

Detection of Potentially Suspicious Person on Real-Time Basis Using Embedded Platform

Sai Prabhu K.B.¹, Seema Sreekumar²

Dept. of Electronics and Communication Engineering, NITTE Meenakshi Institute of Technology, Bengaluru, India^{1,2}

Abstract: Embedded systems have occupied humans in all aspects of their day to day activities. The best suitable example which clearly justifies the above statement is the mobile phones. Why these mobile phones have become as addictive as drugs is due to the world wide connectivity using a most powerful tool called as the Internet. If we are able to use this technology in a progressive way for the welfare and well-being of the society, then we can create any kind of miracles. The Image and Video sharing part is playing a major role in this Internet era. So using this latest trend, this project has been implemented in reference to the above mentioned 3 criteria's which is: The Internet, well-being of society part – as: The Security feature and last part Image & Video sharing. This project is about Detection of Potentially Suspicious Person and streaming the Video and Images of the detected person on Real-Time basis.

Keywords: Raspberry PI, Haar Cascade classifier, Sensors, Face Detection.

I. INTRODUCTION

Embedded computing systems became pervasive section of our day to day activities like mobile phones, ATM machines, digital cameras etc. All those electronic devices that reduce human efforts and time except PC and desktop computing device units are known as embedded systems. Embedded systems play a big role in these days and together by day to day advancement in technology is increasing exponentially. So we tend to have gotten lots and lots of keen to embedded systems that are used for tasks ranging from providing recreation, to aiding the functioning of key human organs.

Embedded system can be a special-purpose system that's meant to perform a little low sort of dedicated functions for a selected application from medical instruments, home securities, geographical point equipment's and traffic signals to temperature controls and industrial machines. An embedded system contains sensors to capture varied input signals and produces a high output. The computing operation is performed with the intelligence provided among the system thus it performs as per the needs the higher operative frequency aboard the pipelined system to execute Millions of Instructions per Second (MIPS). The larger memory capability makes it achievable to develop advanced systems. The embedded system with the connectivity of internet (World Wide Web) permits them to react with the system anyplace and any time. The web controlled embedded systems are terribly rising in our daily aspect of life i.e., personal, medical, industrial or natural requirements. The wide varieties of microcontrollers available in the market for several applications of the embedded system developments are increasing on one hand and rising helpful demands multitasking-capable management systems to be used among an equivalent.

But still we tend to face many types of threats in our society on day to day basis. If we intend to use this developing technology and use the same in contrast for the aim of security, then majority of threats is reduced and many of disasters are avoided. Disasters are natural like landslides and natural calamities but artificial threats from

humans like thievery, bomb threat, violence against women, accidental responses and measures etc. These threats can be reduced before it attains crucial position and necessary action is performed at the proper time thereby avoiding major criminal activities in our society with the help of embedded systems. There are many embedded computing devices accessible within the market and with the assistance of those we are able to develop a secure and safer environment.

This project is an advance project in terms of security associated with threats in our society. The most objective of this project is to spot someone with suspicious behaviour or a suspicious person and also to spot a suspicious object on real time basis.

Whenever we try to implement the designed idea, we get the question "How such a factor can often be enforced??" This can be answered in the succeeding sections. Initially, literature survey for an equivalent indicates that there are many algorithms accessible or defining suspicious behaviour of a person with few bespoke software's like MATLAB and there are algorithms which should be enforced on a microcomputer or a computing devices.

Moreover the suspicious behaviour can be identified on the basis of images which are provided as the reference images. These things are not working on the real time basis because the real time surveillance cameras only captures the videos and stores the video on the Desktop computers which are connected to the camera in offline mode. But a person should be in front of the computing device and make the analysis as per the algorithm's logics and requires more time to get the results.

In order to beat these issues a brand new innovation should be created to mechanically and automatically determine the doubtless suspicious person or determine a suspicious object on real time basis.

So this project may be a new and innovative construct that indicates a threat on real time basis and conjointly lots of effort has been placed to analyse, to construct and also to implement an equivalent on real time basis.

II. RELATED WORKS

The previous existing system has no description about the present. So this current concept is a challenging and also extremely difficult task. The first challenge was to figure out how the video can be processed online, for this a related paper was available on the internet with the following details:

The paper [1] says about the implementation of the Compatible World Wide Web Controlled Embedded System using Arduino microcontroller. Embedded systems are used everywhere. Imagine when such a type of system is accessed globally using Internet i.e., World Wide Web the work associated with it also can be done at a faster rate and saves lot of time and makes easy access to work.

