International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

Bio Metric Based Verification System for Canteen Food Distribution

NUNNA.HEMANTH
NUNNAHEMANTH06@GMAIL.COM
DEPARTMENT OF ECE
BONAM VENKATA CHALAMAYYA COLLEGE OF ENGINEERING

K. RAJASEKHAR MTECH, (PHD), MISTE
RAJA.DUBBLY@GMAIL.COM
PROFESSOR
DEPARTMENT OF ECE
BONAM VENKATA CHALAMAYYA COLLEGE OF ENGINEERING

Abstract— **The main aim of the project is to distribute the canteen food in proper way. To distribute the food according to the need of the students. Some students wants non-veg food and some students wants veg food so according to the need of the students food will distribute properly. But some students don't pay bill for non-veg but they will come to the canteen and eat non veg food this can be avoided by using "BIO Metric Based Verification System for Canteen Food Distribution".**

In this process we have use two verifications .In the first verification, whether the student belongs to this canteen or not. In the second verification whether the student belongs to veg or non veg category. This verification is done through two thumb modules put at the two gates of the canteen. When the student put their thumb on the thumb module it recognizes and displays the name of the student on the LCD display and also announces their name through speech module (APR9600).After completion of all the students verification,the information of students will go as a message to a manager using gsm.information such as no of students are vegitarion ,non vegitarion and also no of absents.

KEYWORDS: Arduino , Bio Metric , LCD, Speech module.

I. INTRODUCTION

The skin on our palms and fingers exhibits a flow like patterns of ridges and valleys. The papillary ridges on the finger, called friction ridges, which help the hand to grasp objects and increase friction and improve the tactile sensing of the surface structure. These ridge patterns are now scientifically proved as unique for each person. The cuts and burns in a person's finger may alter these patterns temporarily but they reappear after the injury heals. Fingerprints are now used widely for identification and verification purpose. They are used for attendance purpose in organizations to avoid proxy for criminal identification like terrorist, murderer and violators and also in passports (a matter of national high importance) of person.

In this busy and competitive world, Security plays a crucial role. Manually, human cannot find ways to provide security to his confidential matters. So instead of doing manually, we can find an alternate method which can provide a full fledged security. In the society, where individuals can easily access their information anytime and anywhere, people are also facing with the risk that others can access the same information or data anytime and anywhere. So for this generally passwords, identification cards and verification of pin techniques are being used but doing like this there is a disadvantage. The disadvantage is that the passwords could be hacked and a card may be lost or stolen. So the most secured system is fingerprint verification because fingerprint of one person never match with the other person. Biometrics studies include fingerprint, voice, signature and face recognizing and verification. Among all these methods fingerprint proves to be one of the best one providing good mismatch ratio, high accurate in terms of security and also reliable.

!!.PROPOSED WORK

The proposed technology named RADIO FREQUENCY IDENTIFICATION TECHNOLOGY (RFID) is used for implementing automatic attendance system for students in Educational institutions. The RFID based automatic attendance system includes the RFID reader, tags, computer system and host system application. THE RFID based automatic attendance system is used for automatically taking students attendance and giving warning to students on cases of low attendance which could degrade the performance of

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

student or prevent the student from taking the course examination. I find some disadvantages in this technology. Some of disadvantage of using RFID systems are STANDARDIZATION:

Though the characteristics of the application and the environment of use determine the appropriate tag, the sparse standards still leave much freedom in the choice of Communication protocols and the format and amount of information stored in the tag. Companies transcending a closed loop solution and wishing to share their application with others may encounter conflicts as cooperating partners need to agree in standards concerning communication protocols, signal modulation types, data transmission rates, data encoding and frames and collision handling algorithms

2. SECURITY AND PRIVACY ISSUES

Depending on the field of application and in some cases, prescribed by law it may become necessary to prevent unauthorized persons from reading or writing data stored on or Transmitted from tags. To this end, encryption must be ensured at all interfaces where data could be intercepted or transmitted

3) POSSIBLE VIRUS ATTACKS

4) COST

III. TOP LEVEL SYSTEM DESCRIPTION

Figure.1 shows the block diagram of the Microcontroller based security system. This design combines the Microcontroller with the Fingerprint Module, display, and communication interfaces. This integration accelerates development while maintaining design flexibility and simplifies testing. Figure.1 shows the block diagram of the Microcontroller based system. The design combines the microcontroller with the Fingerprint Module, display, and communication interfaces. This integration accelerates whimaintaining design flexibility and simplifies testing development

