SECURITY SYSTEM FOR ATM TERMINAL BY USING BIOMETRIC TECHNOLOGY AND GSM

CH S N Sirisha Devi[(1)] *Maya patil*[(2)]
(1) & (2) Department of Electronics and Communication Engineering
Sridevi Women's Engineering College Gandipet, Hyderabad

Abstract: *This paper proposes a design, to add more security to the current ATM terminals by using biometric and GSM technology. The design of ATM Terminal based on Finger Print Recognition System and GSM will give two way securities for the customers first the authentication process with the help of customer fingerprint and then second the system sends the dynamically generated PIN number to customer's personal mobile number.*

Keywords*-ATM terminal, ARM9; fingerprint recognition, image enhancement GSM MODEM.*

I. INTRODUCTION

Now-a-days, in the self- service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. Using the ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is very common. In the existing design it is designed by using ATM card only and ATM machine is activated by placing the card and then entering the pin number of the particular card but this system is not safe to use because anybody can access the system if they have the card and pin number like we share our card and pin number to our friends who may miss use it this is the main disadvantage of this system. The main objective of this system is to develop an embedded system, which is used for ATM security applications. In these systems, Bankers will collect the customer finger prints and mobile number while opening the accounts then customer only access ATM machine. The working of these ATM machine is when customer place finger on the finger print module when it access automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the micro controller. The code received by the customer should be entered by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access.

II. THE CHARACTERISTICS OF THE SYSTEM DESIGN

The embedded ATM client authentication system is based on fingerprint recognition which is designed after analyzed existed ATM system. The S3C2440 chip is used as the core of these embedded systems which is associated with the technologies of fingerprint recognition and current high speed network communication.

The primary functions are shown as follows:

- Fingerprint recognition: The masters' fingerprint information was used as the standards of identification. It must certify the feature of the human fingerprint before using ATM system.
- Remote authentication: System can compare current client's fingerprint information with remote fingerprint data server.
- Message alarming: Different 3-digit code as a message to the mobile of the authorized customer without any noise, in order to access the Terminal.

III. Hardware Design

The S3C2440 chip is used as the core of entire hardware. Furthermore, the modules of LCD, keyboard, alarm, fingerprint recognition are connected with the main chip (S3C2440).The SRAM and FLASH are also embodied in the system. There are some modules consisted of the system as follows

- LCD module: The OMAP5910 is used in this module as a LCD controller, it supported 1024*1024 images of 15 gray-scale or 3375 colors.
- Keyboard module: It can be used for inputting passwords.
- Fingerprint recognition module: FIM3030 fingerprint module is used for recognition of fingerprints. This module uses optical sensor

for capturing and detecting of fingerprint images.

- GSM Modem: A GSM modem exposes an interface that allows sending and receiving messages over the modem interface.

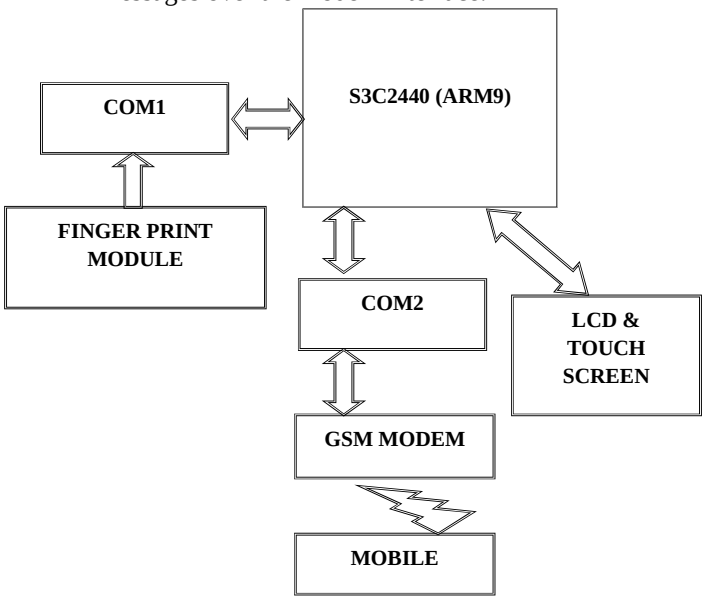

Figure1: The block diagram of hardware

Before using the ATM terminal, the client's fingerprint feature will be connected to the remote fingerprint data

Server to match fingerprint data with the master's, if the result isn't correct, the system will call police automatically and send alarm to the credit card owner. The block diagram of hardware design is shown in figure 1.

IV. SOFTWARE DESIGN

The system operates in below two modes.

Admin mode*:* In this mode the user finger print and mobile number are collected and saved to database before opening the account

User mode*:* In this mode the user finger print is validated with the database for the identification which is required to perform transactions.

This system of software is implemented by the steps as follows: first of all, the Linux kernel and the File system are loaded into the main chip. The next, the system is initialized to implement specific task, such as checking ATM system, GSM communication and so on, and then each module reset for ready to run commands. Before using ATM terminal, the mobile number and fingerprint of the customer is required.

Figure2: The overall flow chart of software

First the system is required the owner's fingerprint. If all the recognition is right, the system would send password to the Account holder and he will enter the same password in touch screen for accessing the ATM Terminal. If authentication Failure then it sends the alert message to the Account holder and Bank The overall flow chart of software is shown in figure 2.

