ENHANCING ATM SECURITY USING FINGERPRINT RECOGNITION AND GSM

S.KANCHANA, K.KRITHIKA
[1]11L122,III BE ECE,PSG COLLEGE OF TECHNOLOGY,COIMBATORE.

Abstract

The main objective our idea is to develop an ATM system using fingerprint access, which improves the security of using ATM. 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 microcontroller. 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.

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

1.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 provide customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years, a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. In recent years, the algorithm that the fingerprint recognition continuously updated and sending the four digit code by the controller which has offered new verification means for us, the original password authentication method combined with the biometric identification technology verify the clients' identity better and achieve the purpose that use of ATM machines improve the safety effectively.

2. 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 system 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 4-digit code as a message to the mobile of the authorized customer without any noise, in order to access the Terminal.
- Two discriminate analysis methods: Besides the fingerprint recognition, the mode of password recognition can be also used for the system.

3.Why biometrics fingerprint

A.Advantages

- Uniqueness
- Surety over the Cards and Keypads
- Against to Cards Duplication, misplacement and improperdisclosure of password
- No excuses for RF/Magnetic Cards forget ness
- No need to further invest on the Cards Cost

B. Comparison between all biometrics

The use of fingerprints as a biometric is both theoldest mode of computer-aided, personal identification and the most prevalent in use today . In the world today,fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others. They are also used for controlling access to highly secured places like offices, equipment rooms, control centers and so on . The result of the survey conducted by the International Biometric Group (IBG) in 2012 on comparative analysis

of fingerprint with other biometrics is presented in Figure. 2

The result shows that a substantial margin exists betweethe uses of fingerprint for identification over other biometrics such as face, hand, iris, voice, signature and middleware.

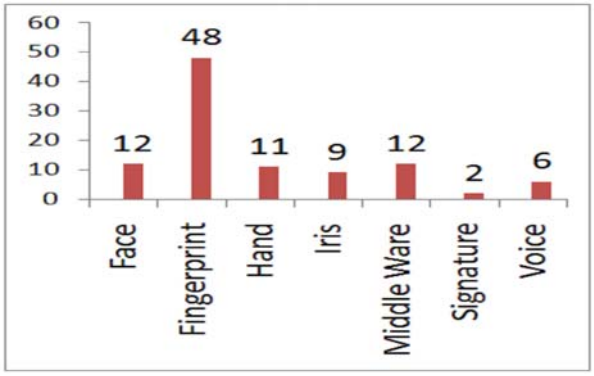


Fig.1. Comparative survey of fingerprint with other Biometrics

The row for the eye biometric describes features applying toeither iris or retinal scanning technologies.

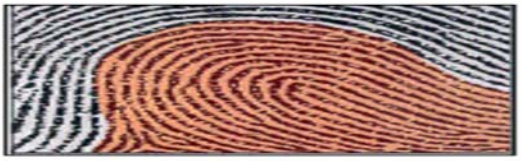
- All technologies are appropriate for 1-to-1matching, only fingerprint and eye technologies are proven to have acceptable recognition rates to be practical for 1-to-many matching. This is an indication that these two modalities provide the highest recognition rates for verification as well.
- Variation of the salient features used for recognition is very different for different modalities. Fingerprint and eye features remain consistent for a lifetime, whereas the others change with growth. On a day-to-day basis, there is far less variation for all modalities, though voice can change with illness and signature with demeanor.
- As far as sensor cost, eye systems are currently more costly than the others; voice systems can be zero cost to the user if a telephone is used.
- Fingerprint and voice systems have the smallest comparative sizes with eye systems currently the largest.

4.Introduction of Fingerprint

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider useof the term, fingerprints are the traces of an impression from the friction ridges of any part of a human hand. A friction ridge is a raised portion of the epidermis on the fingers and toes (digits), the palm of the hand, consisting of one or more connected ridge units of friction ridge skin. These are sometimes known as "epidermal ridges" which are caused by the underlying interface between the dermal papillae of the dermis and the interpapillary (rete) pegs of the epidermis. These epidermal ridges serve to amplify vibrations triggered, for example,when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. These ridges also assist in gripping rough surfaces, as well as smooth wet surfaces.Impressions of fingerprints may be left behind on a surface by the natural secretions of sweat from the eccrine glands that are present in friction ridge skin, or they may be made by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of thefingers.

