ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014
International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

Design of Biometric Based Transaction System using Open Source Software Development Environment

SavitaChoudhary

Assistant Professor, Dept. of CSE, Sir MVIT, Bangalore, India.

ABSTRACT*:* This paper presents a biometric based identification system instead of card based transactions. The key intention is to map multiple account information using a single fingerprint. This system reduces the need to maintain a card for each account.

KEYWORDS*:* Biometric, Fingerprint

I. INTRODUCTION

Biometrics [1] is an automated method of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Physiological characteristics such as hand images, finger images, facial characteristics or iris recognition and behavioral characteristics such as dynamic signature verification, speaker verification or keystroke dynamics are commonly used.

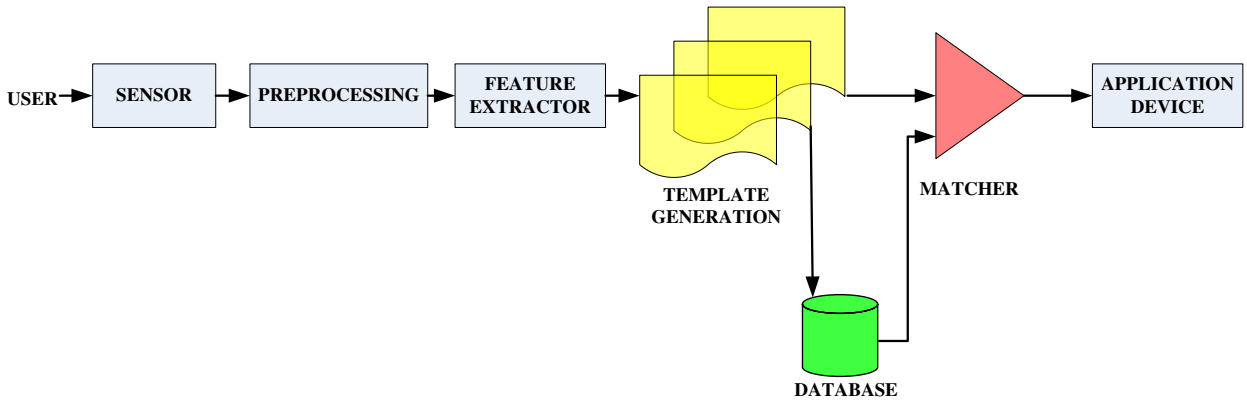


Figure 1: Biometric Authentication System

As shown in figure 1, biometric authentication requires comparing a template or identifier against a newly captured biometric sample. During the Enrollment, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison. Biometric recognition [2] can be used in Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. The major blocks of biometric authentication system includes a sensor interface, pre-processing module, feature extraction and a comparing algorithm for identifying a genuine user from a fraudulent intruder. There are various types of biometric identifiers such as [3]:

- Fingerprints wherein the patterns of friction ridges and valleys on an individual's fingertips are unique to that individual.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014
International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

- Face Recognition identifies a person by their facial image; it can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission.
- Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy and learned behavioral patterns. This incorporation of learned patterns into the voice templates has earned speaker recognition its classification as a "behavioral biometric."
- Iris Recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought unique. The iris patterns can be obtained through aoptical acquisition system. The technology works well in both verification and identification modes.
- Hand and Finger Geometry based biometric system measures either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand.
- Signature Verification uses the dynamic analysis of a signature to authenticate aperson. The technology is based on measuring speed, pressure and angle used by the person when asignature is produced.

The traditional authentication systems such as tokens, smart cards, magnetic stripe cards, photo ID cards, physical keys and so forth, has limitations such as [4]:

- They can be lost, stolen, duplicated, or left at home.
- Passwords can be forgotten, shared, or observed.

Using biometrics for identifying human beings offers some unique advantages [5]:

- They are fast
- Easy-to-use
- Accurate
- Reliable, and
- Less expensive authentication

Section II provides the advantages of fingerprint based authentication among other biometrics. Section III introduces the traditional system. The proposed system and design details are presented in Section IV. Results and conclusion is given in section V and VI respectively.

II. FINGER PRINT BASED AUTHENTICATION

Fingerprint based biometric authentication system usually works on three level [6]. As shown in the figure 2, the dark line that makes up a fingerprint is formed by the peaked portion of the friction-ridge skin and white space that is trough portion. The identification is based on the location and direction of the peak ending and splits in the peak path.

