IoT based Home Security through Image Processing

Santhosh K[1], Dr. Kiran P[2]

[1] *Computer Science and Engineering, RNS Institute of Technology, Channasandra, Bangalore, India*

[2] *Associate Professor, Computer Science and Engineering, RNS Institute of Technology, Bangalore.*

Abstract - IoT based Home Security through Digital Image Processing gives a framework for programmed framework to control and verify the home, in view of computerized picture handling with the assistance of Internet of Things (IoT). The framework comprises of a sensor, computerized camera, database and a cell phone. Sensors are put in the edge of the entryway which alarms camera, to catch a picture who means to go into the house, at that point sends the picture to the database. Picture examination is performed to distinguish and perceive and coordinate the picture with the put away dataset of the confirmed individuals. On the off chance that the picture caught does not coordinate with the dataset, at that point an alarm message is send to the proprietor of the house. The Face location and Recognition calculations are considered for the preparing spatial and time intricacy of the picture caught to cross check with the dataset put away in the database. The fundamental preferred standpoint of such a framework incorporates the simplicity of setting up, lower expenses and low upkeep.

Keywords: Internet of Things (IoT), Home Security, Digital Image Processing.

I. INTRODUCTION

In the present situation, ensuring safety and security has become an inevitable essentiality. Since it is well known that influence of modern technology has reached its peak, demand for security systems are going up progressively. Modern home needs intelligent systems with minimum human effort. With the advent of digital and wireless technologies, automated security systems becomes more intelligent. Surveillance camera helps the user to get a remote view of his home and the sensor networks add extra security features depending on the type of sensors. Adding Wi-Fi to security systems enables faster data transmission, and it will help the user to monitor and control the systems globally. In this approach, we introduce a newly revised security system using Raspberry Pi (IoT/Wi-Fi module) which integrates sensor alerts with video surveillance techniques. Raspberry Pi is a low cost, low power, single board computer which can handle multiple functions like a normal computer. Intrusion and fire detection are the prime features of this system. This system is purely based on Wi-Fi connectivity. Here, we use Wi-Fi module for wireless transmission instead of ZigBee. Having Wi-Fi connectivity is an added advantage for any system. Data can be fetched from anywhere and it can be moved to cloud for storage and monitoring. Also it has long range and high bandwidth, which makes it perfect for streaming video, sending email etc.

Moreover, the IoT module makes the system cost effective, compact, globally controllable and accessible. The objective of the project is to design and implement a low cost, reliable, energy efficient, long range, globally accessible, storage effective surveillance system using Raspberry Pi SBC, GSM Modem and Node MCU (IoT Module).

The need for security system at home is considered as one of the most important aspects of the modern life. Security mainly means protection against loss or damage, security systems have been evolving over time. These security systems may be Motion Detectors, Sensors or Actuators. In the present situation safety and security has become an inevitable essentiality. Since the influence of modern technology has reached its peak, demands for security systems have gone up progressively. Newer homes require intelligent systems with minimum human efforts.

Image analysis is nothing but mining of data in a sequential form from the images captured using Digital Image Processing techniques. Image analysis task is very complicated as it involves identifying a person from their face. Image analysis is mainly used for Pattern recognition, Digital Geometry and Signal Processing. Image Processing is nothing but processing of images using any form of signal processing to which the input is always an image or a series of images. The output of image processing will be either an image or a set of parameters which is related to the input image. The image processing technique treats the input image as a two-dimensional signal and applies the signal processing techniques to the image.

II. LITERATURE SURVEY

Wireless sensor networks play significant role in real environment. This paper presents a preliminary study of a smart WSN able to detect fire alarm. It has been set up useable a wireless sensor network with these three sensors.

