International Journal of Electrical Engineering.
ISSN 0974-2158 Volume 12, Number 1 (2019), pp. 37-43

http://www.irphouse.com

Biometric based Digital Transaction System using Raspberry PI

M.Sreelatha[1], Dr. M.V. Lakshmaiah[2], B.Bilvika[3]

[1]Research Scholar, Department of Physics, Sri Krishnadevaraya University, Anantapur, India.

[2]Head, Department of Electronics and Physics, Sri Krishnadevaraya University, Anantapur, India.

[3]Research Scholar, Department of Electronics, Sri Krishnadevaraya University, Anantapur, India.

Abstract

Biometric based digital transaction system is used for various kinds of payment system instead of carrying the ATM cards to different places and to memorize their different passwords and pin numbers which is most difficult. Biometric digital transaction system is much safe, secure and very easy to use even without using any password or secret codes to remember as compare with previous system like credit card payment system, wireless system and mobile system etc. Biometric digital transaction system is reliable, economical and it has more advantage as compared with others. In daily life the usage of credit cards, check card for shopping, bus card, subway card for travelling, student card for library and department, and many kinds of cards for unlimited purposes and so on. Since a person has to take many cards and has to remember their passwords or secret codes and to keep secure to take with him all time, it is difficult, so the biometric payment system will solve many problems. Greater adoption of biometric digital transaction system will drive down the cost of biometric readers and thus making it more affordable to small business owners. In this paper we proposed high speed and more secured Biometric based digital transaction system using Raspberry Pi 3.

Keywords: Biometric, Digital transaction, credit cards, Passwords, Raspberry Pi 3.

I. INTRODUCTION

Financial institutions engaging in any form of Internet banking should have effective and reliable methods to authenticate customers. An effective authentication system is

necessary for compliance with requirements to safeguard customer information, to prevent money laundering and terrorist financing, to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements. There are a variety of technologies and methodologies that can be used by financial institutions to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens". One method which is different from all above is biometric identification; here the "biometrics" is defined as "the automated means of recognizing a living person through the measurement of distinguishing physiological or behavioural traits".

II. LITERATURE SURVEY

The author Ann Cavoukian et al. has proposed [1] a scheme that offers the security benefits of biometric encryption along with different uses of biometrics. The most purpose is that BE technology can facilitate to beat the prevailing "zero-sum" mentality, namely, that adding privacy to identification and data of systems can essentially weaken security and functionality.

In the paper, the authors Yagiz Sutcu et al. described end to take a fusion of a minutiae-based fingerprint authentication theme associated and an SVD-based face authentication theme, and show that by using a recently planned cryptographically primitive known as secure sketch, and a notable geometric transformation on trivia, thus it will [2]create it easier to mix completely different modalities at a time associated to create impracticable to forge an «original» combination of fingerprint and face image that passes the authentication.

Wencheng Yang et al. suggests a multimodal biometric scheme that has several advantages [3] over single modal biometric systems. It provides better recognition accuracy. The multimodal biometric system creates two common biometrics statistics, face and fingerprint by employing real multimodal information and two unreal multimodal databases. Through the experimental results it was identified that there is a significant difference between the system performances obtained with the real and unreal multi-modal databases.

Ross A et al. shows that three levels of data regarding the knowledge of parent [4] fingerprint are often extracted from the minutiae or trivia template alone. The orientation-estimation algorithm controls the direction of native ridges using the tiny triplets. In paper fingerprint recognition is aided by minutiae matching.

III. GENERAL DESCRIPTION OF THE HARDWARE

A.HARDWARE:

A.1 Block diagram

This system overcomes all the security problems in existing system and provides high security and efficiency. We developed high speed with high secured digital transaction system as shown in Figure 1. In this system, Raspberry Pi 3 used to interface the finger print scanner to detect the human finger prints and it also programmed to search the finger data from the given database server. Digital transaction options are visible on touch screen and it can use as a keypad also to do the online transactions. This is a perfect and optimal solution for saving and protecting one from the hassle of stolen or lost key or an unauthorized entry .Fingerprint is an excellent solution for the problems arises by cards which provide high accuracy. The skin on our palms and soles exhibits a flow like pattern of ridges called friction ridges. The pattern of friction ridges on each finger is unique. This makes fingerprint a unique identification for everyone.