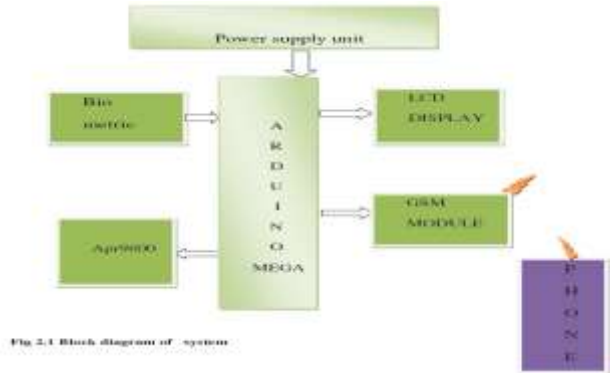

Fig.1Top Level system Diagram

The design includes following three modes:

Mode 1: The fingerprint module is connected with the PC using RS232 through serial communication. The Software called SFG Demo is then used for interfacing purpose. The fingerprint module is interfaced with the PC through the SFG Demo. By using SFG Demo software we are storing the fingerprint template of all the individuals with a unique id inside the fingerprint module.

Mode 2: Then we are connecting fingerprint module with microcontroller, the use of microcontroller is to extract the data from fingerprint module .By using microcontroller1 we are receiving the enrollment id or unique id of specific person. For example- Suppose if in a class, templates of all the students are stored. Then when a student places his/her finger in the fingerprint sensor, matching of template takes place in 1: N fashion inside the fingerprint module. Then the unique ids are received by using microcontroller

IV.ARCHITECTURE OF MATCHING INSIDE FINGERPRINT MODULE (R305)

It is actually very difficult to devise a proper algorithm for matching of fingerprint and making the algorithm robust. This chapter discusses the current state of the art feature extraction techniques and gives a literary review of algorithm of matching the extraction.

Data Acquisition

Traditionally in law enforcement applications fingerprints were acquired off-line by transferring the inked impression of thumb on a paper. Recently, the automated fingerprint verification systems use live-scan digital images of fingerprint acquired from a fingerprint sensor or module. These sensors or module are based on optical, capacitance, ultrasonic and thermal and other imaging technologies.

The optical sensors are most popular and are fairly expensive. These sensors are based on FTIR (Frustrated Total Internal Reflection) technique. When a finger touches the sensor surface which actually is a side of a glass prism, in which one side of the prism is illuminated through a diffused light. While the fingerprint valleys that do not touch the sensor surface reflect the light, ridges that touch the surface absorb the light.

The sensor exploits this differential property of light reflection to differentiate the ridges (which appear dark) from valleys.

Fig.2 R305 module and fingerprint recognition with various features

Like the optical sensor algorithm for data acquisition there are two other algorithms for data acquisition namely, capacitive sensor utilization method and ultra sound technology based sensors. As in our project we have tried to use the first one that is optical sensors method. So we have not described the other two methods

Image Pre-processing

The pre-processing steps try to compensate for the variations in lighting, contrast and other inconsistencies which are introduced by the sensor during acquisition process. There are many processes but presently some methods are very famous which the following are:

Gaussian Blur: A convolution operation which applied to the original fingerprint image to reduce image noise introduced by sensor during data acquisition.

Sliding window contrast adjustment: Sliding window contrast adjustment is used to compensate for any lighting inconsistencies within a fingerprint and to obtain contrast consistencies among different fingerprints

Histogram based intensity level adjustment: This is a final step is to further enhance the ridges and valleys.

Feature extraction

The feature extraction technique for minutiae points (bifurcations and endings), pores and ridge contours is described in this section.

Minutiae Extraction:

Most of the minutiae extraction techniques trace the fingerprint skeleton to find different types of minutiae points. Orientation Estimation: A fingerprint image is an oriented texture pattern and a ridge orientation at a pixel (x, y) is the angle that the ridges within a small neighborhood centered at (x, y) form with the horizontal axis. Thus a fingerprint is divided into many blocks. An analysis of gray scale gradient within a block is done to estimate the representative ridge orientation within that block. Segmentation: During this stage the portions of the fingerprint image depicting the finger foreground is segmented. This further eliminates the spurious features from background and noisy region within a fingerprint.

Ridge Detection:

An important property of the ridges in a fingerprint image is that the gray level values on ridges attain their local maxima along a direction normal to the local ridge orientation. The resulting ridge map often contains false ridges in the form of holes and speckles. The ridge map is cleaned using a connected component algorithm. Finally the ridges are thinned using standard thinning algorithm.