An application was developed for determining physical home information with digital output. It has been designed a system android with Arduino hardware which consists of three sensors (flame, gas, heat) in home rooms. If the sensor readings value exceeds the pre-defined threshold level, the application system of the sensor network interface on mobile phone can be visible to users as notification form whenever they want [2]. The purpose of the project is to make a system, which would detect and take snapshots and videos of the motion when detected and upload to an external server. The major use of the 'Motion Detection' is at homes, buildings and also for surveillance for security for example of server rooms. Henceforth, by enhancing the capabilities of these technologies and integrating them, we hope to introduce the 'Motion Detection' system and to contribute to the current security system [1]. In this design, the authors use multiple sensor groups with low power consumption for the detection of an intruder. The MCU stays in a sleep state, unlike the traditional surveillance system which stays in the detection state. We reduce the power consumption in the alert or sleep state by 10.9 times by remaining 90% in the alert state and 10% in the detection state, and we use two sensor groups to improve the detection reliability of the alert state. In addition our home embedded surveillance system reduces unnecessary memory consumption for the capture of images without an intruder, compared to previous surveillance systems [4]. In this article, the authors describe the basics of the IoT architecture. By formalizing the various design parameters to consider, we provide a practical framework for users to build their own IoT devices and applications. We illustrate with concrete examples how various applications types can be built on top of the proposed architecture, and propose how the emerging real-time Web techniques can be applied to develop Web-compliant, highly interactive and integrable physical mashups. Finally, we provide an initial performance analysis and discussions to support the future research efforts that will make the Internet of Things a reality [7]. The experiment shows that the overall sensing probability improves with the use of multiple sensors having an MVM. The result is a higher cost because of the use of multiple sensors, amplifier circuits and the voting circuit. However, the improvement of the reliability significantly reduces the occurrences of false alarm from the home surveillance system [3].

III. ARCHITECTURE

The architectural configuration procedure is concerned with building up a fundamental basic system for a framework. It includes recognizing the real parts of the framework and interchanges between these segments. The beginning configuration procedure of recognizing these subsystems and building up a structure for subsystem control and correspondence is called construction modelling outline and the yield of this outline procedure is a portrayal of the product structural planning. The proposed architecture for this system is given below. It shows the way this system is designed and brief working of the system.

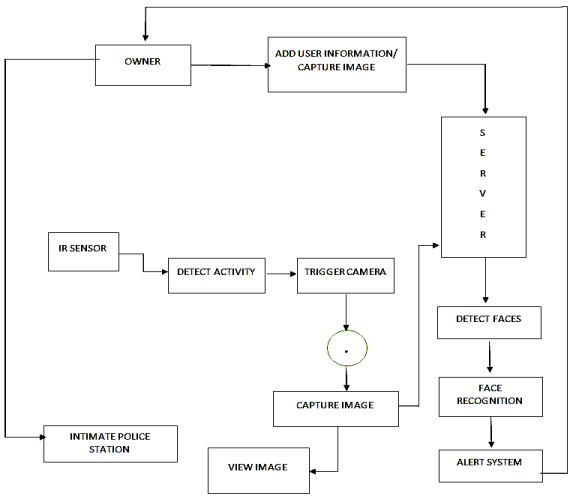

Fig 1- Architecture Diagram.

A. Registeration

Owner of the device can register to make use of the services. While registration the owner needs to provide the email id, mobile number and can set the password. Owner can login into the portal and can add the user. While adding the user, owner needs to provide the name of the user can you capture the face of the user and the face image will be saved in the server. For one user multiple face images are capture and stores this images into the server and will be used later for face recognition.

B. Security Device

We have used Raspberry Pi and few sensors and HD camera for the security system. We have used PIR sensor, IR sensor and fire sensor. All these sensors along with HD camera connected with the Raspberry Pi. IR sensor whenever it detects any motion or PIR sensor detect any human being triggers the camera. Once the camera is triggered it captures the image and the image is sent to the server. Once the server receives the image it applies face detection algorithm on to the image. If face detected then the face recognition algorithm is activated and if matches with anyone of the image that is saved in the server, it can recognize the image then it doesn't send to the owner and maintenance a log in the server containing the username and the time when the sensor detected the user. If any unknown person is recognized the owner receives an alert in the Android phone along with the image. If the owner wants he can press on the Alert button and the notification will be sent to the police station and if no face is detected

then the owner gets the notification with the image and can take necessary action.

