RASPBERRY PI BASED HOME SECURITY SYSTEM

Annapu Reddy Ravi Theja[1], Anusha R[2], Archana S[3], Arpitha R Sabarad[4], Dr. Manjula R Bharamagoudra[5]

[1,2,3,4,5] *School of Electronics and Communication Engineering, REVA University, (India)*

ABSTRACT

With advancement in technology, there is a massive need to upgrade our security systems. Conventional wisdom holds that if skilled and determined thieves want to break into a residence, they can. Some home owners use this belief as an excuse to forgo security measures and systems. Essential Home Security doesn't deny the premise but offers an illustrated, practical, and alternative outlook and outlines strategies to transform your residence into a much harder, riskier, and less-rewarding target. The goal is an environment that many thieves may simply choose to bypass in lieu of easier marks. Keys, passwords, and PIN codes are quite easy to breach. What was in need was a unique security system which will provide us more security so that thieves can't breach easily into the residence. A fingerprint-based lock is a wonderful solution to the conventionally encountered inconveniences. A system like this, allows access to only those whose fingerprints that are prestored in the memory. Even with a complete power failure, the stored fingerprints are retained. The fingerprint module interfaced with the Raspberry-pi can be integrated in our homes as a part of the security system. Through this paper, we present a Raspberry-pi based home security system.

I. INTRODUCTION

Ensuring the security of your home and the safety of your family members is critical to providing a happy and comfortable family life. Moreover, considering the increasing number of home burglaries, it is paramount that you keep your home protected from all sorts of criminal intrusions, there are many other risks that can make your home an easy target for criminals, like allowing strangers into your home, leaving some windows unlocked when rushing out, or leaving your landscape unattended so thieves have a place to hide. To reduce such threats, you should be more careful and seek professional help in designing an integrated home security system.

There are many ways in which the threats can take place even after taking care of security measures, some of them are - a key based lock system can be easily breached with the help of tool kits, a PIN based security system that could be hacked by using some software or some hardware tools, a Password based lock which is not a feasible method as it can be opened by trying out some random combinations.

There are a lot of elements to think about when it comes to home security systems and that includes how the security system could benefit you and your family. A few reasons how that is true includes - Protects valuables, deters crime, allows remote access to your home via cameras installed throughout your home, makes room for peace of mind, lowers homeowners Insurance by eliminating the need to pay a monthly fee for other security systems.

Fingerprint based security system can be used at many places like Industries, Offices, Bank lockers, Colleges or even at our homes.
This project is a fine combination of the “Biometrics technology” and the “Raspberry-pi technology”. It makes use of a Biometric sensor to provide access to the user for door locking/unlocking; the access is given after detection of fingerprint through the biometric sensor.

We have seen that most of the devices today are using fingerprint sensors for security purpose like in mobile phones, e-verifications, biometric for Aadhar-card, etc. And in our daily life we don’t have enough security systems. Hence, we are implemented a security system that could be installed at various places. In this system, we are used a Raspberry-pi with the fingerprint sensor for security purpose.

The main aim of our project is to develop a secure locking system based on fingerprint scanning. The steps followed for the implementation are -Enroll fingerprints of authorized users into the system, check whether the fingerprints are already stored in the system, Display the position of the existing fingerprint, Grant access to the door by checking whether the fingerprint is a valid stored one, Delete the unrequired fingerprints from the system based on the people who should be given access.

II. RELATED WORK

Below, we have discussed a few research papers on the fingerprint-based home security system

2.1 Hoi Le et al. [1] proposed online fingerprint identification with a fast and distortion tolerant hashing method, National ID card, electronic commerce, and access to computer networks are some scenarios where reliable identification is a must. Existing authentication systems relying on knowledge-based approaches like passwords or token-based such as magnetic cards and passports contain serious security risks due to the vulnerability to engineering-social attacks and the easiness of sharing or compromising passwords and PINs. Biometrics such as fingerprint, face, eye retina, and voice offer a more reliable means for authentication. The limitation is due to large biometric database and complicated biometric measures, it is difficult to design both an accurate and fast biometric recognition.

