

# Multi-Usable Smart Card System using Embedded Controller

G.Sivasangari<sup>1</sup> P.Jamuna<sup>2</sup>

<sup>1</sup>P.G Scholar <sup>2</sup>Associate Professor

<sup>1,2</sup>Department of Electrical Engineering

<sup>1,2</sup>Nandha Engineering College (Autonomous), Erode-52

**Abstract**— The paper develops the Automatic Teller Machines process. Now a day’s usage of banking sector is essential to the people with a help of ATM Cards. In the proposed systems multiple ATM cards are merge into a one card is smart card. ARM7 plays a vital source and execute a certain task in an efficient process. The ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. Host computer is user side. Packets are transfer server to domain with a help connection establishment. LED display improves the clarity of color contrast. Efficiency of these display improve the quality and reduce the power consumption. Finger Print authentication system is a type of security system.

**Key words:** ARM7, LED, Ethernet, Host computer, Packets

## I. INTRODUCTION

In our electronically inter-connected society, reliable and user-friendly recognition and verification system is essential in many sectors of our life. The person’s physiological or behavioural characteristics, known as biometrics, are important and vital methods that can be used for identification and verification. Fingerprint recognition is one of the most popular biometric techniques used in automatic personal identification and verification.

Many researchers have addressed the fingerprint classification problem and many approaches to automatic fingerprint classification have been presented in the literature; nevertheless, the research on this topic is still very active. Although significant progress has been made in designing automatic fingerprint identification systems over the past two decades, a number of design factors (lack of reliable minutia extraction algorithms, difficulty in quantitatively defining a reliable match between fingerprint images, poor image acquisition, low contrast images, the difficulty of reading the fingerprint for manual workers, etc.) create bottlenecks in achieving the desired performance. Nowadays, investigating the influence of the fingerprint quality on recognition performances also gains more and more attention.

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. Each individual has unique fingerprints. Most fingerprint matching systems are based on four types of fingerprint representation schemes are grey scale image, phase image, skeleton image and minutiae. Due to its distinctiveness, compactness, and compatibility with features used by human fingerprint experts, minutiae-based representation has become the most widely adopted fingerprint representation scheme.

## II. OBJECTIVE

The main objective of the proposed model is,

- 1) To implement a multi usable smart card system for authentication purpose.

- 2) To merge the multiple ATM cards into one single card is smart card.

## III. METHODOLOGY

### A. Block Diagram

A block diagram of the circuit of a smart card with fingerprint authentication system is shown in figure 1.1. The main sections of this block diagram are described with their features.

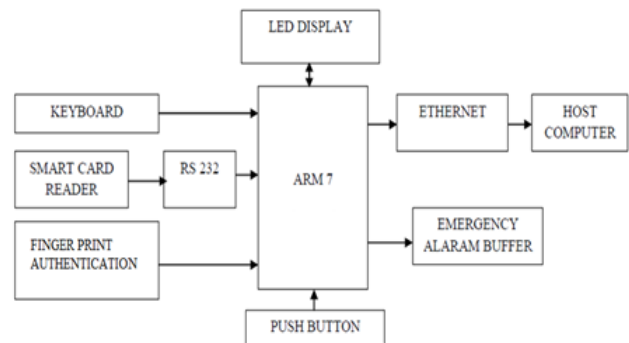


Fig. 1.1: block diagram of the circuit of a smart card with fingerprint authentication system

### B. Block Description:

#### 1) Keyboard:

A keyboard is a set of buttons arranged in a block or "pad" which usually bear digits, symbols and usually a complete set of alphabetical letters. If it mostly contains numbers then it can also be called a numeric keypad. Keypads are found on many alphanumeric keyboards and on other devices such as calculators, push-button telephones, combination locks, and digital door locks.

#### 2) Smart Card Reader:

Readers and terminals operate with smart cards to obtain card information and perform a transaction. Generally, a reader interfaces with a PC for the majority of its processing requirements. A terminal is a self-contained processing device.

#### 3) Fingerprint Imaging:

The image reconstruction can take place on a separate biometric microcontroller or directly on the host processor in a PC or mobile phone application. The complete fingerprint representation is built up line by line and recorded as the finger is swiped over the "single line" sensor array.

The image reconstruction can take place on a separate microcontroller or directly on the host processor in the case a PC or mobile phone applications as signified in the following figure 1.2. The patented, sensor specific image reconstruction principle is the core of IDEX' IP, and the basis for the user-friendly, robust, high-quality imaging offered by the Smart Finger technology.

