

Face Recognition Based Digital Door Lock Security System

Najaf Haider, Kundan Singh, Ankit Kumar, M.S.Bennet Praba

Student, CSE, SRMIST, Tamilnadu, India

Student, CSE, SRMIST, Tamilnadu, India

Student, CSE, SRMIST, Tamilnadu, India

Assistance professor, CSE, SRMIST, Tamilnadu, India

ABSTRACT

There are many type of digital door lock security system just like keypad lock, bluetooth based model, pir motion sensor etc. Now the technology is improved and these type of locks are outdated. As robbery or burgalary took place very oftenly. To make more secure to our properties and the things which we have. The system should be more advanced and more attentive towards the technology. To make the home more secure we are going to implement face recognition digital door security system. And it will be accessed only by the authorised person and these technology is more secure than other one. And the video surveillance will be there within these technology and the footage of unauthorised person will be directly transmitted to the local cops.

KEYWORD:RFID,PIR SENSOR, MICROCONTROLLER, DOORLOCK, ALARM,MOTOR

1. INTRODUCTION

In 2011 the study report by National Crime Records Bureau (NCRB) [1], 58862 burglary cases was registered in India. According to the study by Alarm Industry Research and Educational Foundation (AIREF) [7], thief spends less than 60 seconds for breaking the normal door lock. The report of "Home Safety Fast Facts" conducted by the Electronic Security Association's (ESA) [6] concludes that 9 out of 10 burglars avoid homes which are having door alarm security system. These facts have encouraged the development of numerous security systems for both residential and commercial applications. Today it is essential to provide the security system employing various sensors and alarm system in residential communities. Mallory Jone [5] implemented a security alarm system that has a number of sensors for smoke, fire, intrusion and application operation. A central monitoring system was provided for continues indication of sensors. Transmitters were connected with sensors and receivers were connected with monitoring system for effective communication.

The central monitor then display the indication with respect to each transmitter connected with particular sensor. Pratiksha [3], described a home security system with the GSM/GPRD technology services to achieve controlling of door lock by short message service (SMS). Also Adnan Ibrahim discussed the design and development of PIC supported security system with the GSM system for sending the alert message on mobile for continues three unsuccessful attempts of password [2]. Another system was proposed by Ushie [4], in which door can be remotely controlled by a GSM phone set like a transmitter and another GSM phone set with a dual tone multi frequency (DTMF) connected to the door motor with DTMF decoder interfaced with microcontroller chip.

2.EXISTING SYSTEM-

Existing system is not very adequate related to current technology. It doesn't provides full safety to the user as it doesn't detects small fast movable objects. It's not economically sound. PIR works only in certain range of temperature. GSM module doesn't gives proper result in case local server is down.

2.1. PIR:

The present framework manages PIR framework. PIR remains for aloof infrared radiation sensor for discovery of essence of any impediments display in its way. It can distinguish its way just upto a couple of range. Hence the as of now framework needs greater improvement for its more extensive utilize. It is likewise temperature subordinate subsequently it works just for a couple of scope of temperature. Its not relevant neither for significantly higher nor much lower temperature i.e its is temperature touchy. PIR sensor works just in LOS locale. LOS remains for viewable pathway. It doesn't work past LOS. Clients need to choose painstakingly in the event that they wish to be checked 24 hours per day by a PC framework. Numerous won't feel good being in this circumstance, as there is by all accounts a great deal of doubt of innovation - particularly among more seasoned individuals.

A Sensor Network may require a considerable measure of extra wiring to be introduced around the house to enable sensors to work - unless the sensors utilized are remote. Utilizing remote makes sensor gadgets substantially more costly. Retrofitting a current home as opposed to another form could cause a considerable measure of change for the time of the establishment..

2.2 RFID:

RFID turns out to be excessively costly for some applications when contrasted with other following and distinguishing proof techniques, for example, the straightforward scanner tag.

It is troublesome for a RFID peruser to peruse the data in the event that the labels are introduced in fluid or metal items. The issue here is that, fluid and metal surfaces have a tendency to reflect radio waves, which makes the labels confused. In such applications, they must be set in different arrangements and plots for taking appropriate readings, which might be excessively unwieldy and tedious.

Obstruction has been seen to occur in RFID frameworks, when gadgets, for example, forklifts and walkies-talkies are in the region. The nearness of cell phone towers too has been found to meddle with these radio waves. The retail part goliath Walmart, which has introduced billions of RFID labels in their items all through the world, have announced such issues in their frameworks.