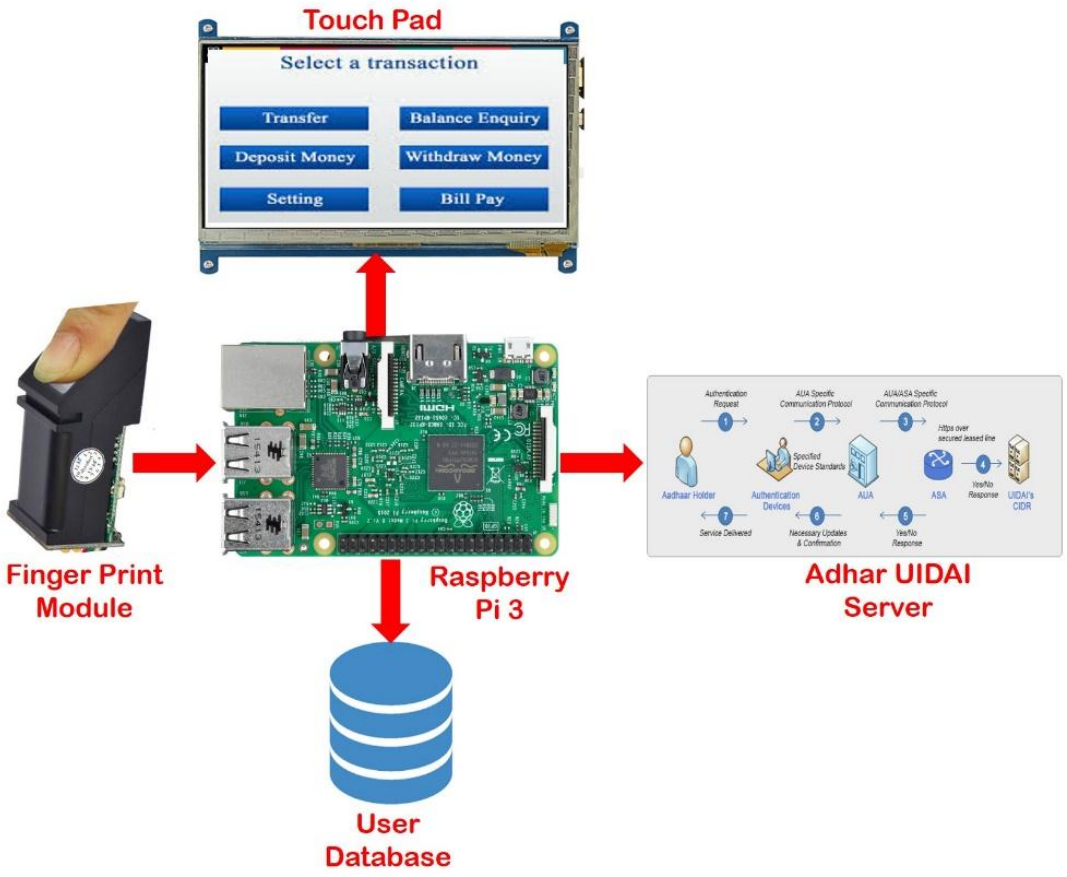

Figure 1: Block Diagram of Biometric Digital Transaction System.

Fingerprint based digital transactions incorporates the proven technology. Fingerprint scanner scans the fingerprints of users and used for ensuring authentication. Fingerprint scanning is more accurate and cost effective method and duplication is virtually impossible. A Fingerprint recognition system can easily perform verification. In verification, the system compares an input fingerprint to the enrolled fingerprint of a specific user to determine if they are from the same finger.

The proposed fingerprint enhancement and fingerprint matching algorithms will strengthen the security and complexity of the proposed random finger generation based digital transaction system. Thus this paper aims to build a high secure digital transaction system which is using low cost devices.

A.2 Fingerprint Module:

The captured fingerprint traits are sent to the Raspberry Pi has enhancement and fingerprint verification for capturing fingerprints. Figure 3 Block diagram of fingerprint based digital transaction system. The main stages of this algorithm include normalization, ridge orientation estimation, ridge frequency estimation and filtering. The first step in this approach involves the normalization of the fingerprint image so that it has a pre-specified mean and variance. An orientation image is then calculated, which is a matrix of direction vectors representing the ridge orientation at each location in the image. The next step in the image enhancement process is the estimation of the ridge frequency image. The frequency image defines the local frequency of the ridges contained in the fingerprint. The next step in the enhancement process is to construct the final filtered image using the pixel values from the pre-filtered images. Lastly, local adaptive 50 thresholding is applied to the directionally filtered image, which produces the final enhanced binary image. After a fingerprint image has been enhanced, the next step is to extract the minutiae from the enhanced image. Following the extraction of minutiae, a final image post processing stage is performed to eliminate false minutiae.

