International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 3 | Mar-Apr 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

A Modern Technique for Unauthorized Human Detection and Intimation

Keerthanna G. S[1], Praveen Kumar P[1], Vishnu Prasad K[1], Ms. S. Sri Heera[2]

[1]Student, [2]Assistant Professor

[1,2]Department of Computer Science and Engineering, Easwari Engineering College, Chennai, Tamil Nadu, India

How to cite this paper: Keerthanna G. S | Praveen Kumar P | Vishnu Prasad K | Ms. S. Sri Heera "A Modern Technique for Unauthorized Human Detection and Intimation" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-3, April 2019, pp.170-174, URL: http://www.ijtsrd.com/papers/ijtsrd21659.pdf

IJTSRD21659

ABSTRACT

Technological advancements are inevitable and the field of IoT is no exception. The utilization of the technologies in various sectors is highly employed. Even though we use technology in various sectors, the employment of technology for security purposes is very low. The Existing security in various places only CCTV is used for monitoring and recording. Even there are existing security systems where an alert is sent via an email which requires a stable internet connection. It is unlikely that we expect the user to be always connected to an internet source. In the Proposed system, authorized user's faces will be trained and stored in a Database. Initially, when an unknown/known person enters in the zone the camera module will capture the intruder's face. The captured intruder's face will be compared with the trained faces in the database. If the person's face doesn't match, the micro controller will send an alert SMS to the recognized user and also the intruder's captured image will be E-mailed to the user. The authorized user should acknowledge the SMS message. If he fails to acknowledge the message within a threshold time limit, an alert call will be made to the concerned user. By this the user gets intimated in real time.

KEYWORDS: *Face recognition, Image Processing, IoT, Security system*

1. INTRODUCTION

It is known that the technological advancement in these days is developing at a faster pace. The utilization of the technologies in various sectors is highly employed. Even though we use technology in various sector, the employment of technology for security purposes are becoming very low. Security is said to be one of the most important sections in everyone's lives. Home security is one of the major issues in our society. In today' scenario, CCTV cameras are used for monitoring and providing security. CCTV is used for recording the video. It does not help in alerting the user. An External Security should be kept for viewing and monitoring the CCTV footages. This is a Very Difficult thing to do. Even the CCTV camera scan be easily hacked or the footages stored in memory can be erased easily. The proposed a system which captures an image of human when detected and sends it to the concerned user. This enhances security as well as it helps to view contents remotely.

In recent years, there has been a growing interest among consumers in the smart home concept. Smart homes contain multiple, connected devices such as home entertainment consoles, security systems, lighting, access control systems and surveillance. Intelligent home automation system is incorporated into smart homes to provide comfort, convenience, and security to home owners. Home automation system represents and reports the status of the connected devices in an intuitive, user-friendly interface allowing the user to interact and control various devices with the touch of a few buttons. Some of the major communication technologies used by today's home automation system include Bluetooth, WiMAX and Wireless LAN (Wi-Fi), Zigbee, and Global System for Mobile Communication (GSM). Another advantage of using the GSM network in home automation is its high security infrastructure, which provides maximum reliability whereby other people cannot monitor the information sent or received. Hence, this research work implements SMS based control for home appliances using the GSM architecture without accessing the local network.

1.1. MICROCONTROLLER

A microcontroller differs from a microprocessor, which is a general-purpose chip that is used to create a multi-function computer or device and requires multiple chips to handle various tasks. A microcontroller is meant to be more self-contained and independent, and functions as a tiny, dedicated computer.They are typically designed using CMOS (complementary metal oxide semiconductor) technology, an efficient fabrication technique that uses less power and is more immune to power spikes than other techniques. There

are also multiple architectures A microcontroller is an integrated chip that is often part of an embedded system. The microcontroller includes a CPU, RAM, ROM, I/O ports, and timers like a standard computer, but because they are designed to execute only a single specific task to control a single system, they are much smaller and simplified so that they can include used, but the predominant architecture is CISC (Complex Instruction Set Computer), which allows the microcontroller to contain multiple control instructions that can be executed with a single macro instruction. Some use a RISC (Reduced Instruction Set Computer) architecture, which implements fewer instructions, but delivers greater simplicity and lower power consumption.

1.2. GSM MODEM

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves. The working of GSM modem is based on commands, the commands always start with AT (which means ATention) and finish with a <CR> character. For example, the dialing command is ATD<number>; ATD3314629080; here the dialing command ends with semicolon.

The AT commands are given to the GSM modem with the help of PC or controller. The GSM modem is serially interfaced with the controller with the help of MAX 232. Here max 232 acts as driver which converts TTL levels to the RS 232 levels. For serial interface GSM modem requires the signal based on RS 232 levels. The T1_OUT and R1_IN pin of MAX 232 is connected to the TX and RX pin of GSM modem.