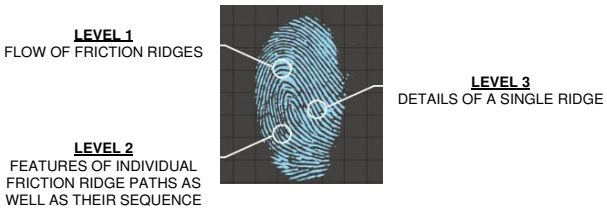


Figure 2: Three Level Fingerprint Identification Process

To compare the relative merits of fingerprint as a biometric, we can consider the following properties of a good biometric [7]:

- Universality - each person has the characteristic
- Uniqueness - the characteristic is unique per person
- Permanence - characteristic remains the same over time
- Collectability - how easy is it to measure the characteristic

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014
International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

- Performance - accuracy, speed, and resource requirements
- Acceptability - culturally accepted by the population
- Circumvention - robust against fraudulent attacks

III. TRADITIONAL TRANSACTION SYSTEM

Using automatic teller machine (ATM), a customer is able to conduct several banking activities such as cash withdrawal, money transfer, paying utility bills beyond official hours and physical interaction with bank staff. ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. Password or personal identification number (PIN) is one of important aspects in ATM security system which is commonly used to secure and protect financial information of customer from unauthorized access. The system works by comparing the code against a stored list of authorized passwords and users. Figure 3 shows a basic block module of an existing transactions system, wherein a front end GUI enables the user for its identification. Once authenticated, the customer is allowed for the transactions. Through the combination of Application servers and platform the entire transaction is completed.

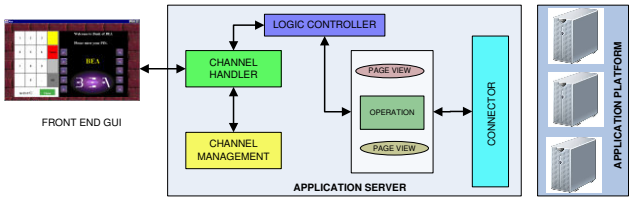


Figure 3: Traditional Card Based Transaction System

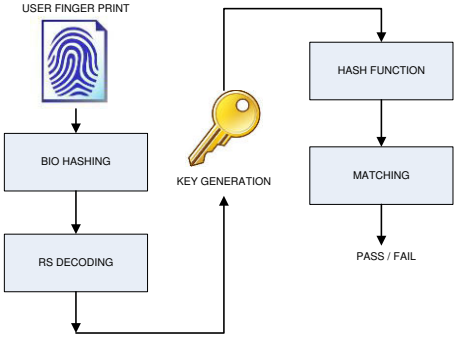
Such a system is secure in most of the cases by recent studies shows that the thefts have used sophisticated cracking algorithms to steal ATM holder's money. The traditional system has its own drawback such as [8]:

- Most commonly PINs are 4-digitnumbers in the range 0000-9999 resulting in 10,000 possible numbers, so that an attacker would need to guessan average of 5000 times to get the correct PIN.
- The strength of PIN as a security system is weakened since the likelihood of the code leaking to other people increased.

Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to financial transactions, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

IV. PROPOSED SYSTEM

Proposed system uses fingerprint of the user for authentication. This system works using a scanner, followed by a hashing algorithm and decoding. Each transaction generates a key which is verified from the database. Figure 4, shows a flow graph of such a system.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014
International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

Figure 4: Biometric Identification

The design of Biometric Based Transaction includes hardware description, software design and use of open source software development environment.

A. *Hardware description*

The hardware consists of a general purpose computer with following configuration- Pentium ® Dual Core CPU, 2.50 GHz, 2 GB RAM, VGA output and general interfaces like keyboard and mouse.

B.*Middleware – open source*

Middleware allows the application to directly interact with USB port Fingerprint scanners and execute functions through high level Application Programming Interface (API). As shown in figure 5, middleware provides a means to application programming and low level device interface.

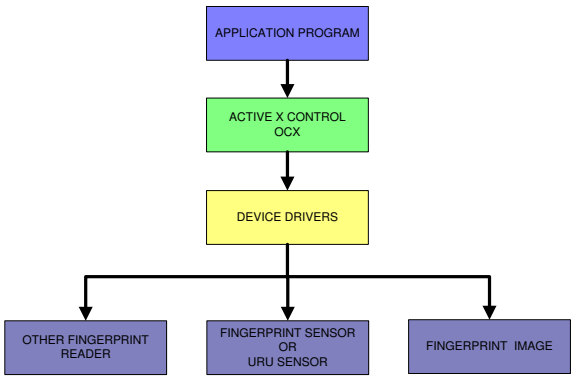


Figure 5: Middleware

It combines the 1: N fingerprint recognition engine and provides High Level Application Programming Interface which allows easy and swift implementation of software and User Interface. It provides an easy inter-operability.

C.*Software Design*

The software design encompasses the use of database, front end graphical user interface and middleware management.