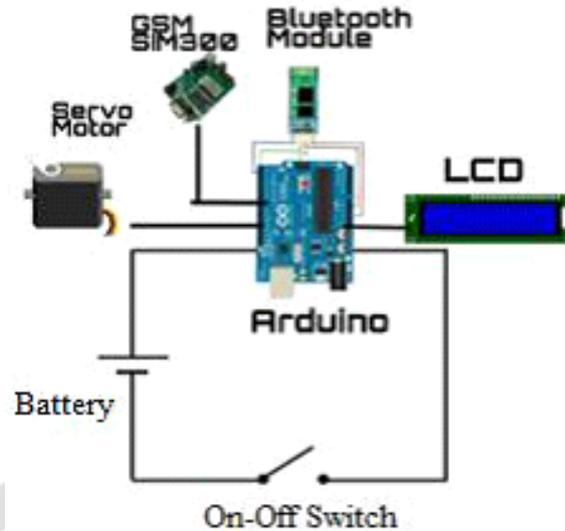
RFID flag frequencies over the world are non institutionalized. For example, the US and Europe have an alternate scope of frequencies at which RFID labels work. This makes it compulsory for universal delivery organizations and different associations to know about the working example in different countries.

RFID is considered by numerous to be an obtrusive innovation. Customers tend to stress over their security when they buy items with these labels, as there is a conviction that once radio chips are introduced in an item, it keeps on following a man, and his own data can be gathered by it and transmitted to the peruser. So while numerous stores guarantee that they deactivate the labels after the item has been bought, purchasers still keep on remaining uneasy of this innovation.

2.3 Blue tooth:

It is a mind boggling chip which utilizes an outer 8 bit streak memory. It is a little module Bluetooth module is utilized for remote transmission. Its range is 10 meters. This module depends on Cambridge which deals with less power that is 3.3V. It has transmitter (Tx) and recipient (Rx) pins which are utilized for the transmission of information. The Tx of the module is associated with the Rx of the Arduino and Rx of the module is associated with the Tx of arduino. The advanced mobile phone bluetooth application is utilized to bolt/open the entryway secure bluetooth module, which has a scope of around 10m. Bluetooth HC-05 gadget is associated with the arduino pack. To open and close the entryway bolt first we set up association between advanced mobile phone bluetooth with arduino controller bluetooth gadget. As the association has been done between these two bluetooth gadgets LCD demonstrate

that association is finished. At that point we enter the secret word from our advanced mobile phone to open or close

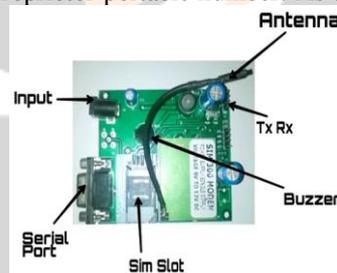


the entryway bolt.

ig 2.2

2.4 GSM module:

It is most secured and most appropriate module in every one of the three modules. In which we can open and shut the entryway bolt utilizing GSM portable SMS. We can store the proprietor various GSM numbers in the arduino program. The proprietor sends the instant message from the GSM versatile to the GSM pack associated with the arduino controller, at that point the ar-duino controller give the charge to servo engine to open or close the entryway bolt according to the secret key given. On the off chance that the secret word recognized from obscure number for three back to back endeavors, at that point the arduino controller begins the ringer and furthermore send a notice message of false passage at the way to the proprietor portable number. As this sys-tem work with the GSM organize



the proprietor can send or get the back rub aa

fig 2.1

3.RELATED TECHNOLOGY:

According to our overview as of now there exists framework neither at less expensive rates nor simple to deal with. Different frameworks are difficult to introduce, hard to utilize and keep up. Current frameworks are for the most part exclusive, shut and not extremely easy to use. In view of Arduino or GSM or minimal effort home security framework and home mechanization framework we talk about some framework in detail as underneath:

3.1 PIR Communication module

PIR stands for passive infrared radiation. It Works on the principle of radiation emission. Through this radiation any obstacles in its path can be detected and hence indicates any danger. It is temperature sensitive. It works only in few range of temperature. It doesn't works properly in fluctuating temperature. It has limited Line of Sight(LOC). It ranges only upto few metres. It doesn't detects small things properly which comes in its path.

3.2 GSM based Control system:-

The extensive capabilities of this system are what make it so interesting. From the convenience of a simple phone, a user is able to control and monitor virtually any electrical device. This makes it possible for users to rest assured that their belongings are secure and that an electrical appliance was not left running when they left the house.

