International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 03 | Mar 2023 www.irjet.net p-ISSN: 2395-0072

Intrusion Detection System Using Face Recognition

Ayush Dubey[1], Ajay Pandey[2], Riya Pandey[3], Zuhair Bhati[4], Reena Kothari[5]

[1,2,3,4,5] *Department of information Technology, Shree LR Tiwari College of Engineering, Maharashtra, India*

Abstract - *The Intrusion Detection System Using Face Recognition is a security system that uses facial recognition technology to detect and prevent unauthorized access. This system works by capturing images of people attempting to gain access to a secure area and comparing them to a database of authorized personnel. The system can identify and alert security personnel if there is a match with an unauthorized person. The proposed system utilizes machine learning algorithms and deep learning techniques for improved accuracy and reliability. This system uses a Raspberry Pi, Sensor, Camera, Email services and Python & Shell Script. The system can be used in various settings, including airports, banks, and government institutions, to enhance security and prevent potential security breaches.*

Key Words: Security System, Facial Recognition, Raspberry Pi, Python Scripts, Machine Learning.

1.INTRODUCTION

Security has always been a top priority for organizations seeking to protect their assets and prevent unauthorized access. Traditional security measures such as locks, badges, and passwords have been effective to some extent, but they are not foolproof. As technology continues to evolve, organizations need to adopt advanced security measures that offer higher accuracy and reliability. One such measure is the Intrusion Detection System Using Face Recognition.
This is an advanced security system that utilizes facial recognition technology to detect and prevent unauthorized access. This system captures images of individuals attempting to gain access to restricted areas and compares them to a database of authorized personnel. If there is a match with an unauthorized person, the system alerts security personnel, who can then take appropriate action.

This paper aims to provide a comprehensive understanding of the Intrusion Detection System Using Face Recognition and its potential to enhance security measures in organizations.

The objective is to offer insights into the working principles of the system, its advantages, its applications, and its limitations, providing a foundation for future research and development.

2. PROPOSED SYSTEM

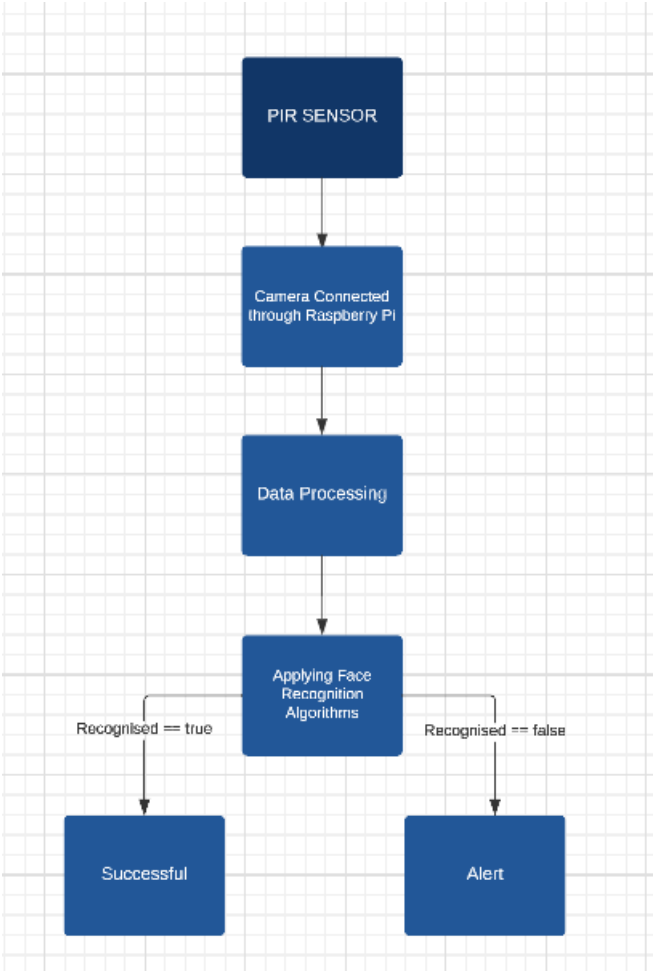

Fig -1: Flowchart

The proposed system for the Intrusion Detection System Using Face Recognition is designed to provide a highly reliable and efficient way to detect and prevent unauthorized access. The system comprises the following components:

It uses Hardware such as

- Raspberry Pi
- Camera Module
- Jumper Cables
- Motion Sensor

And software such as

- Python Scripts
- Mutt email client
- Raspberry Pi-Camera Interfacing
- GPIO Pins Programming

This system uses Face Detection component which is responsible for detecting and localizing faces in the input image. It utilizes algorithms such as Haar cascades or deep learning techniques such as Convolutional Neural Networks (CNNs) to accurately detect and extract faces from the input image.