D.*Database:*

Access stores all database tables, queries, forms, reports, macros and modules in the Jet database as a single file. For query development, Access offers a query designer, a graphical user interface that allows users to build query without knowledge of structured query language.Figure 6 shows the screen print of the database module.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014
International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

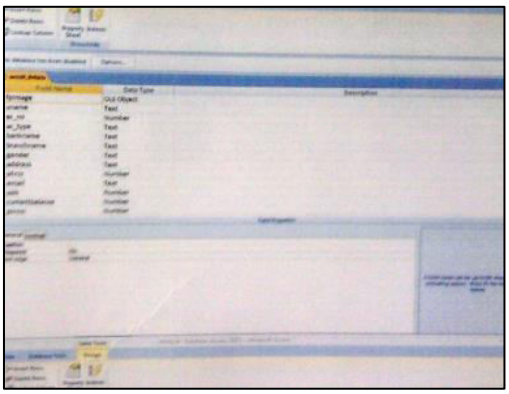


Figure 6: Database Management Screenprint

E. *Graphical User Interface:*

Visual Basic is used for the design of front end interaction program with the user. Figure 7 shows the pop up screen of the system.

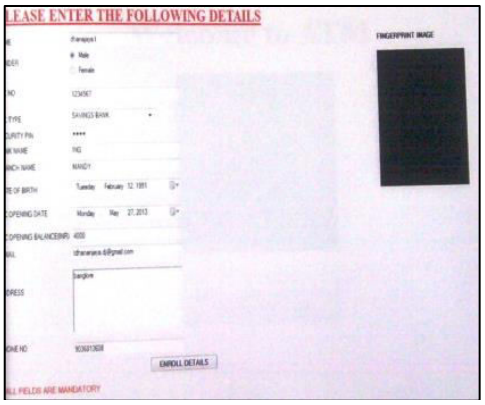


Figure 7: User Interface Module

F. *Middleware management:*

Read-in and Read-out finger print template is performed by the middleware. Fingerprints are saved and called by means of variant variables. Stored in one dimensional array and read by the database by method encoded template and method decode template.

V. RESULTS

The biometric based transaction system is designed using open source software development environment. The results are shown in table 1.

Table 1: Results

Typical Characteristics	Value
Template Size	310 or 1152 Byte
Rotation	0-360 degree
FAR	<=0.001%
FRR	<=2.0%
Registration Time	0.5 Second

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 2, May 2014
International Conference On Advances in Computer & Communication Engineering (ACCE - 2014)
on 21st & 22nd April 2014, Organized by
Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India

Average Verification Time	2500 pieces/ second
Image Quality	>=300 DPI

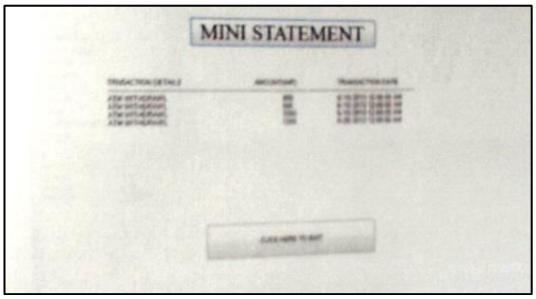


Figure 8: Successful Traction

Figure 8 shows a successful transaction performed by the user. Overall 20 customer database was used the experiment.

VI. CONCLUSION

Implementation of this software module will ease the customers in not carry many credit or debit cards to the ATM. The results indicates that this system is also used to provide security monetary transactions, where multiple account can be accessed using a single fingerprint by the account holder.

REFERENCES

1. Jain, A.K.; Ross, A.; Prabhakar, S., 'An introduction to biometric recognition', Circuits and Systems for Video Technology, IEEE Transactions on , vol.14, no.1, pp.4,20, Jan.2004.
2. SalilPrabhakar, SharathPankanti, Anil K. Jain, 'Biometric Recognition: Security and Privacy Concerns', IEEE Security & Privacy, vol. 1, no. 2, pp. 33-42, March-April 2003.
3. Dileep Kumar, YeonseungRyu, 'A Brief Introduction of Biometrics and Fingerprint Payment Technology', International Journal of Advanced Science and Technology Vol. 4, March, 2009.
4. Shimal Das, JhunuDebbarma, 'Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System', International Journal of Information and Communication Technology Research Volume 1 No. 5, September 2011.
5. Emilio Mordini, Sonia Massari, 'Body, Biometrics and Identity', Bioethics ISSN 0269-9702 (print); 1467-8519 (online) Volume 22 Number 9 2008 pp 488–498.
6. A.K. Sinha, 'Financial transactions get personalized and secure with biometrics.
7. Chien Le, 'A Survey of Biometrics Security'.