1.3. MATLAB

MATLAB® is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar noninteractive language such as C or FORTRAN.MATLAB features a family of application-specific solutions called toolboxes. Very important to most users of MATLAB, toolboxes allow you to learn and apply specialized technology. Toolboxes are comprehensive collections of MATLAB functions (M-files) that extend the MATLAB environment to solve particular classes of problems.

1.4. ALGORITHM

Local Binary Pattern (LBP) is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number.It was first described in 1994 (LBP) and has since been found to be a powerful feature for texture classification as shown in Fig 1.4. It has further been determined that when LBP is combined with histograms of oriented gradients (HOG) descriptor, it improves the detection performance considerably on some datasets.The four parameters used are listed below

- **Radius**: the radius is used to build the circular local binary pattern and represents the radius around the central pixel. It is usually set to 1.
- **Neighbors**: the number of sample points to build the circular local binary pattern. Keep in mind: the more sample points you include, the higher the computational cost. It is usually set to 8.
- **Grid X**: the number of cells in the horizontal direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.
- **Grid Y**: the number of cells in the vertical direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.

The algorithm is trained by using a dataset with the facial images of the people wanted to be recognized.An ID (it may be a number or the name of the person) is set for each image, so the algorithm will use this information to recognize an input image and give you an output. Images of the same person must have the same ID.

The first computational step of the LBPH is to create an intermediate image that describes the original image in a better way, by highlighting the facial characteristics. To do so, the algorithm uses a concept of a sliding window, based on the parameters **radius** and **neighbors**. Each histogram created is used to represent each image from the training dataset. So, given an input image, we perform the steps again for this new image and creates a histogram which represents the image as shown in Fig 1.4.1. So to find the image that matches the input image we just need to compare two histograms and return the image with the closest histogram.

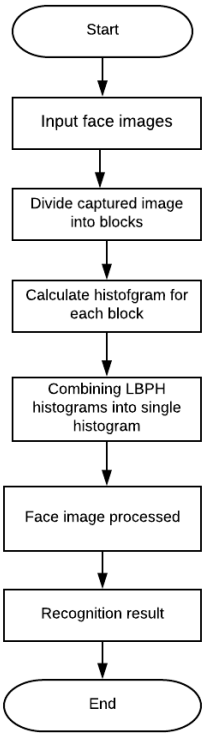


Fig1.4.1 Flowchart

2. RELATED WORK

IIhan Aydin and Nashwan Adnan Othman developed a security system that enables a camera to detect faces, capture it and sends the images to Smartphone via telegram application. Whenever a movement is detected, the camera is used to capture the face of the person. The captured face will be forwarded to the user's mobile phone via an application. Limitation of this system is

there is no face recognition. The camera captures everything when it detects a movement.

Dwi Ana Ratna Vati and Dika Abadianto designed a Smart home security application where the face detection is based on Template matching and face recognition is based on the Principle Component Analysis. Template matching is a technique in digital image processing for finding small parts of an image which match a template image. It can be used in manufacturing as a part of quality control, a way to navigate a mobile robot, or as a way to detect edges in images. Limitations of this design are that the face recognition has only 80% Accuracy only.

Teddy Surya Gunawan, F.D.A Rahman, Mira Kartiwa and M.H.H Gani developed a smart home system where Eigen face is used for Feature Extraction and Principle Component Analysis was used as a Classifier. The output of face recognition algorithm is then connected to the relay circuit, in which it will lock or unlock the magnetic lock placed at the door. Limitations include recognition accuracy being 90% and it also does not send any notification. Only the door can be Locked and Unlocked.

Sandesh Kulkarni, Minakshee Bagul, Akansha Dukare, Archana Gaikwad developed a Security system where the face detection is done with Voila jones face detector and LWF for face recognition. The Viola-Jones algorithm is a widely used mechanism for object detection. The main property of this algorithm is that training is slow, but detection is fast. This algorithm uses Haar basis feature filters, so it does not use multiplications. The system authenticates the face and unlocks the door if the face is an authorized one else the door remains firmly locked. Limitations are that there is no real time update for the user.

Sudeep Tanwar and Sudhanshu Tyagi developed a smart home system that uses Fire and Gas sensors. A buzzer is activated when a fire breaks out or the exhaust fan is turned on if there is gas leakage. There are a number of sensors used that helps in detecting fire and gas leaks. After the sensor figures there is Limitation of this system is it uses cheap sensors for detecting a fire and gas there is no proper real time update to the authorized user.