2.2. Manvjeet Kaur et al. [2] proposed a fingerprint verification system using minutiae extraction technique. Most fingerprint recognition techniques are based on minutiae matching and have been well studied. However, this technology still suffers from problems associated with the handling of poor-quality impressions. One problem besetting fingerprint matching is distortion. Distortion changes both geometric position and orientation and leads to difficulties in establishing a match among multiple impressions acquired from the same fingertip. Marking all the minutiae accurately as well as rejecting false minutiae is another issue still under research. The poor quality of impressions and distortion is the issue suffered by this technology.

2.3. Ratha et al. [3] proposed an adaptive flow orientation-based segmentation or binarization algorithm. In this approach the orientation field is computed to obtain the ridge directions at each point in the image. To segment

the ridges, a 16x16 window oriented along the ridge direction is considered around each pixel. The projection sum along the ridge direction is computed. The centres of the ridges appear as peak points in the projection. The ridge skeleton thus obtained is smoothened by morphological operation. Finally, minutiae are detected by locating end points and bifurcations in the thinned binary image. The limitations is processed images need to be thinned for proper matching.

2.4. Wei Cui et al. [4] proposed the research of edge detection algorithm for fingerprint images. This paper introduces some edge detection operators and compares their characteristics and performances. At last the experiment show that each algorithm has its advantages and disadvantages, and the suitable algorithm should be selected according the characteristic of the images detected, so that it can perform perfectly. The Canny Operator is not susceptible to the noise interference; it can detect the real weak edge. The advantage is that it uses two different thresholds to detect the strong edge and the weak edge, and the weak edge will be included in the output image only when the weak edge is connected to the strong edge. The Sobel Operator has a good performance on the images with gray gradient and high noise, but the location of edges is not very accurate, the edges of the image have more than one pixel. The Binary Image Edge Detection Algorithm is simple, but it can detect the edge of the image accurately, and the processed images are not need to be thinned, it particularly adapts to process various binary images with no noise. So, each algorithm has its advantages and disadvantages. However, the Canny Operator is not susceptible to noise interference and in the Sobel Operator, the location of edges is not very accurate, the edges of the image have more than one pixel.

2.5. Asker M. Bazen et al. [5] proposed a correlation-based fingerprint verification system. In this paper, a correlation-based fingerprint verification system is presented. Unlike the traditional minutiae-based systems, this system directly uses the richer grey-scale information of the fingerprints. The correlation-based fingerprint verification system first selects appropriate templates in the primary fingerprint, uses template matching to locate them in the secondary print, and compares the template positions of both fingerprints. Unlike minutiae-based systems, the correlation-based fingerprint verification system is capable of dealing with bad-quality images from which no minutiae can be extracted reliably and with fingerprints that suffer from non-uniform shape distortions. Experiments have shown that the performance of this system at the moment is comparable to the performance of many other fingerprint verification systems.

2.6. S. Mil'shtein et al. [6] proposed a fingerprint recognition algorithm for partial and full fingerprints. In this study, they propose two new algorithms. The first algorithm, called the Spaced Frequency Transformation Algorithm (SFTA), is based on taking the Fast Fourier Transform of the images. The second algorithm, called the Line Scan Algorithm (LSA), was developed to compare partial fingerprints and reduce the time taken to compare full fingerprints. A combination of SFTA and LSA provides a very efficient recognition technique. The most notable case of partial fingerprints. At this time, the major drawback of developed algorithms is lack of pre-classification of examined fingers. Thus, they use minutiae classification scheme to reduce the reference base for given tested finger. When the reference base had shrunk, they apply the LSA and SFTA.

III. PROPOSED WORK

3.1. Methodology

In our project, we interface Raspberry pi with the fingerprint scanner and make use of a smartphone app named the VNC viewer to command the Raspberry Pi. The control options are displayed on the phone and the user just needs to choose the operation that should be executed. The fingerprint module used here, works on UART (Universal Asynchronous Transmitter Receiver) and it has been interfaced with Raspberry Pi using a USB (Universal Serial Bus) to serial converter. The connections are done according to the block diagram shown below. The registered users through finger print sensor are given access to the home using the unlocking system through solenoid valve.