The main component of this project is the Raspberry Pi, a small computer that powers the intrusion detection system's backend operations. We use Python and shell script to code all of our programs.

Functional setup of IDS components:

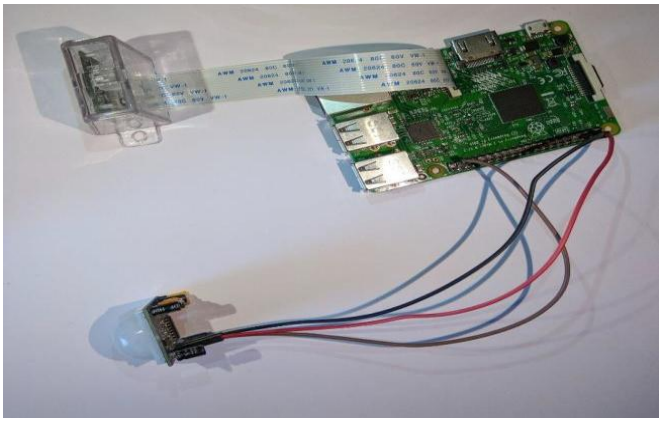

Fig -2: Proposed System containing all the functional units

Due to its user-friendly features and cost advantages, Raspberry Pi has been chosen as the system's processing unit. The Raspberry Pi has been given the algorithmic rule that was programmed in Python. It is programmed so that it first sets all of the GPIO Pins to provide a correct interface between all of the attached devices and the Raspberry Pi, after which all of the connected modules will carry out their functions as intended.

3. Algorithm

Below is a list of algorithms analyzed for the Facial Recognition Process:

3.1 CNN

Convolutional Neural Networks (CNNs) are a type of neural network that are commonly used for image classification, object detection, and other computer vision tasks. They are made up of a series of layers, including convolutional layers, pooling layers, and fully connected layers, that allow the network to learn hierarchical representations of the input data. This makes CNNs particularly effective for tasks such as object recognition, where the network needs to be able to identify objects at different scales and orientations.

3.2 SVM

The support vector machine (SVM) is a classification technique applied on linear as well as nonlinear data. It is a composite version of KNN combined with SVM for image catalog recognition and is increased in. [7] In this algorithm, training is done with the help of the nearest K the neighbors of the data point are not labeled. First, K- nearest data points are determined. Then pair the distance between these K data points is calculated. Hence, we get a distance matrix from the calculation distance. The Kernel matrix is then designed from distance matrix is obtained. This core matrix is provided as input to the SVM classifier. The result is the class of the data point is unknown. In addition, a can use SVM but time consuming is one of the defects. It also involves calculation pair distances.

3.3 FisherFaces

FisherFaces is a technique for face recognition that uses linear discriminant analysis (LDA) to find a low-dimensional representation of face images that maximizes the separation between different individuals. The basic idea behind FisherFaces is to project high-dimensional face images onto a lower-dimensional subspace where each dimension corresponds to a linear combination of pixel values. This projection is done in a way that maximizes the ratio of between-class variance to within-class variance, which effectively separates the face images corresponding to different individuals. To perform face recognition using FisherFaces, a set of training images is first used to learn the subspace projection. This involves computing the mean face and eigenvectors of the covariance matrix of the face images, and selecting the top eigenvectors that maximize the Fisher criterion. Once the subspace projection is learned, a new face image can be projected onto the subspace, and compared to the training images using a nearest neighbor or other classification algorithm.

4. Literature Review

Mehek Male, Sahil Colvalkar, Ajay Pandey, and Sarvesh Pandey, [1] developed a security system that uses motion detection to identify potential intruders in a protected area. It is designed to be used in a variety of applications, including home security, commercial security, and military and law enforcement operations. The system works by using motion sensors to detect any movements within a protected area. When motion is detected, the system sends an alert to the user or security personnel. The system can be configured to

work with a variety of sensors, including infrared sensors, ultrasonic sensors, and microwave sensors. It appears to be a promising solution for detecting intruders and enhancing security in a variety of settings. However, its effectiveness and suitability may depend on various factors such as the specific application, environment, and the quality of sensors and system setup. It is always recommended to evaluate the system's capabilities and limitations before implementing it in a particular setting.