Ayman Ben Thabet and Nidhal Ben Amor Developed a home security system where Raspberry pi is used along with OpenCV library includes PCA algorithm for face recognition. If a person is not a authorized one, then the Alarm bell starts to ring. Initially, the person's face will be captured manually and fed as input to the OpenCV. PCA algorithm is used for recognizing the image and if the images don't match, then an alert is made to the authorized user. Limitations of this system are the alarm keeps ringing causing nuisance and disturbance to the neighboring houses.

Nashwan Adnan Othman and Ilhan Aydin developed a real time recognition system where PIR sensor is used for detection with a camera capturing the image and Raspberry pi sends an email containing the image. The PIR sensor is used for detecting an intruder. Whenever there is motion the PIR sensor triggers the camera. The camera captures the intruder's face and it will be sent as a mail to the authorized used using raspberry pi. Limitations involve there is no face identification process. Captured image will be simply notified to the user.

3. PROPOSED MODEL

The system generally detects for human presence in an area. Based on the presence of human, then the image is captured and an alert is provided. This causes a drawback when a recognized person enters an area. This causes an alert. And also buzzer is intimated only for people present in the surrounding. This causes major drawback.

Figure 3.1 shows the architecture of the proposed system.The system trains a set of person's images who are allowed to enter the room. So here a camera is used in-order to capture the person. The image taken is provided to the MATLAB section for image processing. Local Binary Pattern algorithm for processing the images. The trained images will be stored in the database. When the person fall into the zone then the camera detects him and captures his face. After capturing, the image will be compared for recognition with the images in the database. The image processing identifies the person whether the person is recognized or not. If a person's images are un-identified, the system notifys the user by providing an alert message (SMS) through GSM module and send that image as a mail to the concerned user. If he/she fails to respond to that SMS within a threshold time, then a Call will be sent to the Authorized User.

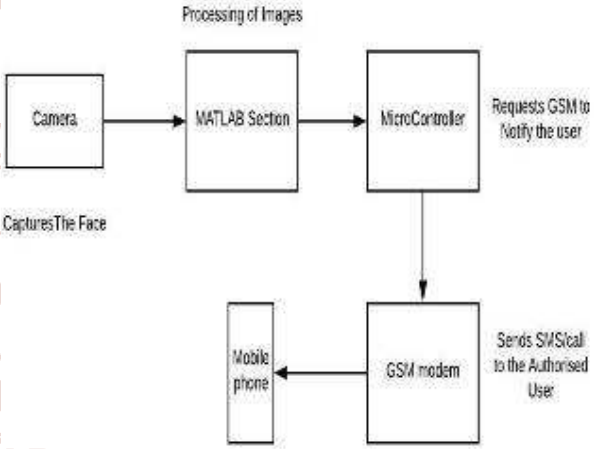


Figure 3.1 System Architecture

4. MODULAR DESIGN

The Proposed system consists of the following modules.

1. Training the Images.
2. Recognition of Authorized User
3. Intimation about Intrusion

4.1. Training the Images

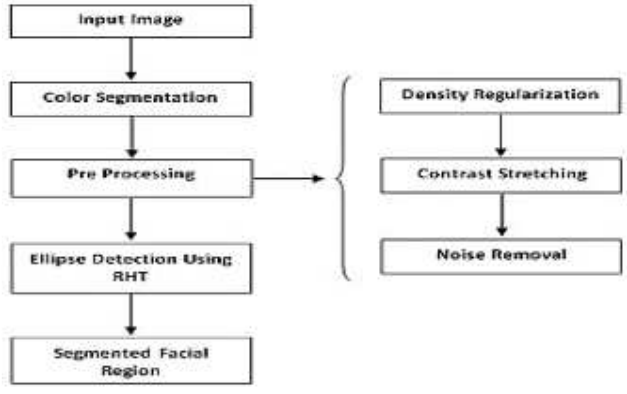


Fig 4.1 Training the Images

The System is trained with various heterogeneous images. This is done with the help of Camera and MATLAB section. It can be seen in the figure 4.1. After the images are captured, they are preprocessed, segmented and their features are extracted and stored within the database.