The ARM Cortex M3 microcontroller LM3S8962 has on chip Ethernet controller, RJ45 jack, sensors / transducers etc. These peripherals are used to access internet through a RJ45 jack present on the microcontroller. The programming of the microcontroller is done using Embedded C language. The on chip peripherals consists of data acquisition module, power supply module, media access controller, serial port, memory interface unit, physical layer, clock circuit and RJ 45 jack port. Each of these peripherals performs predefined specific functions and overall this microcontroller needs small coding in order to connect to the internet. Once the basic coding is completed there is a need to assign an IP address to access the internet through a Gateway by assigning a DNS gateway address. After assigning an IP address the device is ready to access the internet.

The paper [2] is about the Detection of Potentially Suspicious Behaviour. In large public transportation areas such as Metro stations and airports security staff rely on video Surveillance systems to facilitate their work. These systems are largely labor intensive so video Surveillance systems are extremely difficult to monitor randomly Occurring incidents. There is few automated video surveillance Systems which are mainly used for offline Video analysis after an event has occurred. These videos are most notably in The case of riot investigations and forensics. However, these systems are very little use in real time alerts.

III. SYSTEM CONFIGURATION

The concept was to detect the suspicious person in front of the camera; initially we have to upload an image of the person in the database. All the hardware components should work instantly without any delay and at first the PIR sensor should indicate that there is a person in front of the sensor and as an output it instructs the microcontroller to turn on the camera module. The camera will capture the image which is placed adjacent to the PIR sensor, compare it with the database and if there is a match a video should be recorded for a certain time interval and it should be stored in a particular location. Then the video should be redirected to the browser. The computer at the client end should be able to view the video and download the same from via internet. An alternative thing was to capture an image when there is any suspicious or high intensity sound

and when there is any kind of high vibration sensed in and around the camera or the sensor environment. When any of these variations are sensed, the camera should turn on and capture a High Definition image and store the image in a particular location. After this the images are redirected to the webpage and hosted via internet. The client end user should be able to download the image with date and time as the name of the image. Below the functional block diagram gives the clear picture of the same.

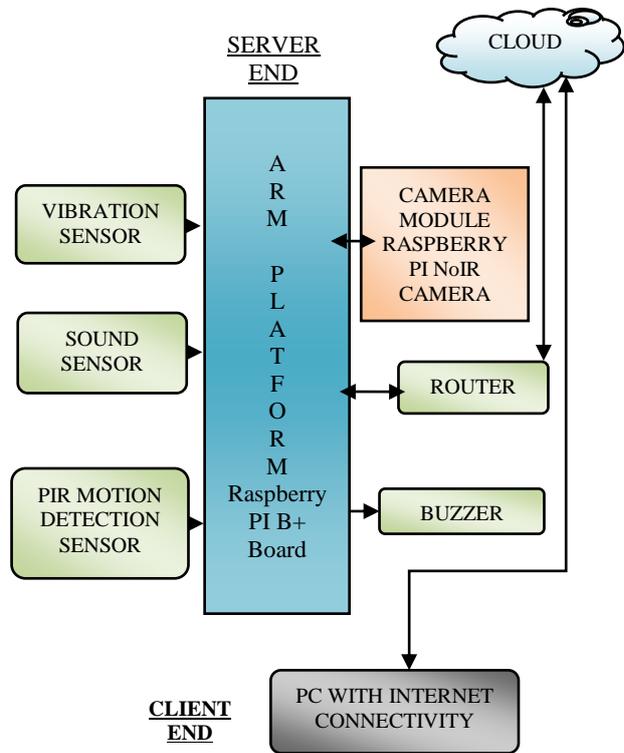


Fig 1 Schematic Diagram

Sensors detect variations and gives high output. The Microcontroller directs camera module to capture image or to record video as per the variation and output of the sensors. The captured image is stored in the microcontroller and the microcontroller is responsible for transmission of captured images and recorded video as input data to cloud via router. Router automatically generates IP address for the microcontroller and connects to internet directly to host images and videos. The hosted images and images can be viewed using a specific IP address or web address with the help of a browser. Pc with internet connectivity is responsible for viewing and downloading the captured images and recorded video data from server through cloud i.e. to access image and videos. The complete stepwise process flow is provided in the flow chart.