Usman Shuaibu Musa, Megha Chhabra and Aniso Ali, Mandeep Kaur, [2] published their research work on Intrusion Detection System (IDS) using Machine Learning (ML) techniques which has become an increasingly popular research area in recent years. IDS is a security mechanism that identifies malicious activities and potential security breaches in computer systems. ML techniques provide a promising approach to improve the accuracy and efficiency of IDS.

Irving Vitra Paputungan, Mahbub Ramadhan Al Fitri and Unan Yusmaniar Oktiawati [3] presented a research paper which explores the design and development of a DIY home security system that utilizes motion and movement detection technology to enhance security measures. The system uses an infrared sensor to detect movement within a specific range and triggers an alarm if the movement is detected within the user-defined boundary.

Lixiang Li, Xiaohui Mu, Siying Li and Haipeng Peng [4] have proposed a comprehensive and insightful overview of the current state of face recognition technology. The article provides a thorough introduction to the history and development of face recognition technology, as well as a detailed explanation of the various techniques and algorithms used in modern facial recognition systems. The authors also explore the ethical and social implications of the technology, including privacy concerns and potential biases.Overall, this review provides a valuable resource for anyone interested in understanding the technical and societal implications of face recognition technology. It is well-researched, clearly written, and provides a balanced perspective on the topic.

M. Khan, S. Chakraborty, R. Astya and S. Khepra [5] published a Face detection and picture or video recognition which is a popular subject of research on biometrics. Face recognition in a real-time setting has an exciting area and a rapidly growing challenge. Framework for the use of face recognition application authentication. This proposes the PCA (Principal Component Analysis) facial recognition system.

5. RESULTS & ANALYSIS

Let us just go through the components used in this Intrusion detection system and then analyze the output results.

Fig -3: Passive Infrared Sensor

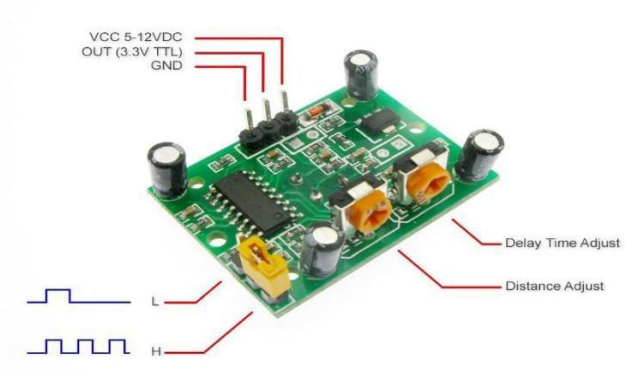

Fig -4: Pin layout of the PIR (Passive Infrared) sensor

Fig -5: Raspberry Pi 3 Model B v1.2 (Front)

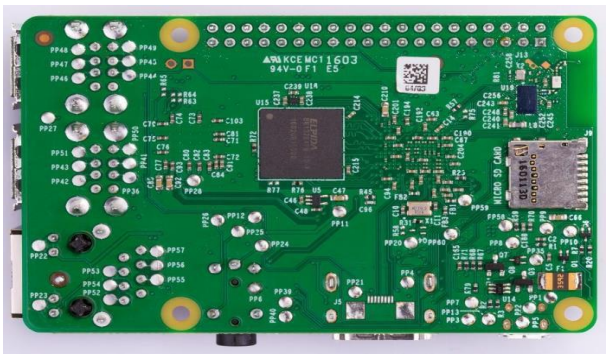

Fig -6: Raspberry Pi 3 Model B v1.2 (Back)