C. Status Live

Now if the owner wants to check the live status, he can do that or get the information in his Android application. He can send a request for life photo to the Raspberry Pi, on receiving the request from the owner by the Raspberry Pi, it triggers the camera and camera captures the photo and a photo will be sent to the server and owner can view it form his Android application.

IV. WORK FLOW

A. Use Case Diagram

A use case chart is a kind of behavioural graph made from a Use-case examination. Its object is to present a graphical diagram of the usefulness gave by a framework regarding performers, their objectives (spoke to as utilization cases), and any conditions between those utilization cases. Use case chart gives us the data about how that clients and utilization cases are connected with the framework. Use cases concentrate on the conduct of the framework from an outside perspective. The performers are outside the limit of the framework, while the use cases are inside the limit of the framework. On-screen characters are spoken to with stick figures, use cases with ovals, and the limit of the framework with a container encasing the use cases.

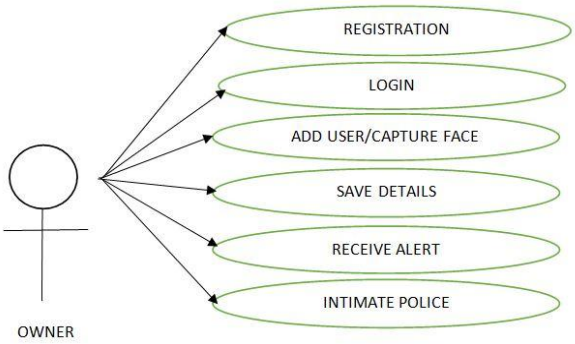

Fig 2- Use Case Diagram

B. Data Flow Diagram

The DFD is straightforward graphical formalism that can be utilized to speak to a framework as far as the info information to the framework, different preparing did on this information and the yield information created by the framework. A DFD model uses an exceptionally predetermined number of primitive images to speak to the capacities performed by a framework and the information stream among the capacities. The human personality is such that it can without much of a stretch see any progressive model of a framework in light of the fact that in a various levelled model, beginning with an extremely straightforward and unique model of framework, distinctive points of interest of a framework are gradually presented through the diverse orders. A data-flow diagram (DFD) is a graphical representation of the "stream" of information through a data framework. DFDs can likewise be utilized for the perception of information handling.

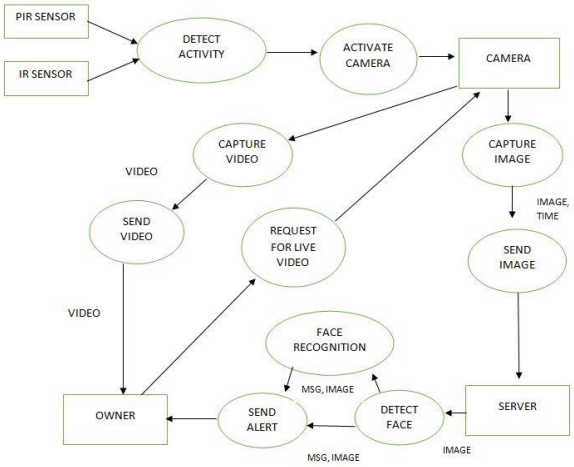

Fig 3- Data Flow Model

C. Sequence Diagram

A sequence diagram as shown is a system is an interaction diagram that shows how process operates with one and other and in what order. It's a construct of a message sequence chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and sequence of messages exchange between the objects needed to carry out the functionality of the scenario. Sequence diagram are sometimes called event diagrams or event scenarios.

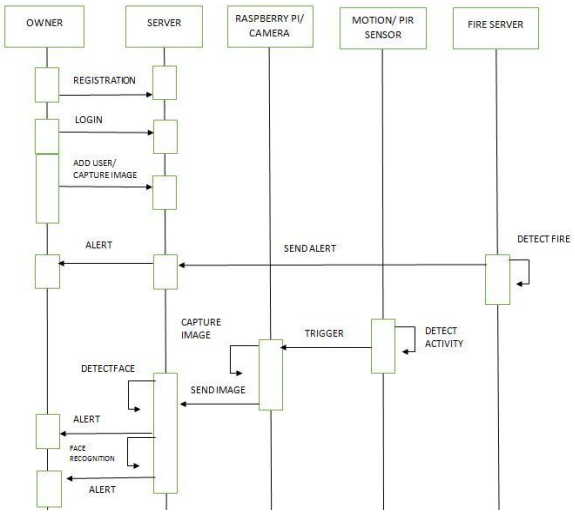

Fig 4- Sequence Diagram

V. PROPOSED METHODOLOGY

In the proposed system, a security system is introduced using raspberry Pi 3 which integrates sensor alerts with image surveillance techniques. The IR sensor is used for