3.3 RFID

RFID stands for radio frequency identification. It emits radio frequency wavelength which detects any unauthorised activity in its path. It has two modes one stores the data and other sends the data to RFID reader. They are categorised into two types active tag and passive tag. Active tag doesn't require any power from the reader. Active tag have longer range than passive tag. It is basically a chip that's integrated in our everyday's daily use item. It is used to identify its server through its chip. Though it is encrypted but then also it's not a great deal for a hacker to hack it and store its personal information. It helps to identify the product remotely. It helps the businessman to track and manage their stock level. Educative environments such as public and private academic institutions are established with latest information communication technology (ICT) which includes RFID based devices. Innovation of academic infrastructure using latest ICT with maximum security is a future development in most of academic applications. Regarding the RFID based devices involved in educative environments; the level of security must be reconsidered in some applications. For instance different applications such as library, car park, laboratory etc. need different levels of security. However, there is a security problem, which is a practical challenge considered between the RFID reader and RFID tags. If more than one RFID card or tag is held by the user, more than one user is registered by the reader at the fixed time intervals. It means that monitoring of students' attendance is recorded wrongly and students who are physically absent may be involved in the serious criminal activities. In order to avoid this problem, security of RFID based devices in educative environments is a potential challenge. In this paper, a theoretical model of RFID based device with security protocol is considered to employ in educative environments. Possible security analysis expected to use in educative environments are mentioned as research methods because RFID devices in latest ICT need reasonable security which must be low-cost.

4. PROPOSED SYSTEM:

Our system is far better than the existing system and it is user friendly. And it doesn't depend upon the local network as in GSM module. It is more sensible and it has large range to recognize the authorised person. Unauthorised person cannot access it. It works on face recognition which is very user friendly and more secure. It has large range of LOC (line of control). Whenever it is interrupted or accessed by unauthorised person, the video footage will be directly transmitted to the local cops. For making this system, successful we are using local binary pattern histogram. For face recognition to process the image of authorised person in whole procedure. In whole process first it recognises the face photo and match with the internal photo which is initially

Although it sounds like a very simple task for us, it has proven to be a complex task for a computer, as it has many variables that can impair the accuracy of the methods, for example: illumination variation, low resolution, occlusion, amongst other.

In computer science, face recognition is basically the task of recognizing a person based on its facial image. It has become very popular in the last two decades, mainly because of the new methods developed and the high quality of the current videos/cameras.

Face recognition is different of **face detection**:

- **Face Detection:** it has the objective of finding the faces (location and size) in an image and probably extract them to be used by the face recognition algorithm.
- **Face Recognition:** with the facial images already extracted, cropped, resized and usually converted to grayscale, the face recognition algorithm is responsible for finding characteristics which best describe the image.

The face recognition systems can operate basically in two modes:

- **Verification or authentication of a facial image:** it basically compares the input facial image with the facial image related to the user which is requiring the authentication. It is basically a 1x1 comparison.
- **Identification or facial recognition:** it basically compares the input facial image with all facial images from a dataset with the aim to find the user that matches that face. It is basically a 1xN comparison.

4.1 Local Binary Patterns Histograms (LBPH)

As it is one of the easier face recognition algorithms I think everyone can understand it without major difficulties.

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. 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.

Using the LBP combined with histograms we can represent the face images with a simple data vector.

As LBP is a visual descriptor it can also be used for face recognition tasks, as can be seen in the following step-by-step explanation.

1. **Parameters:** the LBPH uses 4 parameters:

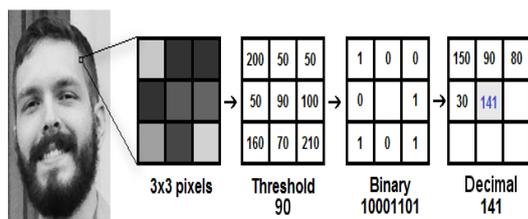
- **Radius:** the radius is used to build the circular local binary pattern and represents the radius around the central pixel. It is usually set to 1.
- **Neighbors:** the number of sample points to build the circular local binary pattern. Keep in mind: the more sample points you include, the higher 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.

Don't worry about the parameters right now, you will understand them after reading the next steps.

2. Training the Algorithm: First, we need to train the algorithm. To do so, we need to use a dataset with the facial images of the people we want to recognize. We need to also set an ID (it may be a number or the name of the person) 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. With the training set already constructed, let's see the LBPH computational steps.