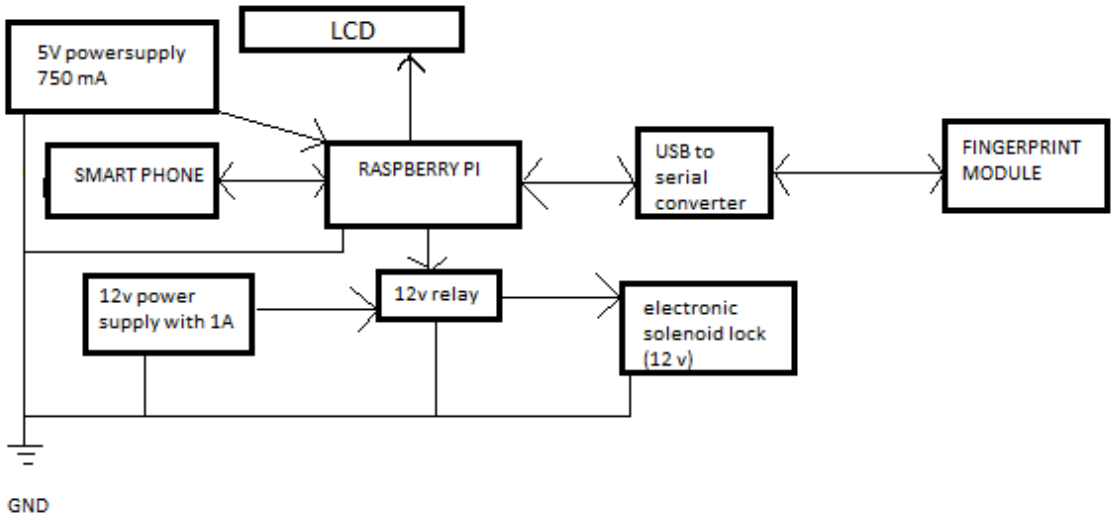

Fig 3.1 – Block Diagram of a Raspberry Pi Based Home Security System

3.2. Hardware and Software requirements

3.2.1 The components required for the Hardware implementation are:

1. Raspberry Pi
2. Fingerprint Module
3. USB to Serial Converter
4. LCD 16x2
5. Power supply
6. 12V Relay
7. Electronic solenoid lock
8. Smart phone

3.2.2 The Software requirements includes:

1. Raspberry Pi (OS Installation): Raspbian comes pre-installed with plenty of software for education, programming and general use. It has Python, Scratch, Sonic Pi, Java, Mathematica and more. We are using Python 2.7 for our project development.

2. Fingerprint sensor: Library files installation as given into the Raspberry pi so that we can interface this module with the Raspberry Pi USB port by coding in python.
3. Smartphone: The VNC Viewer app is installed to command the Raspberry Pi.

3.3 Implementation process

3.3.1 Hardware Implementation

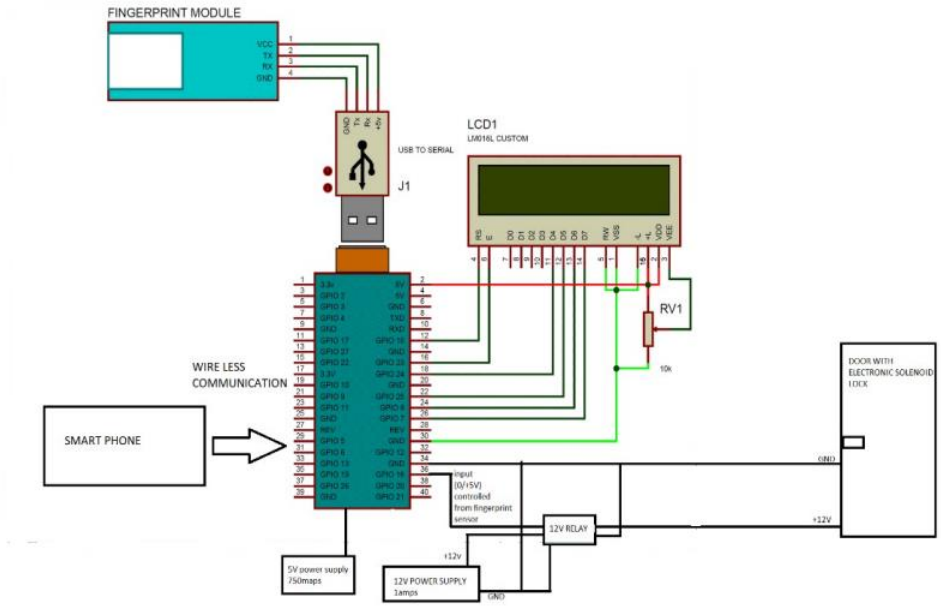

Fig 3.2 - Circuit Diagram of a Raspberry Pi Based Home Security System

The required connections are done as shown in the Fig. The fingerprint scanner module which works on UART is connected to Raspberry Pi USB port by using a USB to Serial converter.