detecting the motion. The HD camera is used for capturing the image. After the image gets captured it is sent to the server. It detects the face and recognizes the person. If the image gets recognized then the LED lights blink. If the face does not get recognized then it sends some alert to the owner and then the owner can intimate to the police station. The sensor that are fixed in the door, invokes the digital cameras in the rooms to capture image or motion. The captured image is sent to the fog where the dataset or database is stored. The Digital image processing techniques analyses and interprets the captured data. Information mining, Image enrichment and Feature extraction are the three imperative mechanism of digital image processing.

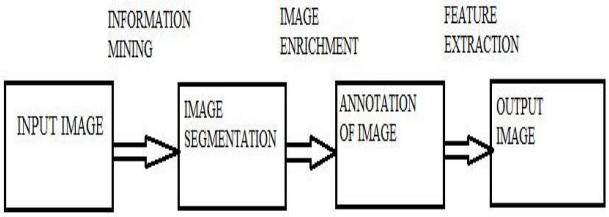

Fig 5- Image Processing

VI. ALGORITHM

Haar-Cascade Algorithm

A. Face Detection

Facial detection is impossible if the face is not isolated from the background. Although many different algorithms exist to perform face detection, each has its own weaknesses and strengths. These algorithms are computationally expensive and that is the major problem of these algorithms. Analyzing the pixels for face detection is time consuming and difficult to accomplish because of wide variations of shape and indecent within a human face. Pixels are also required for scaling and precision. Viola and Jones devised an algorithm, called Haar Classifiers, to rapidly detect any object, including human faces, using Ada Boost classifier cascades that are based on Haar-like features and not pixels.

B. Haar-Cascade Classifier

The core basis for Haar classifier object detection is the Haar-like features. These features, rather than using the intensity values of a pixel, use the change in contrast values between adjacent rectangular groups of pixels. The contrast variances between the pixel groups are used to determine relative light and dark areas. Two or three adjacent groups with a relative contrast variance form a Haar-like feature. Haar-like features, as shown in Fig. 10.4 are used to detect an image. Haar features can easily be scaled by increasing or decreasing the size of the pixel group being examined. This allows features to be used to detect objects of various sizes.

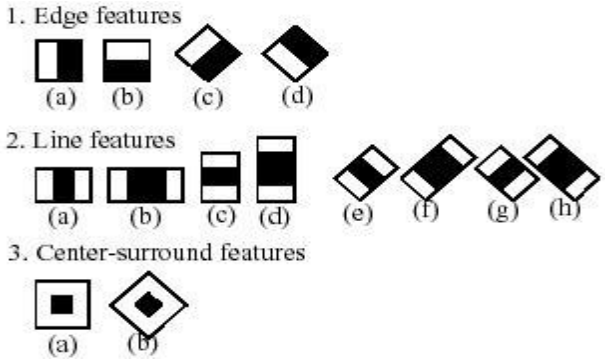

Fig 6- Common Haar Features

Detecting human facial features, such as the mouth, eyes, and nose require that Haar classifier cascades first are trained. In order to train the classifiers, this gentle Ada Boost algorithm and Haar feature algorithms must be implemented. Fortunately, Intel developed an open source library devoted to easing the implementation of computer vision related programs called Open Computer Vision Library (OpenCV). The OpenCV library is designed to be used in conjunction with applications that pertain to the field of HCI, robotics, biometrics, image processing, and other areas where visualization is important and includes an implementation of Haar classifier detection and training.