4.2. Recognition of Authorized User

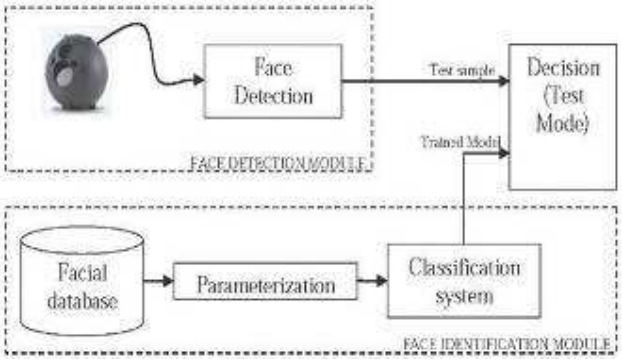


Fig 4.2 Recognition of Authorized user

When an intruder falls into the zone, he will be detected by the camera and his face will be captured. The Image is then processed and they are then compared with the set of trained images in the database as shown in the Fig 4.2.

4.3. Intimation about Intrusion

In the module, if the detected face is not a recognized one, then an SMS will be sent through the GSM model to the Authorized users Mobile. If the User fails to acknowledge the message within the given threshold time, then a Call will be made to the user using the GSM modem as seen in the flowchart Figure 4.3.

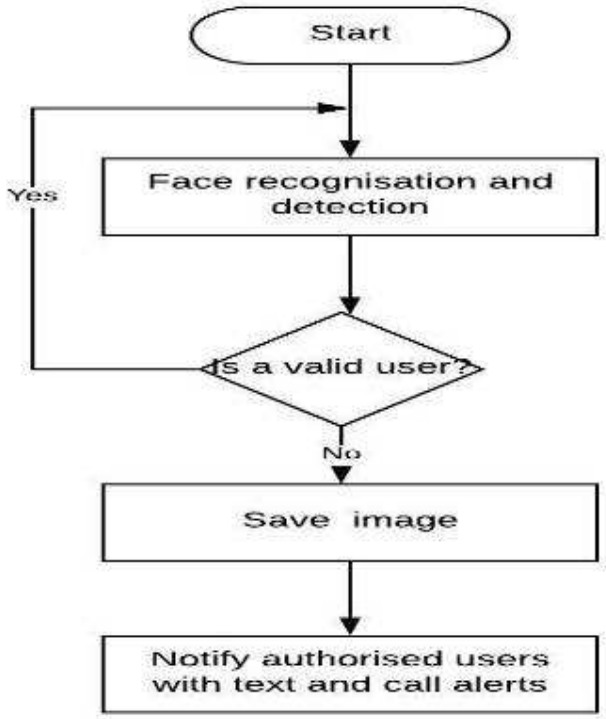


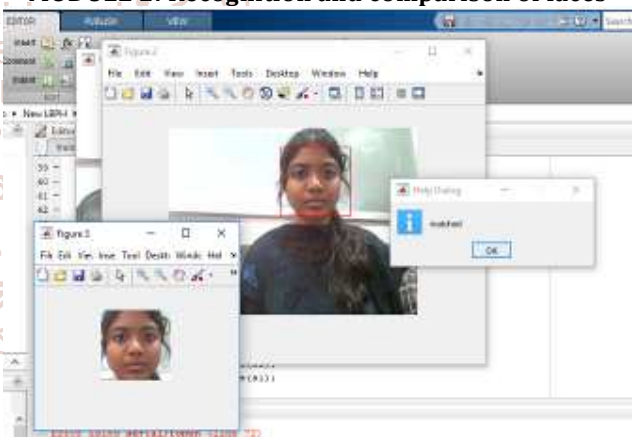
Figure4.3 Intimation about Intrusion

5. RESULT

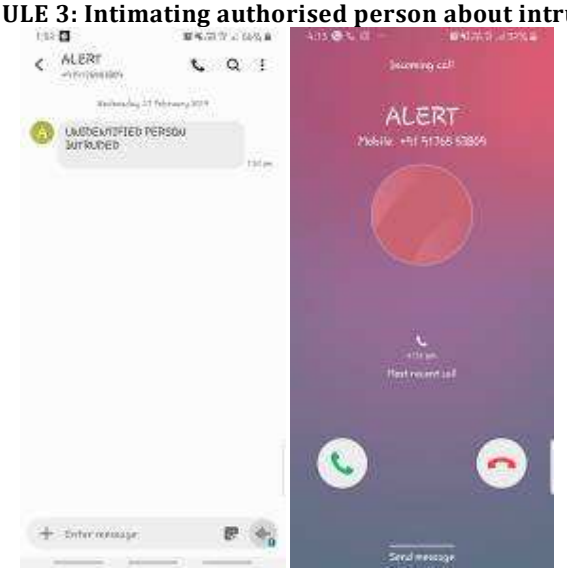
The security system is implemented using a Arduino Uno Micro-controller integrated with GSM module to send intimations about intrusion. The authorized user's faces will be trained using LPBH algorithm and gets stored in a Database. The Image that has been captured is processed and stored in Binary form within the database. When a unknown/known person enters in the zone, it captures the face. Then it compares the detected face with correlation values stored in database. When the values don't get matched with the trained faces in the database then an unmatched value set will be sent to the micro-controller which in turn sends alert texts and call to authorized person with the help of GSM modem. This is very much helpful to alert the surrounding.