In the process of inputting fingerprint, the FIM3030 fingerprint module is used for recognition of fingerprints. This module uses optical sensor for capturing and detecting of fingerprint images. The fingerprint information will be temporarily stored in SRAM and upload to the remote finger data server to compare through bank network. The result of process will be controlled by main chip (S3C2440)

C. FINGERPRINT RECOGNITION PROCESS

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns,

which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns.[1] It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

Patterns

The three basic patterns of fingerprint ridges are the arch, loop, and whorl:

***Arch*:** The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.

***Loop*:** The ridges enter from one side of a finger, form a curve, and then exit on that same side.

***Whorl*:** Ridges form circularly around a central point on the finger or field that is defined as the tangential vector of the fingerprint ridge curves is disclosed.

Fingerprint processing has three primary functions: enroll, search, and verify.

- ***Enrollment*** acquires a fingerprint image from the sensor and saves it in SRAM. The image is processed, enhanced, and compressed to create a fingerprint template. Various filters clean up the image and convert it to a mathematical representation, making it impossible to steal a template and directly recreate a fingerprint image.
- ***Search*** compares a raw candidate image to a list of previously enrolled templates. Through a series of screening processes, the algorithm narrows the list of templates to a manageable size. Those templates that survive screening are compared to the candidate and verification scores are provided. A score exceeding a preset threshold indicates a positive identification.
- *Verification* validates a user's identity by comparing a raw candidate image to a previously enrolled template via real-time, closed-loop pattern-matching algorithms. A score is returned indicating the similarity of the candidate and template to generate a yes/no match decision.

Fingerprint Recognition Algorithm:

To verify the identity of a user by automatically extracting minutiae from his or her fingerprint image, a fingerprint recognition algorithm is required. The fingerprint recognition algorithm is composed of two main technologies: image processing technology that captures the characteristics of the corresponding fingerprint by having the image under-going several stages, and matching algorithm technology that authenticates the identity by comparing feature data comprised of minutiae with Templates in a database.

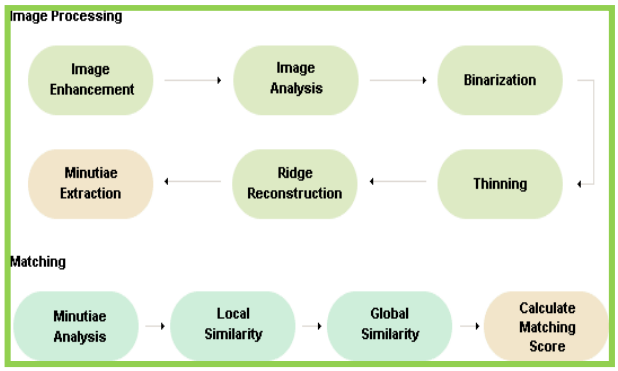

Figure.4: Block map of the fingerprint recognition algorithm consisting of the two Technologies

V. GSM

Global System for Mobile Communications (GSM: originally from Group Special Mobile) is the most popular standard for mobile phones in the world. Its promoter, the GSM Association, estimates that 82% of the global mobile market uses the standard GSM is used by over 2 billion people across more than 212 countries and territories. GSM differs from its predecessors in that both signaling and speech channels are digital call quality, and thus is considered a second generation (2G) mobile phone system. This has also meant that data communication was built into the system using the 3rd Generation Partnership Project (3GPP).

GSM uses a variation of Time Division Multiple Access (TDMA) and GSM is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizers and compresses data then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1,800 MHz frequency band. GSM is the de facto wireless telephone standard in Europe. GSM has over one billion users worldwide and is available in 190 countries.

Technical details:

GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges.

Most GSM networks operate in the 900 MHz or 1800 MHz bands. Some countries in the Americans (including Canada and the United States) use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated. The rarer 400 and 450 MHz frequency bands are assigned in some countries, notably Scandinavia, where these

frequencies were previously used for first-generation systems.

The Future of GSM

GSM together with other technologies is part of an evolution of wireless mobile telecommunication that includes High-Speed Circuit-Switched Data (DSCSD),
General Packet Radio System (GPRS), Enhanced Data rate for GSM Evolution (EDGE), and Universal Mobile Telecommunications Service (UMTS)

VI. RESULTS AND CONCLUSIONS

The Implementation of ATM security by using fingerprint recognition and GSM MODEM took advantages of the stability and reliability of fingerprint characteristics. Additional, the system also contains the original verifying methods which were inputting owner's password which is send by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use.

VII. REFERENCES

[1]Lin Hong, Wan Yifei, Anil Jain. Fingerprint image enhancement: algorithm and performance evaluation[J]. IEEE Transactions on Pattern Analysis and Machine intelligence. 1998,20(8): 777-789.
[2]ESaatci, V Tavsanogh. Fingerprint image enhancement using CNN gabor-Cpe filter[C]. Proceedings of the 7th IEEE International Workshop on Cellular Neural Networks and their Applications 2002: 377-382.
[3]GU J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition, 2004, 37: 543-553.
[4]Cheng J, Tian J. Fingerprint enhancement with dyadic scale-space. Pattern Recognition Letters, 2004, 25(11): 1273-1284.
[5]Aditya Abhyankar, Stephanie Schuckers, “Towards integrating level-3 Features with perspiration pattern for robust fingerprint recognition,” in Proceedings of 2010 IEEE 17th International Conference on Image Processing, September 26-29, 2010, Hong Kong.