Minutiae Detection:

The minutia points are then extracted from the thinned ridge map by examining the 8 neighborhood of each ridge skeleton pixel. The ridge breaks, Ridge bending direction and width are the information extracted but this may contain spurious minutiae. This may occur due to presence of noise, ridge breaks (even after enhancement) and image processing artifacts. Post processing: A number of heuristics are used to remove spurious minutiae. False minutiae are generally found at the borders as the ridges end abruptly. These false minutiae at the border can be recognized by examining the number of foreground pixels in a region around minutia point. If number of foreground pixels is relatively small then the minutia point can be removed.

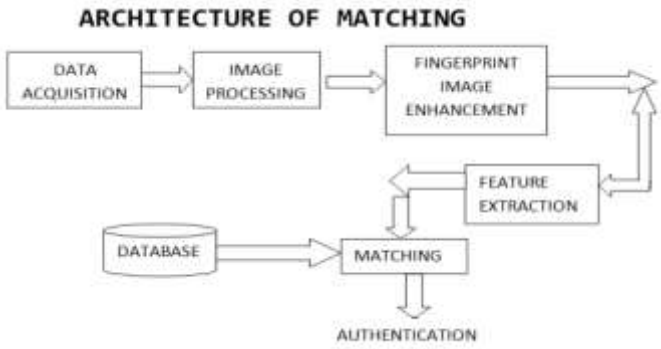

Fig. 3 Architecture of fingerprint matching algorithm

VI. RESULTS AND DISCUSSION

The security can save each person's fingerprint, hence makes

the system more robust. During enrolment the person's fingerprints is assumed to be clean, not dry or damp, no scratches and not swollen.

Problems	Fingerprint Snapshot	Problems	Fingerprint Snapshot
Finger Misplacement		Dirty Finger	
Orientation		Skin Problems	
Wet Finger			

Members are required to place their fingerprint. After the enrolment stage, the data will be saved in the fingerprint scanner and the verification system takes place by comparing the capture fingerprint characteristic with the previously enrolled data. Table I shows the types of issue that might occur when taking attendance system acquiring fingerprint for attendance purposes. We considered all of these factors for the product which are user-friendliness, convenience, portability, and heating resistance.

VII. CONCLUSIONS

1. Easy to use and requires no special training or equipment.
2. Fingerprint is unique for every person it cannot be imitated or fabricated. It is not same in the case of twins also.
3. High accuracy in terms of security
4. No manual errors
5. No false instructions

REFERENCES

[1] Signals, Systems and Computers, 2004 Conference Record of the Thirty-Eighth Asilomar Conference on Publication 7-Nov-2004 Volume: 1, on page(s): 577-581 Vol.1.

[2] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[3] International Journals of Biometric and Bioinformatics, Volume (3): Issue (1).

[4] Mukesh Kumar Thakur, Ravi Shankar Kumar, Mohit Kumar, Raju Kumar "Wireless Fingerprint Based Security System using Zigbee" , International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-1, Issue-5, April 2013.

[5] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.

[6] "Fingerprint Matching" by Anil K. Jain, Jianjiang Feng and Karthik Nandakumar, Department of Computer Science and Enginnering, Michign State University.

Cappelli, R., Lumini, A., Maio, D. and Maltoni, D. (2007). Fingerprint Image Reconstruction from Standard Templates, IEEE Transactions, vol. 29, pp.1489-1503.

Cappelli, R., Maio, D., Maltoni, D., Wayman, J., L. and Jain, A. K. (2006). Performance evaluation of fingerprint verification systems, IEEE Trans. Pattern Anal., 28(1), pp. 3-18.

Chirillo, J. and Scott, B. (2007). Implementing Biometric Security. Indianapolis: John Wiley Publishing Inc., ISBN: 0 7654 25026.

Clavereau, M. (2011). Absence: time to tackle the root causes. Retrieved 15th October, 2013 from http://www.hrmagazine.co.uk

Dale, M. R. (2005). A Process for Combining Structured Analysis and Object Oriented Design. Retrieved 10th February, 2013 from http://www.dtic.mil/ndia/systems/Rickman2.pdf.

Dan, P. and Neil, P. (2005). UML 2.0 in a Nutshell. O'Reilly publication. ISBN: 0-596-00795-7.

Dubin, C. (2011). "Biometrics: Hands Down, ID Management". Retrieved 30th March 2013 from http://proquest.umi.com/pqdweb?index=0&did=2277161341&SrchMode=1&sid=2&Fmt=6VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1304030671&clientId=13314.

Hong, L., Wan, Y., and Jain, A. (1998). Fingerprint Image Enhancement algorithm and performance evaluation, Computer Journal of IEEE transactions pattern annulus machine intelligent, 20(8), pp. 777-789.

Jianjiang, F. (2007). Combining minutiae descriptors for fingerprint matching, Pattern Recognition, pp. 342 – 352.