MODULE1: Training the authorized user faces

MODULE 2: Recognition and comparison of faces



MODULE 3: Intimating authorised person about intrusion



6. CONCLUSION AND FUTURE WORKS

The proposed system presented an improved technique for identifying an intruder and intimating to an authorized user. The system is trained with all the authorized user's faces. The more the system is trained, the better the recognition algorithm works. The images will be trained under various environments, light effects, et cetera. Now, whenever an intruder enters into the boundary zone of the camera, his/her face will be captured and compared with the trained datasets stored in the database. The algorithm after comparison will return a value that will be fed to the microcontroller which in-turn intimates the authorized user about the intrusion. Future implementation of the system is to propose a more effective algorithm that can be implemented for face recognition to help identify the intruder and intimating to the appropriate user.

7. REFERENCES

[1] A. S. Mian, M. Bennamoun, and R. Owens, "Keypoint detection and Local feature matching for textured 3D face recognition," International Journal of Computer Vision, Vol. 79, No. 1, PP. 1–12, 2008.

[2] Alicej.O'Toole, Xiaoboan, Josephdunlop and Vaidehinatu,"Comparing Face Recognition Algorithms to Humans on Challenging Tasks" ACM Transactions on Applied Perceptions,Comput 10,4,Article 11,2016.

[3] A. S. Mian, M. Bennamoun, and R. Owens, "Keypoint detection and Local feature matching for textured 3D face recognition," International Journal of Computer Vision, Vol. 79, No. 1, PP. 1–12, 2008.

[4] D. Smeets, J. Keustermans, D. Vandermeulen, and P. Suetens, "Meshsift: Local surface features for 3D face recognition under expression variations and partial data," Computer Vision and Image Understanding, Vol. 117, No. 2, PP. 158–169, 2013.

[5] H. Li, D. Huang, J.-M. Morvan, L. Chen, and Y. Wang, "Expressionrobust 3D face recognition via weighted sparse representation of multiscale and multi-component local normal patterns," Neurocomputing, Vol. 133, PP. 179–193, 2014.

[6] H. Zhou, A. Mian, L. Wei, D. Creighton, M. Hossny, and S. Nahavandi, "Recent advances on singlemodal and multimodal face recognition: a survey," IEEE Transactions on Human-Machine Systems, Vol. 44, No. 6, PP. 701–716, 2014.

[7] H. Mohammad zade and D. Hatzinakos, "Iterative closest normal point for 3D face recognition," IEEE transactions on pattern analysis and machine intelligence, Vol. 35, No. 2, PP. 381–397, 2013.

[8] Jenifer Marlow, Jason Wise, "Surveying User Reactions to Recommendations Based on Inferences Made by Face Detection Technology", ACM Journals on Intelligent System, 2017.

[9] M. Emambakhsh and A. Evans, "Nasal patches and curves for expression-robust 3D face recognition," IEEE transactions on pattern analysis and machine intelligence, Vol. 39, No. 5, PP. 995–1007, 2017.

[10] S. Berretti, A. Del Bimbo, and P. Pala, "Sparse matching of salient facial curves for recognition of 3-D faces with missing parts," IEEE Transactions on information forensics and security, Vol. 8, No. 2, PP. 374–389, 2013.

[11] S. Soltanpour, B. Boufama, and Q. J. Wu, "A survey of local feature methods for 3D face recognition," Pattern Recognition, Vol. 72, PP. 391– 406, 2017.

[12] T. Russ, C. Boehnen, and T. Peters, "3D face recognition using 3D alignment for PCA," in IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Vol. 2, PP. 1391–1398,2006.

[13] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," ACM computing surveys (CSUR), Vol. 35, No. 4, PP. 399–458, 2003.

[14] X. Li, T. Jia, and H. Zhang, "Expression-insensitive 3D face recognition using sparse representation," in IEEE Conference on Computer Vision and Pattern Recognition (CVPR), PP. 2575–2582,2009.

[15] Xing chen, Yenan Lu, Ran Fang "3D Face Recognition Based on Empirical Mode Decomposition and Sparse Representation", ACM Journal on Image Processing, 2016.

[16] Y. Lei, Y. Guo, M. Hayat, M. Bennamoun, and X. Zhou, "A two-phase weighted collaborative representation for 3D partial face recognition with single sample," Pattern Recognition, Vol. 52, No.4 PP. 218–237, 2016.