Fig -7: Pi-Camera

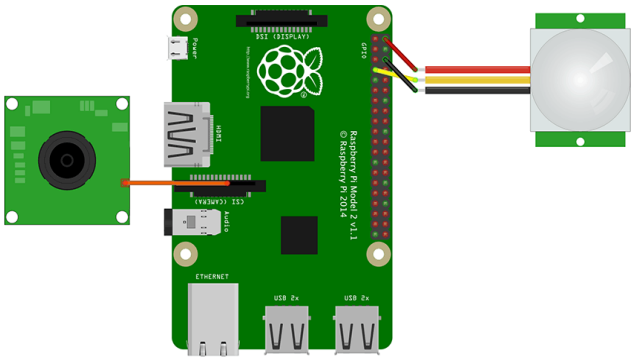

Fig -8: Connection of the Pi-Camera to the Raspberry Pi

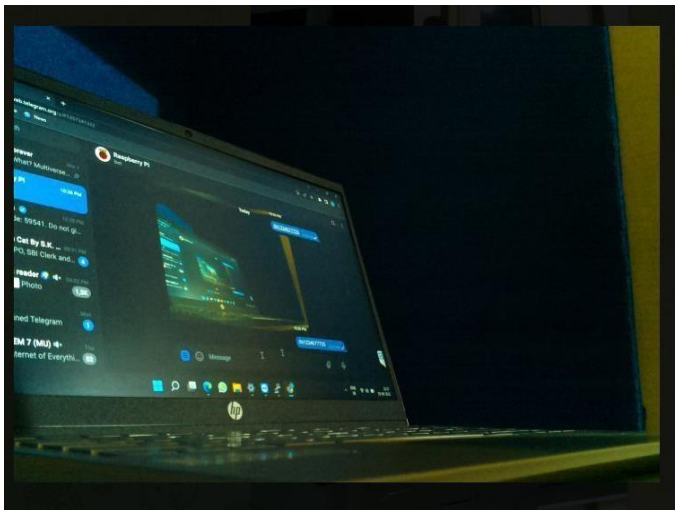

Fig -9: Output Screenshots from Pi-Camera

6. CONCLUSIONS

In today's generation, everything relies on computation and data either directly or indirectly. This project has hardware and software package. Hardware describes how the system was designed, what module will it use. The system is meant for un-welcomed person detection. An Intrusion Detection System using Face Recognition is a sophisticated security system that uses advanced algorithms and machine learning techniques to detect and prevent unauthorized access to a secure area. It works by capturing images of people who are attempting to enter a restricted area, and then comparing those images against a database of known faces. If the system detects a match, it grants access; otherwise, it denies entry and raises an alarm. One of the key advantages of this system is that it is highly accurate and can operate in low-light conditions, making it suitable for use in a variety of environments. It is also a non-intrusive method of access control, which can be important in situations where privacy is a concern. However, there are also some potential drawbacks to using a face recognition-based intrusion detection system. One concern is that the technology may not be completely reliable, especially if the lighting conditions are poor or if the person being scanned is wearing a disguise or mask. Additionally, there are potential privacy concerns associated with using facial recognition technology, particularly if the system is storing and analyzing biometric data. The projected system provides digital computer primarily based home security system by use of terribly advanced low price stable software package.

7. FUTURE SCOPE

By adding an alternative energy panel, the camera is going to be capable of gathering the solar energy and be wireless. We can add a feature, such as if intrusion is detected then automatically all doors will be locked, so the intruder wont

escape. We can send emergency signal to crime department. We can add alarm systems which will alert the security guards. There is always room for improvement when it comes to the accuracy of face recognition algorithms. In the future, we can expect to see more sophisticated techniques that can better handle factors such as changes in lighting, pose, and expression. IDS can be integrated with other technologies, such as artificial intelligence and machine learning, to enhance its performance. For example, IDS can learn from past security breaches and automatically adjust its rules and algorithms to detect new threats.

REFERENCES

[1] Mehek Male, Sahil Colvalkar, Ajay Pandey, and Sarvesh Pandey, "S.W.A.T – Motion Based Intrusion Detection System," (International Research Journal of Engineering and Technology (IRJET) 01 | Jan-2018) p-ISSN: 2395-0072; e-ISSN: 2395-0056.

[2] Usman Shuaibu Musa, Megha Chhabra and Aniso Ali, Mandeep Kaur, "Intrusion Detection System using Machine Learning Techniques", (Published in: 2020 International Conference on Smart Electronics and Communication (ICOSEC) Date Added to IEEE: 07 October 2020)

[3] Irving Vitra Paputungan, Mahbub Ramadhan Al Fitri and Unan Yusmaniar Oktiawati, "Motion and Movement Detection for DIY Home Security System", (Published in: 2019 IEEE Conference on Sustainable Utilization and Development in Engineering and Technologies (CSUDET)),Penang,Malaysia,2019,pp.122125,doi:10.1109/CSUDET47057.2019.9214684.

[4] L. Li, X. Mu, S. Li and H. Peng, "A Review of Face Recognition Technology," in IEEE Access, vol. 8, pp. 139110-139120,2020,doi: 10.1109/ACCESS.2020.3011028.

[5] M. Khan, S. Chakraborty, R. Astya and S. Khepra, "Face Detection and Recognition Using OpenCV," 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2019, pp. 116-119, doi: 10.1109/ICCCIS48478.2019.8974493.