IV. WEBSERVER TO PROCESS IMAGES AND VIDEOS ONLINE

At this moment the captured video and image has to be hosted online using a microcontroller. The microcontroller used is the Raspberry PI B+ board and a Raspberry PI NoIR camera. The process flow for the same is shown below:

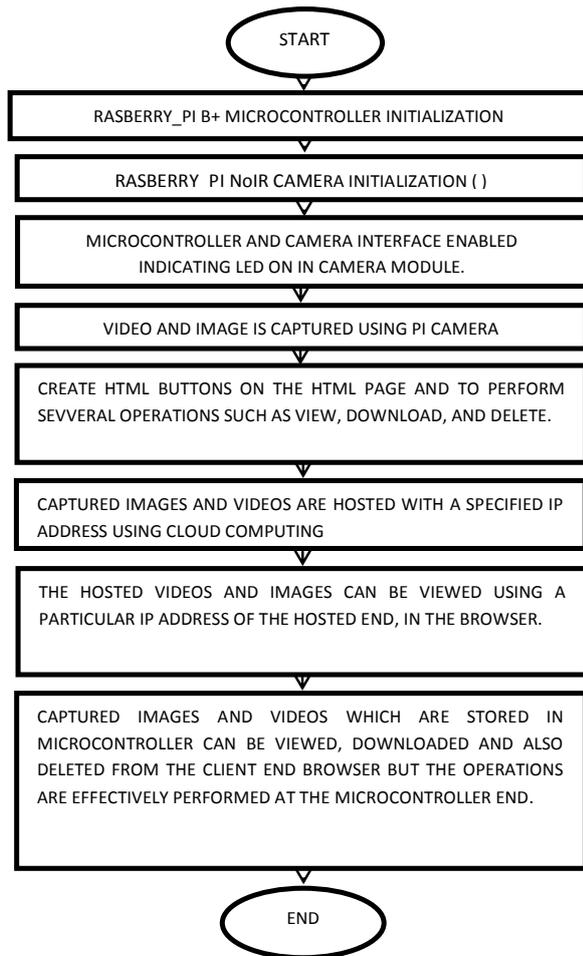


Fig 2 Real-Time video processing

V. IDENTIFYING FACES AND COMPARING

An algorithm called as HAAR-CASCADE CLASSIFIER algorithm is used to identify faces in the image and using this algorithm several modifications has to be made to match and compare the faces and to detect the potentially suspicious person on the image captured.

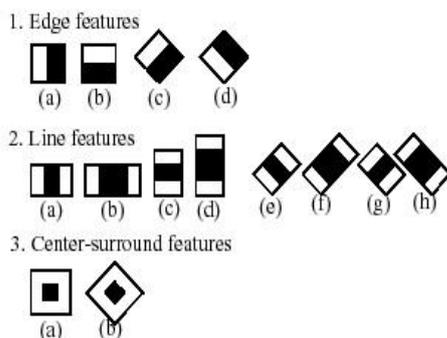


Fig 3 Common Haar features

The basic format of Haar classifier object detection is known as the Haar-like features. The primary features, uses the intensity values of pixels, but instead of that we can use the changes in the contrast value between the adjacent rectangular groups of pixels. The distinction variances or contrast variances between the picture element or pixel groups are used to verify relative light and dark areas. 2 or 3 adjacent groups with a relative

contrast variance types form a Haar-like features. These features, as shown in Figure below which are used to detect an image and they can easily be scaled by increasing or decreasing the size of the pixel group which are being examined. This allows features to be used to detect objects of various sizes.