3. Applying the LBP operation: 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**.

The image below shows this procedure:



Based on the image above, let's break it into several small steps so we can understand it easily:

- Suppose we have a facial image in grayscale.
- We can get part of this image as a window of 3x3 pixels.
- It can also be represented as a 3x3 matrix containing the intensity of each pixel (0~255).
- Then, we need to take the central value of the matrix to be used as the threshold.
- This value will be used to define the new values from the 8 neighbors.
- For each neighbor of the central value (threshold), we set a new binary value. We set 1 for values equal or higher than the threshold and 0 for values lower than the threshold.
- Now, the matrix will contain only binary values (ignoring the central value). We need to concatenate each binary value from each position from the matrix line by line into a new binary value (e.g. 10001101). Note: some authors use other approaches to concatenate the binary values (e.g. clockwise direction), but the final result will be the same.
- Then, we convert this binary value to a decimal value and set it to the central value of the matrix, which is actually a pixel from the original image.
- At the end of this procedure (LBP procedure), we have a new image which represents better the characteristics of the original image.
- **Note:** The LBP procedure was expanded to use a different number of radius and neighbors, it is called Circular LBP.

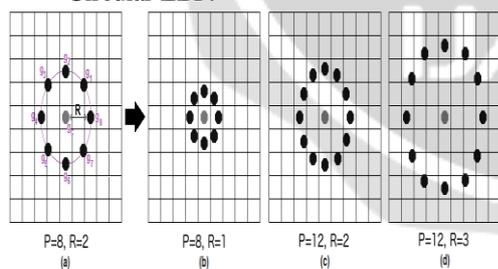


fig 4.2

It can be done by using **bilinear interpolation**. If some data point is between the pixels, it uses the values from the 4 nearest pixels (2x2) to estimate the value of the new data point.

4. Extracting the Histograms: Now, using the image generated in the last step, we can use the **Grid X** and **Grid Y** parameters to divide the image into multiple grids, as can be seen in the following image:

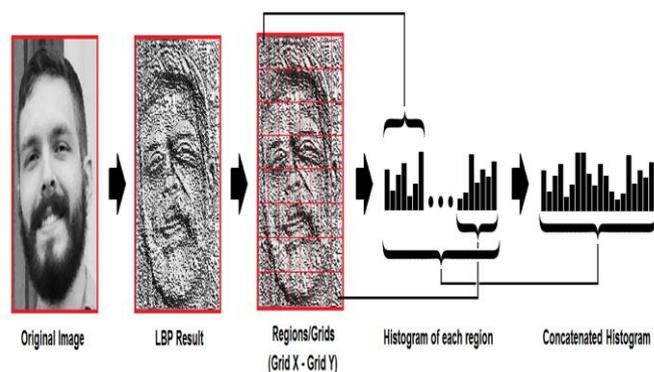


Fig 4.3

Based on the image above, we can extract the histogram of each region as follows:

- As we have an image in grayscale, each histogram (from each grid) will contain only 256 positions (0~255) representing the occurrences of each pixel intensity.
- Then, we need to concatenate each histogram to create a new and bigger histogram. Supposing we have 8x8 grids, we will have $8 \times 8 \times 256 = 16,384$ positions in the final histogram. The final histogram represents the characteristics of the image original image.

The LBPH algorithm is pretty much it.

5. Performing the face recognition: In this step, the algorithm is already trained. 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.

- 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.
- We can use various approaches to compare the histograms (calculate the distance between two histograms), for example: **euclidean distance**, **chi-square**, **absolute value**, etc. In this example, we can use the Euclidean distance (which is quite known) based on the following formula:

$$D = \sqrt{\sum_{i=1}^n (hist1_i - hist2_i)^2}$$

- So the algorithm output is the ID from the image with the closest histogram. The algorithm should also return the calculated distance, which can be used as a '**confidence**' measurement. **Note:** don't be fooled about the 'confidence' name, as lower confidences are better because it means the distance between the two histograms is closer.
- We can then use a threshold and the 'confidence' to automatically estimate if the algorithm has correctly recognized the image. We can assume that the algorithm has successfully recognized if the confidence is lower than the threshold defined.

