Communication and Control, Environment and Management (HNICEM)
2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)

13. Umi Najiah Ahmad Razimi, Mohammed Hazim Alkawaz, and Shamla Devi Segar, "Indoor Intrusion Detection and Filtering System Using Raspberry Pi". 2020 16th IEEE International Colloquium on Signal Processing & its Applications (CSPA 2020).

14. Nafis Mustakim, Noushad Hossain, Mohammad Mustafizur Rahman, Nadimul Islam, Zayed Hossain Sayem, and Md Asaduz Zaman Mamun. 2019. Face Recognition System Based on Raspberry Pi Platform. In 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT). IEEE, 1–4.

15. H. S. Dadi and G. K. Mohan Pillutla, "Improved face recognition rate using HOG features and SVM classifier," *IOSR j. electron. commun. eng.*, vol. 11, no. 04, pp. 34–44, 2016, doi: 10.9790/2834-1104013444.

16 Ramaiah, V. S., Singh, B., Raju, A. R., Reddy, G. N., Saikumar, K., & Ratnayake, D. (2021, March). Teaching and Learning based 5G cognitive radio application for future application. In 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 31-36). IEEE.

17 Saikumar, K., Rajesh, V., Babu, B.S. (2022). Heart disease detection based on feature fusion technique with augmented classification using deep learning technology. Traitement du Signal, Vol. 39, No. 1, pp. 31-42. https://doi.org/10.18280/ts.390104
18 Mythreya, S., Murthy, A. S. D., Saikumar, K., & Rajesh, V. (2022). Prediction and Prevention of Malicious URL Using ML and LR Techniques for Network Security: Machine Learning. In Handbook of Research on Technologies and Systems for E-Collaboration During Global Crises (pp. 302-315). IGI Global.
19 Garigipati, R. K., Raghu, K., & Saikumar, K. (2022). Detection and Identification of Employee Attrition Using a Machine Learning Algorithm. In Handbook of Research on Technologies and Systems for E-Collaboration During Global Crises (pp. 120-131). IGI Global.
20 Raju, K., Pilli, S. K., Kumar, G. S. S., Saikumar, K., & Jagan, B. O. L. (2019). Implementation of natural random forest machine learning methods on multi spectral image compression. Journal of Critical Reviews, 6(5), 265-273.
21 Rao, K. S., Reddy, B. V., Sarada, K., & Saikumar, K. (2021). A Sequential Data Mining Technique for Identification of Fault Zone Using FACTS-Based Transmission. In Handbook of Research on Innovations and Applications of AI, IoT, and Cognitive Technologies (pp. 408-419). IGI Global.
22 Koppula, N., Sarada, K., Patel, I., Aamani, R., & Saikumar, K. (2021). Identification and Recognition of Speaker Voice Using a Neural Network-Based Algorithm: Deep Learning. In Handbook of Research on Innovations and Applications of AI, IoT, and Cognitive Technologies (pp. 278-289). IGI Global.
23 Kailasam, S., Achanta, S. D. M., Rao, P. R. K., Vatambeti, R., & Kayam, S. (2021). An IoT-based agriculture maintenance using pervasive computing with machine learning technique. International Journal of Intelligent Computing and Cybernetics.
24 Raju, K. B., Lakineni, P. K., Indrani, K. S., Latha, G. M. S., & Saikumar, K. (2021, October). Optimized building of machine learning technique for thyroid monitoring and analysis. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1-6). IEEE
25 Ajay, T., Reddy, K. N., Reddy, D. A., Kumar, P. S., & Saikumar, K. (2021, December). Analysis on SAR Signal Processing for High-Performance Flexible System Design using Signal Processing. In 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 30-34). IEEE.