VI. THE INTEGRAL IMAGE

The simple rectangular features of an image are calculated using an intermediate representation of an image, called the integral image. The integral image is nothing but a part of the whole image which is captured and each image can be divided in smaller sub units called as pixels. The integral image is an array containing the sums of the pixels' intensity values located directly to the left of a pixel and directly above the pixel at location (x,y) inclusive. So if A[x,y] is the original image and AI[x,y] is the integral image then the integral image is computed as shown in the below equation 1 and illustrated in Figure below:

$$AI [x,y] = \sum_{x' < x, y' < y} A(x',y') \text{ -----(1)}$$

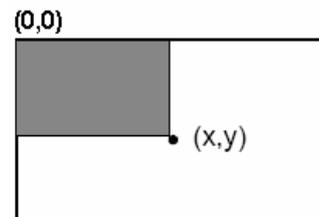


Fig 4 Summed area of integral image

The above technique which is called as integral image capturing technique is used to crop and select the face of person in the image and this part is done automatically with the help of the scripts and code. Once the face is captured, it tries to identify the eyes, nose and mouth in the face of the image which is captured and analysis the same using the changes in contrast values between the adjacent rectangular groups of pixels. Using this method several changes has been done to the basic structure of this algorithm and a new comparison method is adopted. The below mentioned steps are used to capture and compare the images using Haar-Cascade algorithm technique.

Step-1: At the initial stages we have to provide the picture or image of a person by manually uploading the same to the database and the images are stored in the microcontroller.

Step-2: The stored images are called as positives. The positive images are kept as a reference in the database and when any person appears in front of the camera, the camera redirects the captured frames to the positives folder, by creating a template in the form of .xml and this template is compared with the existing faces in the positives folder.

Step-3: If there is a match, with the face of positives then that person face is marked with the black rectangle, but if there is a mismatch the face is marked with white rectangle.

Step-4: If there is match, a video of few minutes will be recorded and this video is redirected to the browser with the help of part-1 implementation of the project.

In case of mismatch, only an image of the person is captured with the face marked with white rectangle and stored in the database.

Note: This comparison is more accurate in black and white image formats and less accurate in colour images because in colour image there are several other parameters which have to be considered like colour depth, distance, line of sight of the camera, clarity of the camera, motion correction etc. Therefore in black and white image formats the complexity of these parameters are also considered but the main concept of the project is to detect the suspicious person and it doesn't depend whether the image is color or not. Once the image is matched, the video recorded for the specified time interval.

Therefore the Haar cascade classifier algorithm can detect the faces in an image or in a picture, but the remaining part of this project like image has to be magnified and only the face part is cropped and should be saved in the positives folder. Another template has to be created to compare with the existing positives and matching process should occur to perform the operations of Step-3 and Step-4, all these are implemented and modified to perform the required operation hence majority of the Haar cascade classifier algorithm is modified and almost a new algorithm is created and implemented in this project. However the basic structure is taken from the Haar cascade classifier algorithm.

VII. SENSOR INTERFACING



Fig 5 Interfacing sensor with microcontroller

This part is about Interfacing Sensors with the microcontroller to detect events or changes by triggering a pulse to indicate an output of the sensor in quantities that is generally as an electrical or optical signal and to check whether the person in front camera is Suspicious person or not. There are 40 GPIO's available in the Raspberry PI B+ microcontroller board and we can connect some sensors as input to act in accordance with the system to detect the suspicious person.

Therefore we have used 3 types of sensors, they are:

- Vibration Sensor.
- Sound Sensor.
- Pyroelectric InfraRed (PIR) motion detection Sensor.

All these sensors are interfaced with the Raspberry PI B+ board and when each sensor is active different operations are performed. The detailed explanation is as follows:

- *Vibration Sensor:* Vibration Sensor which is connected to one of the digital input of the Raspberry PI board is enabled and coded using python as whenever any kind of vibration is sensed the output pulse is triggered and enables the Raspberry PI NoIR camera to capture HD image and store the image in the microcontroller. This image should be redirected to view in the client end browser.
- *Sound Sensor:* Sound Sensor which is also connected to one of the digital input of the Raspberry PI board is coded using the python as whenever any kind of suspicious or high pitch sound occurs, the output pulse is triggered and enables the Raspberry PI NoIR camera to capture HD image and store the image in the microcontroller. This image should be redirected to view in the client end browser.
- *PIR motion detection sensor:* The same thing doesn't apply for motion detection sensor because in case of Vibration sensor and Sound sensor, the vibration and sound can occur from any place need not be in front of the camera but the motion detection sensor is a sensor which detects any kind of movement when some person walks in front of the sensor. This sensor senses any kind of variation in the sensory pad and gives high output pulses to indicate that the sensor is active. This sensor which is connected to the microcontroller receives the high output pulse and it directs the camera module which is placed in adjacent to the sensor to capture an image. If there are any person appears in front of the camera, it captures the image and crops the face of the person and stores the image in template.xml format. This stored image is late on compared with the positive faces which are present in the database. This will take some time because the image captured should compare with all the faces which exist in the database. After series of comparison, if there is any match with the faces in the database then that person is detected as suspicious person and the face is marked with the black rectangle and immediately a video recording happens as mentioned in the algorithm implementation part. If the faces is matched that person is the suspicious person or if there is a mismatch, then that person face is marked with white colour and he is not a suspicious person so only an image of this person is captured for further reference.