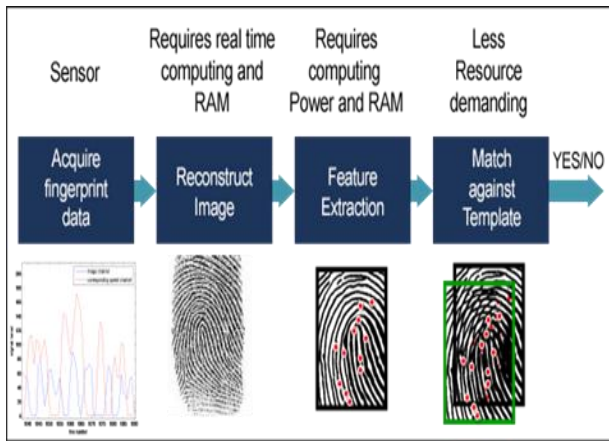


Fig. 1.2: Fingerprint Imaging System

#### IV. FINGERPRINT AUTHENTICATION

Fingerprint authentication based access control solution for enterprises, standalone systems, web applications and wireless networks. This mechanism eliminates the need to remember and type-in passwords each time you need to get access, possibility of fingerprints being lost, stolen or misused.

Fingerprints can be captured using any of the supported fingerprint sensors. Fingerprints captured are secure as only minutia points in them as specified in the following figure 1.3 are used for authentication and fingerprints cannot be developed using the extracted minutia.

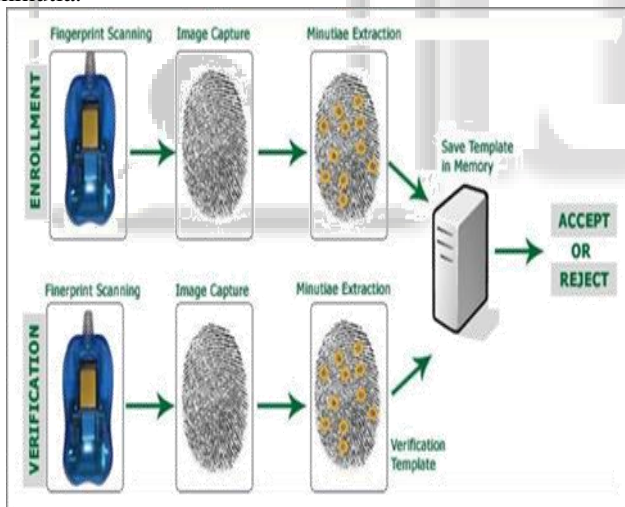


Fig. 1.3: Fingerprint Authentication System

#### V. HOST COMPUTER

A network host is a computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network layer host address.

Computers participating in networks that use the Internet Protocol Suite may also be called IP hosts. Specifically, computers participating in the Internet are called Internet hosts, sometimes Internet nodes. Internet hosts and other IP hosts have one or more IP addresses assigned to their network interfaces. The addresses are configured either manually by an administrator, automatically at start-up by means of the Dynamic Host

Configuration Protocol (DHCP), or by stateless address auto configuration methods.

Every network host is a physical network node (i.e. a network device), but not every physical network node is a host. Network devices such as modems, hubs and network switches are not assigned host addresses (except sometimes for administrative purposes), and are consequently not considered to be network hosts.

Network hosts that participate in applications that use the client-server model of computing are classified as server or client systems. Network hosts may also function as nodes in peer-to-peer applications, in which all nodes share and consume resources in an equitable manner.

#### VI. RESULTS

##### A. Simulation with Fingerprint Authentication:

The below figure 1.4 represents the output for an input image with authentication. This input, resized, preprocessed image and gabor output was taken as the reference image for find out the fingerprint authentication waveforms.

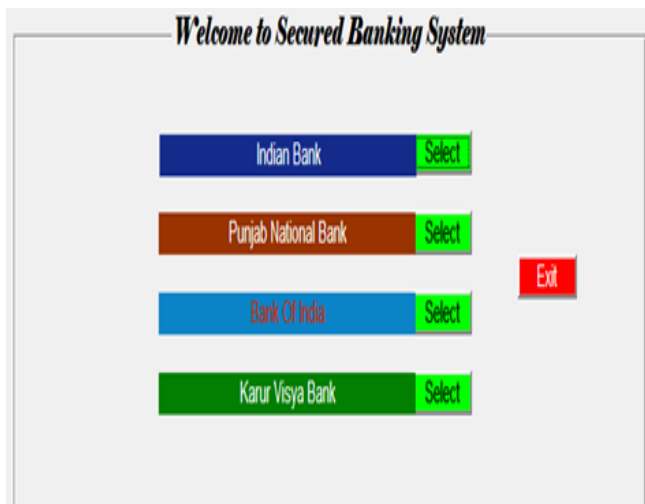
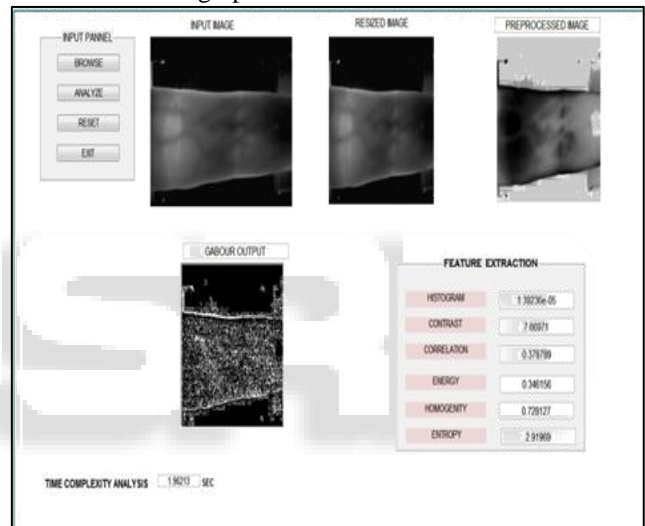