5.Fingerprints for Identification

Classifying fingerprints Beforecomputerisation replaced manual filing systems in large fingerprint operations, manual fingerprint classification systems were used to categorize fingerprints based on general ridge formations (such as the presence or absence of circular patterns on various fingers), thus permitting filing and retrieval of paper records in large collections based on friction ridge patterns alone. The most popular ten-print classification systems include the Roscher system, the Juan Vucetich system, and the Henry Classification System. Of these systems, the Roscher system was developed in Germany and implemented in both Germany and Japan, the Vucetich system (developed by a Croatian-born Buenos Aires Police Officer) was developed in Argentina and implemented throughout South America, and the Henry system was developed in India and implemented in most English-speaking countries. In the Henry system of classification, there are three basic fingerprint patterns: Loop, Whorl and Arch, which constitute 60–65%, 30–35% and 5% of all fingerprints respectively. There are also more complex classification systems that break down patterns even further, into plain arches or tented arches,and into loops that may be radial or ulnar, depending on the side of the hand the tail points towards. Whorls may not have subgroup classifications it including only plain whorls.



LOOP

In a loop pattern, the ridges enter from either side, re-curve and pass out or tend to pass out the same side they entered.

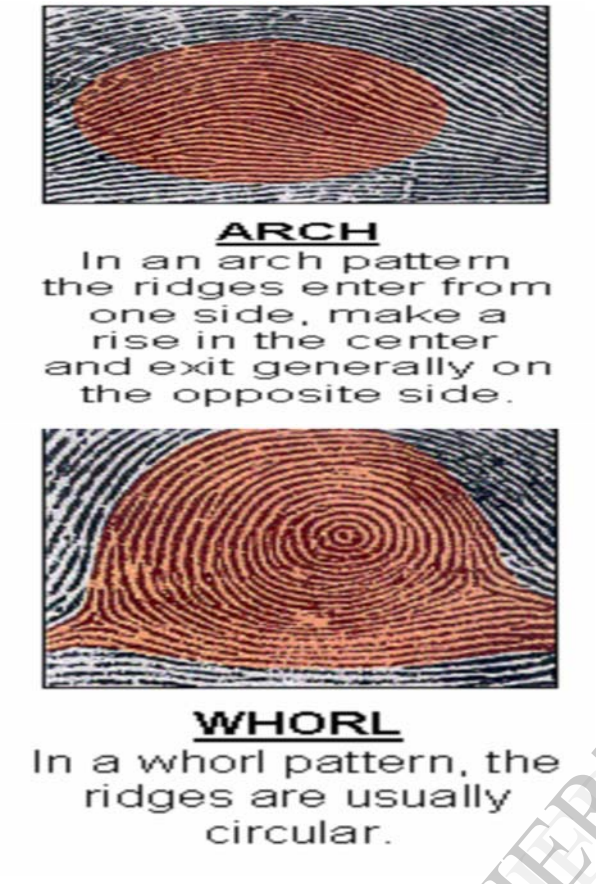


Fig.2 CharacteristicsOf Fingerprint

6.Hardware design and Software design

The design of entire system consisted of two part which are hardware and software. The hardware are designed by the rules of embedded system, and the steps of software consisted of three parts. The more details are shown as follows

A. 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

SRAM and FLASH: The 16-bit 29LV160BB- 70REC of FLASH chip and the 32-bit HY57V561620CT-6 of SRAM chip are connected with the main chip. Their functions are storing the running code, the information of fingerprint and the algorithm.

- LCD module: The OMAP5910 is used in this module as a LCD controller, it supported 1024*1024 image of 15 gray-scale or 3375 colours.
- keyboard module: It can be used for inputting passwords.
- Fingerprint recognition module: Atmel Company's AT77CI04B be used as a fingerprint recognition. It has a 500dpi resolution, anti-press, anti-static, anticorrosion.
- Ethernet switch controller: RTL8308B can provides eight 10/100 Mbps RMII Ethernet ports, which can connect police network and remote fingerprint data server.