The images and video captured can be viewed from the client end browser via online and the required images can be downloaded from the microcontroller end to the client end browser and the original data can be deleted from the database after a backup is taken. The delete option is provided at the browser and any changes done at the browser is effectively implemented and changes takes place at the microcontroller end. In order to make an alert, that there is a suspicious person in front of the camera a Buzzer is used.

The alert happens only if any one of the above conditions is satisfied. The Buzzer is turned off manually or it will turn off after few delay units of time.

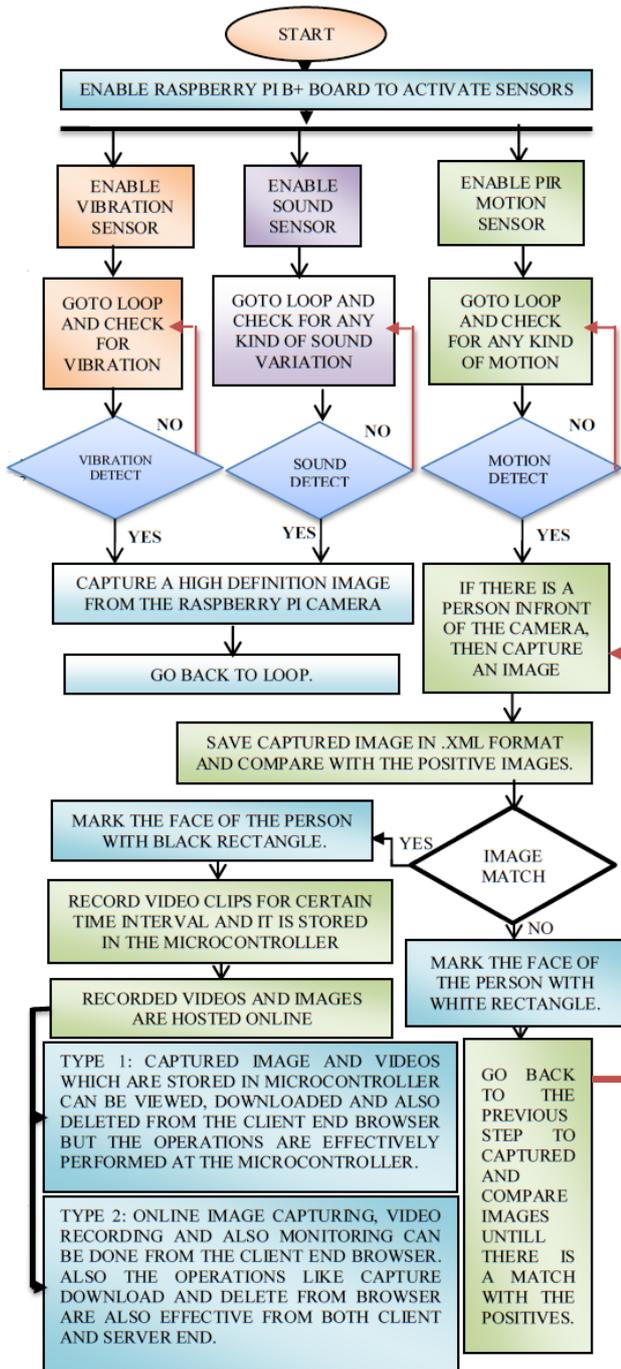


Fig 6 Complete Flow Chart

VIII. EXPERIMENTAL RESULTS



FIG A: CAPTURING SUSPICIOUS POSITIVES

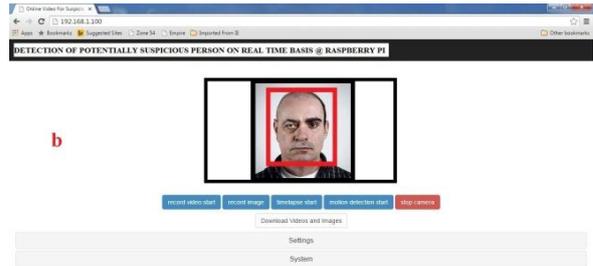


FIG B: POSITIVE MATCH MARKED WITH RED

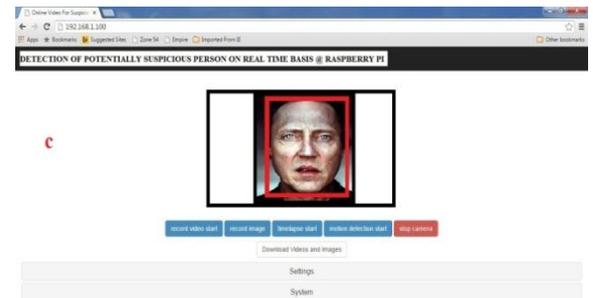


FIG C: POSITIVE MATCH MARKED WITH RED



FIG D: POSITIVE MATCH MARKED WITH RED



FIG E: NEGATIVE MATCH MARKED WITH GREEN

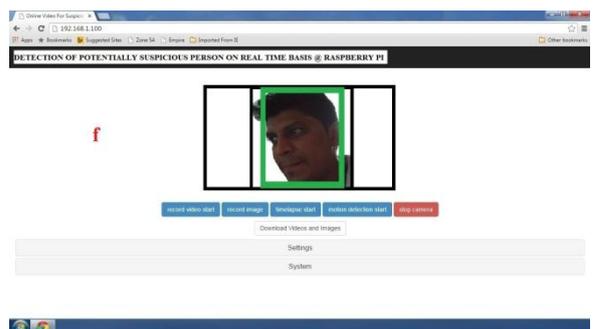


FIG F: NEGATIVE MATCH MARKED WITH GREEN

| RESULT ANALYSIS | FACE DETECTION (if a person is in front of cam) | QUANTITATIVE EVALUATION AND DETECTION. | PRECISION |
|-------------------------|---|---|--|
| Sound Sensor Image. | YES | 100% Successful detection with HD image capturing in color format | 100% |
| Vibration Sensor Image. | YES | 100% Successful detection with HD image capturing in color format | 100% |
| PIR Motion Sensor. | YES | 100% Successful detection with image capturing, comparing and if there is a positive match, a video is recorded | 100% for detection and 97% accuracy in face matching because it depends on motion. |
| Minimum distance | YES | 100% Successful detection with minimum distance of 2 feet | 100% for detection and 95% accuracy in face matching because it depends on motion. |
| Best Result | YES | 100% Successful detection with distance between 3 to 4 feet | 100% for detection and 98% accuracy in face matching because it depends on motion. |
| Maximum distance | YES | 100% Successful detection with maximum distance of 10 feet in lab environment | 100% for detection and 75% accuracy in face matching because it depends on motion. |

TABLE 1: RESULTS ON EXPERIMENTAL BASIS

IX. CONCLUSION

In this project, a person who is identified as suspicious is detected automatically by referring the images present in the microcontroller database. This is done by comparing the face of the person in front of the camera with the existing face images in the database. The matching concept is called as confidence level matching. This value can be varied by accessing the microcontroller. If there is a match in the face, then a video of certain time interval is captured and stored in the microcontroller. This video of suspicious person can be downloaded online using a specified web address. However if there is any kind of suspicious sound or any kind of suspicious vibrations there will be sound sensor and vibration sensor interfaced with the microcontroller to capture a high definition image from the camera, which acts as a safety feature if the suspicious person is aware of the camera and tries to disturb or make contact with the camera module. Even this image can be downloaded online and the suspicious person can be identified.