C. Feature Extraction

The main purpose of using features rather than the pixels directly is that features can act to encode ad-hoc domain knowledge, which is quite difficult to learn using a finite quantity of training data. In order to regionalize the image, one must first determine the likely area where a facial feature might exist. The simplest method is to perform facial detection on the image first. The area containing the face will also contain facial features. The best method to eliminate extra feature detection is to further regionalize the area for facial feature detection. It can be assumed that the eyes will be located near the top of the head, the nose will be located in the centre area and the mouth will be located near the bottom. The upper 5/8 of the face is analysed for the eyes. This area eliminates all other facial features while still allowing a wide variance in the tilt angle. The centre of the face, an area that is 5/8 by 5/8 of the face, was used to for detection of the nose. This area eliminates all but the upper lip of the mouth and lower eyelid. The lower half of the facial image was used to detect the mouth. Since the facial detector used sometimes eliminates the lower lip the facial image was extended by an eighth for mouth detection only. There are two steps involve in facial feature extraction. Facial feature detection is the first step in which face is detected. This requires analysing the entire image. Second step involves isolated face(s) to detect each feature.

VII. IMPLEMENTATION AND RESULTS

A. Web Application

The Owner who wishes to use the application or install the system in their house or office first needs to register in the web application, after which the owner/manager can add or delete the users. The owner can also access permissions to added users by allowing or deleting them in the application. The Login page is as shown.

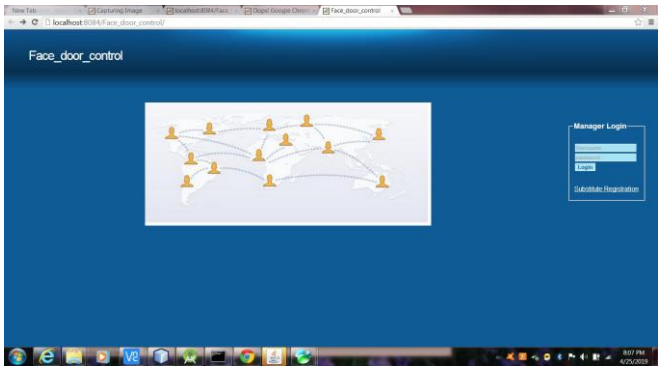

Fig 7- Login Page

Owner can add users by clicking on the Add User option on the main menu, which has an option to upload the user's name, number and photo. The user's details and photo is uploaded and is saved under user's name. After this the owner can grant permission to the user whether or not to enter the house, this process is shown.

Fig 8- Uploading User Details

B. Face Detection

In this approach an IR sensor is used, An IR sensor is used to detect any motion within its area. The IR sensor is fixed to the frame of the door which will always scan for motion within its range, if the IR sensor detects any movement it immediately triggers the camera to take multiple pictures of the area and sends it to the server with the help of Raspberry Pi. Upon receiving the image, it is further checked to identify whether the image has a face. If the image contains a face it is detected.

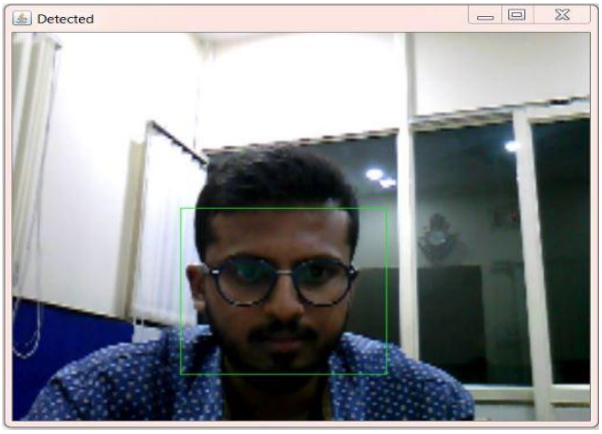

Fig 9- Face Detection

C. Face Recognition

If the image sent by the Raspberry Pi has a face it will be detected and further the images will be saved in a separate folder in the server. Another folder will contain all the images of the users which were taken by the owner while adding users to the application. Then the present image sent by the Raspberry Pi will be compared to the images of the users already present in the server. If the image matches with any of the stored user image then that user name will be matched and permission will be granted accordingly. From the folder the images that are to be matched are taken, the images in this folder are user images which were added by the owner.