5.CONCLUSION:

In today technology advance world autonomous system are gaining popularity soothe advancement in latest technology is continuously rapidly made on different latest door automatically lock security system. Customers are

increasingly looking for customizable devices, so that their experiences can be tailored precisely. Face recognition technology will help in reducing crime like robbery and any other unavoidable crimes. As the technology for smart homes continues to evolve,

6. REFERENCES:

- [1] Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Sixth International Conference on Natural Computation (ICNC 2010) "Network Video Capture and Short Message Service Alarm System Design Based on Embedded Linux" Duanchun ZHOU Guangxing TAN
- [2] Conference on Environmental Science and Information Application Technology-"A Wireless Video Surveillance System based on 3G Network" by Wang Liwei Yan Shi Xu Yiqiu
- [3] International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 7, December 2012. www.ijrcct.org chiefeditor@ijrcct.org Page 507 "Video Frame Retrieval Using Effective Query Processing" N.Ramya Tulasi, Y Indu
- [4] "ARM9 Based Real Time Embedded Network Video Capture And SMS Alerting system" M.L.V.N.B.S.Kumar, Dr.N.S.Murthi Sarma, Ch.Sridevi, A.Pravin ECE Department, BVC Engineering College Odalarevu(2012)
- [5] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012) 138 "ARM Based Mobile Phone- Embedded Real-Time Remote Video Surveillance System With Network Camera Krishna Kishore1, B.Chinna Rao2, P.M.Francis3
- [6] International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.1, Issue 8, October 2013 "IMPLEMENTATION OF EMBEDDED VIDEO RETRIEVE SYSTEM BASED ON ARM9" V. Jyothi, Prof. M.Srinivas Rao, K.Hanuja
- [7] IOSR Journal of Engineering (IOSRJEN) e-ISSN: 2250-3021, p-ISSN: 2278-8719 Vol. 3, Issue 7 (July. 2013), ||V6||PP 14-1814 | P a g e "Embedded Real Time Video Monitoring System using Arm" by Kavitha Mamindla, Dr.V.Padmaja, CH.NagaDeepa
- [8] "Smart Video Security Surveillance with Mobile Remote Control" by Tasleem Mandrupkar Manisha Kumari Rupali Mane(2014)
- [9] "VIDEO MONITORING AND MOTION DETECTION SYSTEM BASED ON ARM-LINUX PLATFORM AND HTTP PROTOCOL WITH SMS CAPABILITY" *Nava Jeevan Raju, O. and Praveen, P.(2014)
- [10] Andi Adriansyah, Akhmad Wahyu Dani " Design of Small Smart Home Control Systems Based on Wireless Sensor Networks and Power Line Communications" 10.1109/TIE .2014 .2379586, IEEE Transactions on Industrial Electronics.
- [11] Kim Baraka, Marc Ghobril, Sami Malek, Rouwaida Kanj, Ayman Kayssi "Low cost Arduino/Android-based Energy-Efficient Home
- [12] "Automation System with Smart Task Scheduling" 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks.
- [13] Zhenyu Zoua, Ke-Jun Lib*, Ruzhen Lia and Shaofeng Wub " Smart Home System Based on IPV6 and ZIGBEE Technology" Procedia Engineering 15 (2011) 1529 – 1533
- [14] Rajeev Piyare "Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone" International Journal of Internet of Things 2013, 2(1): 5-11 Yue Li " Design of A Key Establishment Protocol for Smart Home Energy Management System" 2013

[15]Fifth International Conference on Computational Intelligence, Communication Systems and Networks. Shiu Kumar"UBIQUITOUS SMART HOME SYSTEM USING ANDROID APPLICATION" International Journal of Computer Networks & Communications (IJCN C) Vol.6, No.1, January 2014 Andi Adriansyah,

[16]Akhmad Wahyu Dani" Design of Small Smart Home System Based on Arduino" 2014 Electrical Power, Electronics, Communications, Controls, and Informatics Seminar IBoard datasheet by "www.iteadstudio.com " Tech Support: support@iteadstudio.com XBee datasheet by Digi International, Inc. All rights reserved"www.digi.com " rf-experts@digi.com

[17]Nazrul Anuar Nayan, Ili A.M. Ikhsan, Yasuhiro Takahashi " Using ZigBee Communication Technology in a smart Home Wireless Sensor Network "Proceedings of Second International Conference on Modern Trends in. "C Programming for Arduino" Julien Bayle Copyright © 2013 Packet Publishing "Programming Your Home Automate with Arduino, Android, and Your Computer" Mike Riley, Copyright © 2012 The Pragmatic Programmers, LLC. ZigBee Communication Technology in a smart Home Wireless Sensor Network "Proceedings of Second International Conference on Modern Trends in Science, Engineering and Technology 2014"