A.4 Raspberry Pi3

Raspberry Pi has authenticated the user (by using right thumb) by using fingerprint matching algorithm and displays the user details on the screen. Next to perform the digital transactions, Raspberry Pi has generated the random finger using novel infinity noise algorithm. Then Raspberry Pi verify the injected random finger and perform the operations like balance enquiry, money transfer, money withdraw and deposit the money. If the finger hasn’t match the system asks right thumb for authentication and system start the procedure from beginning. Now the security of our money is literally in our hands or rather on our fingertips. Enter the password to open digital bank account with the help of a keypad. Immediately the bank account will be opened. After the work has been completed if key is pressed again with help of touch pad the account will be closed again or it close automatically after 3 minutes if the user not processing any data. If an unauthorized person tries to scan his fingerprint image then

an indication will be given by a buzzer which is interfaced to the controller and also if wrong password is entered by the user again indication will be given by the buzzer.

A.5 Display Screen:

Display screen is an output device that displays information in pictorial form. A monitor usually comprises the display device, circuitry, casing, and power supply. The display device in modern monitors is typically a thin film transistor liquid crystal display (TFT-LCD) with LED backlighting having replaced cold-cathode fluorescent lamp (CCFL) backlighting. In this research using resistive type touch screen to display the digital transactions. Resistive touch screen is composed of a flexible top layer made of polythene and a rigid bottom layer made of glass separated by insulating dots, attached to a touch screen controller.

IV. RESULTS

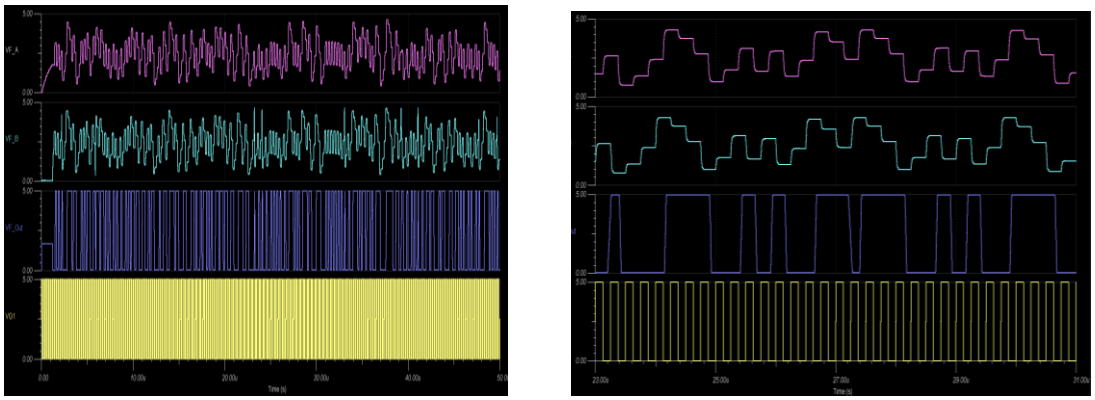

Figure 2: Simulation waveforms for the small infinite Noise Multiplier

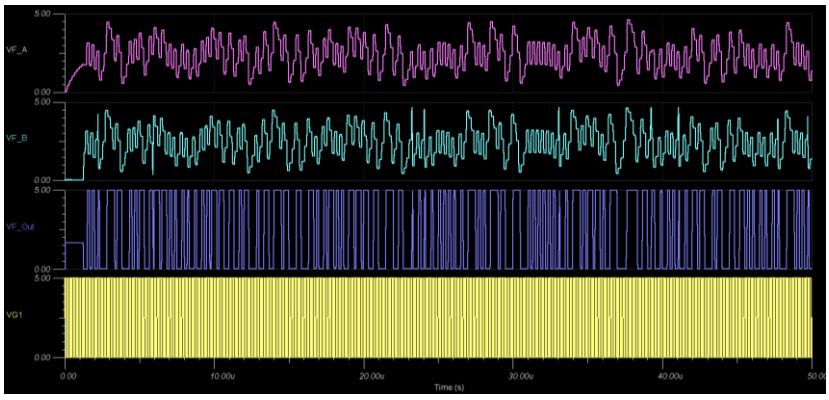

Figure 3: Simulation waveforms for the fast infinite Noise Multiplier.