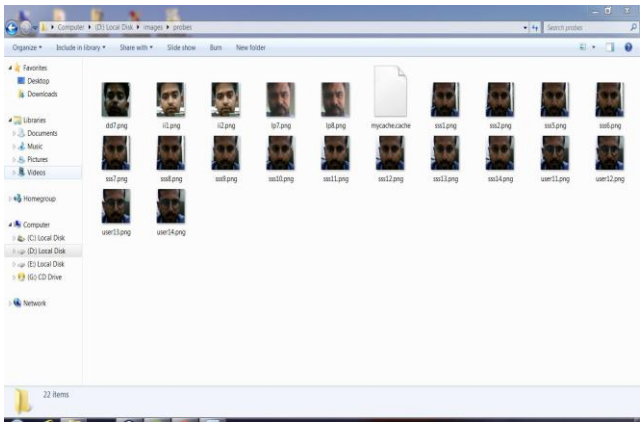

Fig 10- Registered User Images

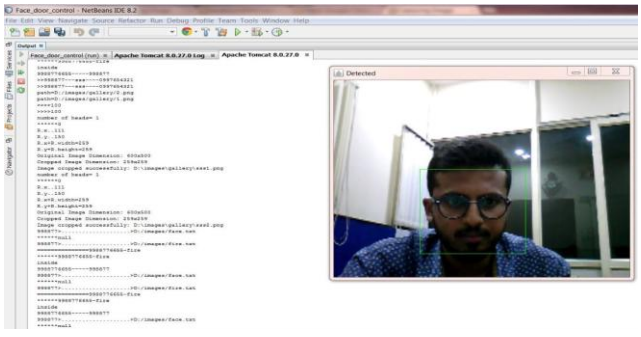

Fig 11- Face Recognition

The Image is sent by the server to the Android Phone, Owner can select permission in the Android application whether to allow or to not allow that person.

Fig 11- Image Received on Android Application.

VIII. FUTURE SCOPES

In future the Home Security System can be improved by adding a video camera of high resolution which will have the ability to capture a video of certain length and send it to the owner on request. The owner can view the video on the android application and intimate the police if some unknown person has entered their home or office.

ACKNOWLEDGEMENT

I would like to thank Dr. Kiran P (Dept. of CSE, RNSIT, Bangalore) for his valuable suggestions and comments that helped improving this work, this support is greatly appreciated.

REFERENCES

[1] Amid Nizam Ansari, Mohamed Sedky, "An Internet of Things approach for Motion Detection using Raspberry Pi", Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things, 2015.

[2] Karwan Muheden, Ebubekir Erdem, "Design and Implementation of Mobile Fire Alarm system using Wireless Sensor networks", 2016 IEEE 17th International Symposium on Computational Intelligence and Informatics (CINTI).

[3] Ying-Wen Bai, Li-Si Shen, Zong-Han Li, "Design and Implementation of Embedded Surveillance system by Multiple Ultrasonic Sensors", IEEE Transactions on Consumer Electronics (Volume: 56 , Issue: 1 , February 2010).

[4] Ying-Wen Bai. Zi-Li Xie, Zong-Han Li, "Design and Implementation of a Home Embedded Surveillance System using Low Alert Power", 2011 IEEE International Conference on Consumer Electronics (ICCE).

[5] Kumar, Sushant, and S. S. Solanki, "Remote home surveillance system," IEEE Int.Con.Advances in Computing, Communication, and Automation, 2016, pp. 1-4.

[6] Bai, Ying-Wen, Li-Sih Shen, and Zong-Han Li, "Design and implementation of an embedded home surveillance system by use of multiple ultrasonic sensors", IEEE Transactions on Consumer Electronics 56, no. 1 (2010).

[7] K. Gill, S. H. Yang, F. Yao, and X. Lu. A zigbee-based home automation system. IEEE Transactions on Consumer Electronics,55(2):422–430,May 2009.