A 16x2 LCD display is used for displaying all the messages pertaining to the operations that will be running. It helps in easy interfacing with the user. A 10k pot is also used with the LCD for controlling the contrast of the same. 16x2 LCD pins RS, EN, d4, d5, d6, and d7 are connected with the GPIO Pins 18, 23, 24, 25, 8 and 7 of Raspberry Pi respectively.

The Raspberry pi is connected to a 12V Relay, which is also connected to an Electronic solenoid lock. In general, the relay is used where a safe low voltage circuit controls a high voltage circuit. Relay is used in our system as an automatic switching device. Since, the Raspberry Pi system gives an output of only 5V but to power up the electronic lock we need an input of 12V. Relay has 3 inputs +12v, Input (+5v from MCU), GND. When the Input from MCU is +5v then relay turns on. At the output side of the relay we have three pins, they are NC, NO, +12/GND based on the connections. When relay is on, NO will turn on and NC will turn off.

Also, in this Raspberry pi interfacing with the fingerprint scanner, we make use of a smartphone app named the VNC viewer to command the Raspberry Pi. Here we scan for the IP address of the Raspberry Pi and connect to it. Options to control are displayed on the phone. The user gets to choose any one of them and the operation is executed. For commanding the Raspberry pi, we make use of the VNC viewer. Once these connections are done, we power up the board.

3.3.2 Software Implementation

We begin by downloading the OS Raspbian into the SD card and then inserting it into the SD card slot of the Raspberry Pi board. On booting, we download the library files required for the operation of Fingerprint scanner and the LCD display.

On creating a new file, we type our source code in Python language by calling in the library files, GPIO pins are then initialized. When this software part is ready, we make the hardware external set-up.

IV. CONCLUSION

Having considered some of the inadequacies found in most of the security logistics, in this project weexploited 'fingerprints', which uniquely identifies the individual for all practical purposes. In this project of ours, we have successfully implemented a security system that potentially makes use of this Fingerprint scanner for collecting the fingerprints and processes the data to perform desired operations specified by our code. As discussed, we have made use of Raspberry Pi board that controls the various hardware components that are interfaced. We also have made use of LCD that displays messages to guide the user. The various applications of this model include that it can be installed wherever security is of at most importance, it can be fitted in front of doors in houses, offices and many other places like lockers in banks, in places where security is a prerequisite. Our software features that it provides the operations of enrolling and deleting of fingerprints along with the time duration of opening and closing of the door, all of which can be decided by the user themselves. Being very specific, our security system also shows the position in which the fingerprint is stored in a set of scanned data. The data stored can also be deleted only on the wish of the user and start from the beginning afresh. Hence this gets no older with time. Not only this, our model is potential enough to store as many as 256 fingerprints. Hence there is no fear of lack of storage space for storing data of multiple users.

REFERENCES

[1] Hoi Le, The Duy Bui, "Online fingerprint identification with a fast and distortion tolerant hashing." Journal of Information Assurance and Security-4, page no. 117-123, 2009.

[2] Manvjeet Kaur, Mukhwinder Singh, AkshayGirdhar, and Parvinder S. Sandhu, "Fingerprint Verification System using Minutiae Extraction Technique." World academy of Science, Engineering and Technology, page no. 46, 2008.

[3] N. K. Ratha, K. Karu, Shaoyun Chen and A. K. Jain, "A real-time matching system for large fingerprint databases," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 8, pp. 799-813, Aug 1996.

[4] Wei Cui, Guoliang Wu, Rongjin Hua, and Hao Yang, "The Research of Edge Detection Algorithm for Fingerprint Images." IEEE 2008.

[5] Asker M. Bazen, Gerben T.B. Verwaaijen, Sabih H. Gerez, "A Correlation-Based Fingerprint Verification System." Workshop on Circuits, Systems and Signal Processing, Veldhoven, the Netherlands, November 2000.

[6] David G. Lowe, "Distinctive Image Features from Scale Invariant Key points." International Journal of Computer Vision, 2004.

[7] S. Mil'shtein, A. Pillai, A. Shendye, C. Liessner, and M. Baier, "Fingerprint Recognition Algorithms for Partial and Full Fingerprints." IEEE 2008.