a. Original Image b. Enhanced Image

Figure 4. Fingerprint Image enhancements

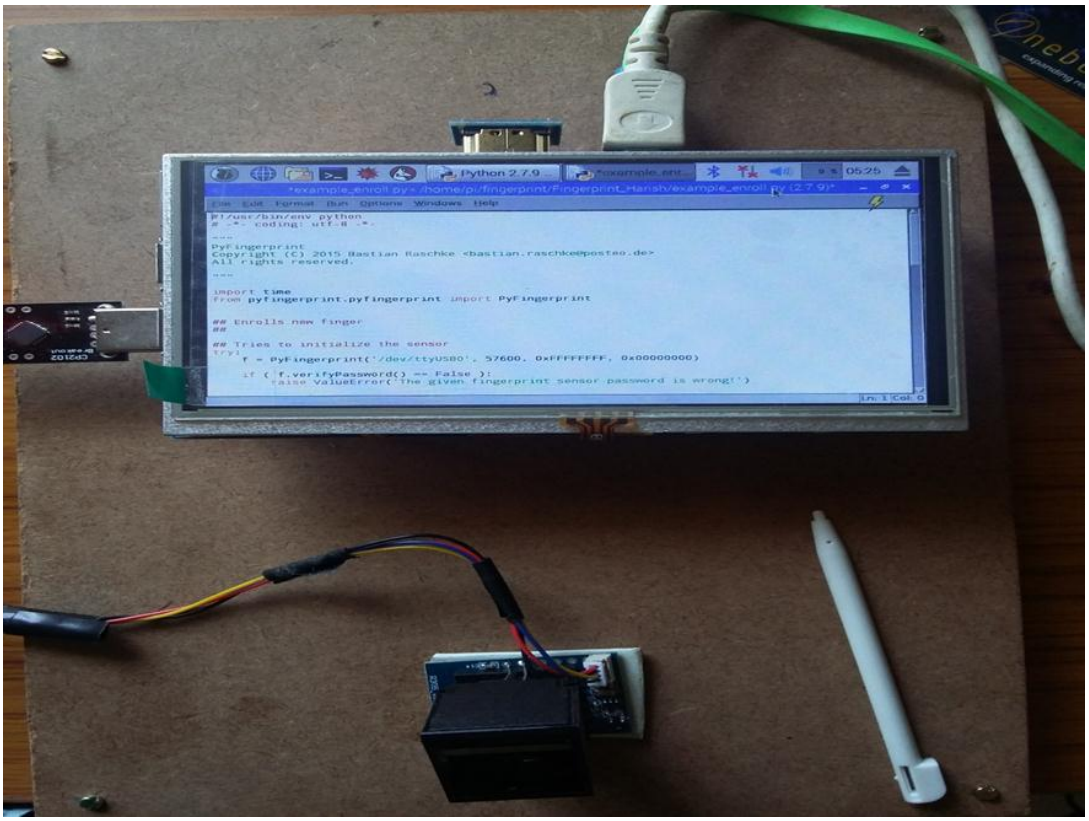

Figure 5: Hardware implementation of fingerprint based digital transaction system

V. CONCLUSION

The conclusion of this whole paper is that the card-less payment system should be replaced and there must be more easier, reliable, secure, cash free and tension free payment system, i-e biometric payment system in which no body have to take with dozens of cards for shopping, travelling pass in office, university or bank as door lock. And he must have some secure codes to access as authorization and there is also one another disadvantage is that there may be stolen of cards or it can be losses at any

time without any care. So to consider all these kinds of problems and disadvantages of card payment system the fingerprints payment system is suggested to be implemented because it is easier, reliable, feasible, secure and easily authorized to everyone. The system has successfully overcome some of the aspects existing with the present technologies, by the use of finger print Biometric as the authentication Technology.

REFERENCES

[1] John C. Dvorak, Forbes.com, SmartCards Get Smarter 06.01.01, 3:00 PM EThttp://www.forbes.com/2001/06/01/0601dvorak.html.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer- Verlag, 2003.

[3] American Express Announces Winners of ©Code Blue© Contest - Global Competition Spurs Innovation in Java(TM) Technology-Based Smart Card Development http://www.SmartCardcentral.com/news/pressrelease/may2001/amex_052301.asp

[4] Scottson & Michaels, Inc. has been in the business of Credit Card Fraud Verification Processing since 1994. http://www.scottson-michaels.com/ccfraudhistory.htm.

[5] Yang Y.J.; The Security of Electronic Banking. Proc. Nat. I International Systems Security Conference. National Computer Security Center. 1997; pp.41-52.

[6] Arrests made over Internet banking fraud; Internet Business News, Aug 2000; Retrieved from http://www.allbusiness.com/finance/615165-1.html (Accessed on Dec 2010).

[7] Fire Alarm Company Burned by e-Banking Fraud; Retrieved from http://krebsonsecurity.com/2010/04/fire-alarm-company-burned-by-e-bankingfraud/ (Accessed on Dec 2010).

[8] Internet World Stats - Usage and Population Statistics; Retrieved from http://www.internetworldstats.com/stats3.htm (Accessed on Dec 2010).

[9] APWG ; Retrieved from http://www.antiphishing.org/ (Accessed on Dec 2010).

[10] Maltoni D, Jain AK, Maio D, Prabhakar S, Handbook of Fingerprint Recognition, Springer, 2004.