Fig. 1.4: Simulation Output with Authentication System

##### B. Simulation with Fingerprint Non-Authentication:

The below figure 1.5 represents the output for an input image with non-authentication. This input, resized, preprocessed image and gabor output was taken as the reference image for find out the fingerprint non-authentication waveforms.

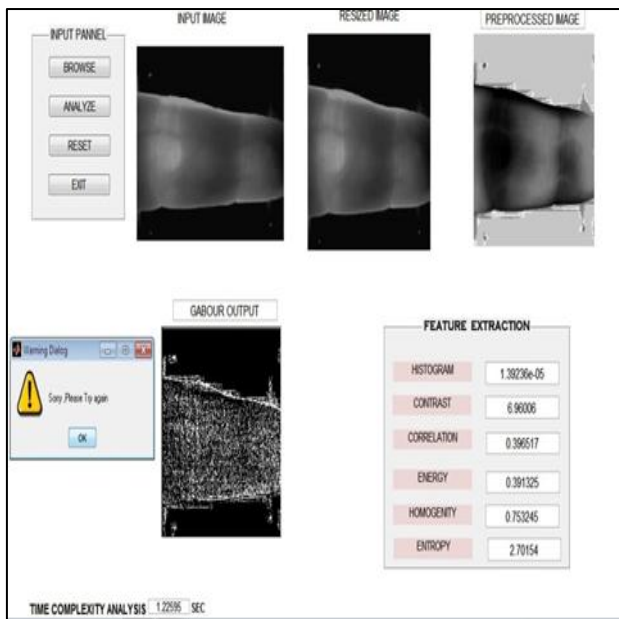


Fig. 1.5: Simulation Output with Non-Authentication System

## VII. CONCLUSION

Multiple bank accounts will maintain in a single bank account. That must be also in single smart card. RS232 make a connection among hardware. ARM7 plays an efficient task to operate. LCD display improves the quality. The edge point of fingerprint authentication can be detected by locating zero crossings of second derivative grey level profiles. However, the derivative filters are very sensitive to the accompanying noise. Therefore it is judicious to employ some pre-processing, such as averaging, to reduce the effect of noise. This two-step process was found to be quite effective for the localization of venous structure in the acquired fingerprint images.

## REFERENCES

- [1] G.Prabu, K.Tamilselvan, P.Prabhakaran, "Multiple Banking System Using ARM 7 TDMI Processor with Finger Print Authentication", February-2014.
- [2] Ch. S. L. Prasanna, M. Venkateswara Rao, "Design of  $\mu$ C/ Os-II RTOS Based Scalable Cost Effective Monitoring System Using Arm Powered Microcontroller", International Journal of Scientific and Research Publications, Volume 2, Issue 4, ISSN 2250-3153, April 2012.
- [3] Dong Sik Kim, Sung-Yong Son and Jeongjoon Lee, "Developments of the In-Home Display Systems for Residential Energy Monitoring", IEEE Transactions on Consumer Electronics, Vol. 59, No. 3, August 2013.
- [4] Edit Toth-Laufer and Annamaria R. Varkonyi-Koczy, "A Soft Computing-Based Hierarchical Sport Activity Risk Level Calculation Model for Supporting Home Exercises", IEEE Transactions On Instrumentation And Measurement, Vol. 63, No. 6, June 2014.
- [5] Francesco Caimmi, Stefano Mariani, Marco De Fazio, and Paolo Bendiscioli, "Investigation of the Effectiveness and Robustness of an MEMS-Based

Structural Health Monitoring System for Composite Laminates", IEEE Sensors Journal, Vol. 14, No. 7, July 2014.

- [6] Indersain, Neetika Sharma, Dushyant Singh, "Design and Implementation of  $\mu$ C/Os II Based Embedded System Using ARM Controller", International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-1, Issue-2, April 2013.