REFERENCES

- [1] Raj Kumar Tiwari and Santosh Kumar Agrahari, *Arduino "Compatible World Wide Web Controlled Embedded System,"* IJEIT VOL 3, Issue 9, March 2014.
- [2] Electronics Corporation of India Limited "Automated Real-Time Detection of Potentially Suspicious Behaviour in Public Transport Areas," A Govt. of India (Dept. of Atomic Energy) Enterprise 2013.
- [3] EL Maadi Amar and DJOUADI Mohand, "Suspicious Motion Patterns Detection and Tracking In Crowded Scenes" in IEEE 2013.
- [4] Mohannad Elhamod and Martin.D.Levine, "Automated Real-Time Detection of Potentially Suspicious Behaviour in Public Transport Area" IEEE Transactions on Intelligent Transportation Systems, VOL. 14, NO. 2, JUNE 2014.
- [5] Miwa Takai, "Detection of Suspicious Activity and Estimate of Risk from Human Behaviour shot by Surveillance Camera", Second

World Congress on Nature and Biologically Inspired Computing Dec-2010

- [6] Li Yingjie and Yin Yixin, "Towards suspicious behaviour discovery in video surveillance system", Second International Workshop on Knowledge Discovery and Data Mining, 2009.
- [7] D.Arsic and B.Hornler, "A Hierarchical Approach for Visual Suspicious Behavior Detection in Aircrafts", Institute for Human Machine Communication, Germany, IEEE 2009
- [8] Peter Buck and Svenja Leifert, "Integrative Visual Analytics for Suspicious Behaviour Detection", IEEE Symposium on Visual Analytics Science and Technology, October 2009.
- [9] Arnold Wiliem and Prasad Yarlagadda, "A Context-Based Approach for Detecting Suspicious Behaviours", Digital Image Computing: Techniques and Applications, 2009
- [10] Daniel Barbera and Zoran Durich, "Detecting Suspicious Behaviour in Surveillance Images" IEEE International Conference on Data Mining Workshops, 2008
- [11] Yasuyuki and Eri sato, "Suspicious Behaviour Detection based on Case-Based Reasoning using Face Direction", International Joint Conference, 2006
- [12] Sander Soo, "Object detection using Haar-cascade Classifier", Institute of Computer Science, University of Tartu, 2014
- [13] Mustafa E. Yildirim, J. S. Park, J. Song, and B. W. Yoon "Gender Classification Based on Binary Haar Cascade", International Journal of Computer and Communication Engineering, Vol. 3, No. 2, March 2014
- [14] Ms. Jaya M. Jadhav, Ms. Deipali V. Gore "Introducing Celebrities in an Images Using HAAR Cascade Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 8, August 2013.
- [15] Xiaofei He, Shuicheng Yan, Yuxiao Hu, Partha Niyogi, Hong-Jiang Zhang "Extracting facial features using laplacian face based on the paper face recognition using laplacian face", IEEE Transactions on Pattern Analysis and Machine Intelligence (Pami), Vol. 25 No. 3 March 2005.
- [16] Paul Viola and Michael Jones "Rapid Object Detection using a Boosted Cascade of Simple Features" by Accepted Conference On Computer Vision And Pattern Recognition, 2001
- [17] Stewart Weiss "Introduction to System Programming": referred by a Text book. and Referred a website on "Programming the Raspberry Pi"
- [18] O'Reilly, "Getting Started with Raspberry Pi" by Matt Richardson and Shawn Wallace Published., 1005 Gravenstein Highway North, Sebastopol, CA 95472. 2013
- [19] Robert Love, "Linux System Programming", Published by O'Reilly Media, Inc. copyright 2007.
- [20] Daniel Leles Baggio, "Mastering OpenCV with Practical Computer Vision Projects" And Dr. Andrew N. Harrington, "Hands-On Python A Tutorial Introduction for Beginners Python 3.1 Version".

BIOGRAPHIES



Mr. SAI PRABHU K.B. Master of Technology [M.Tech] in VLSI Design and Embedded Systems from NITE MEENAKSHI INSTITUTE OF TECHNOLOGY, Bengaluru under Visvesvaraya Technological University and

Bachelor of Engineering [B.E] in Electronics and Communication from Visvesvaraya Technological University. Has also worked in the IT industry for 1 year from 2011-2012. His research interest includes microprocessor, microcontroller & embedded system design.

Mrs. SEEMA SREEKUMAR received Master of Technology [M.Tech] in VLSI Design and Embedded Systems from Visvesvaraya Technological University and currently working as Assistant Professor, Department of Electronics & communication Engineering, NITTE MEENAKSHI INSTITUTE OF TECHNOLOGY, Bengaluru INDIA. She has 9 years of experience in teaching for UG & PG courses. Her research interest includes microprocessor, microcontroller & embedded system design.