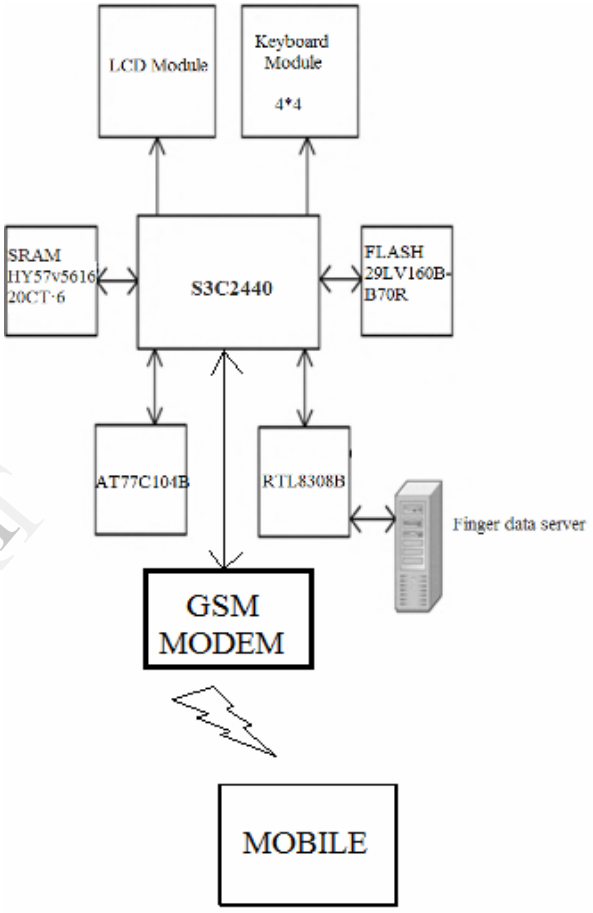


Figure 3. The block diagram of hardware

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 3.

B. Software design

The design was component of three parts included the design of main program flow chart, the initializing ones, and the algorithm of fingerprint recognition flow chart. 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.

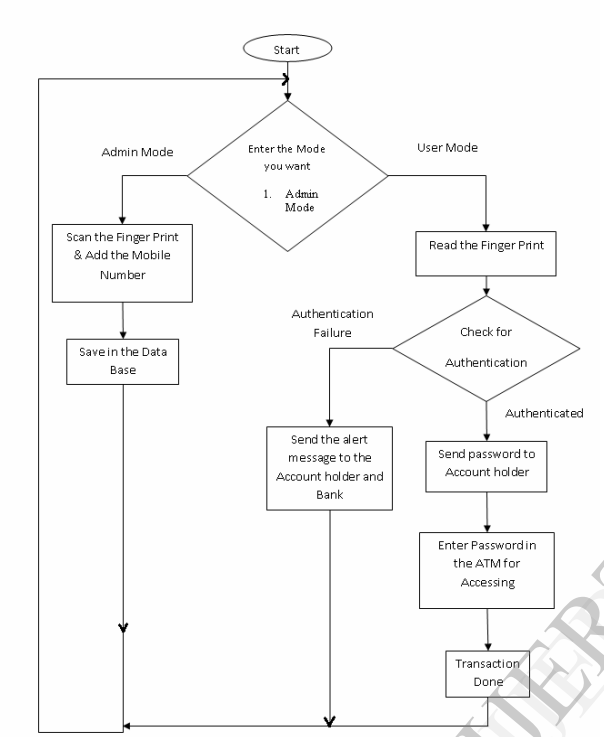


Figure 4. The overall flow chart of software

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 send the alert message to the Account holder and Bank. The overall flow chart of software is shown in figure 4.

In the process of inputting fingerprint, the AT77CI04B which is a linear sensor that captures fingerprint images by sweeping the finger over the sensing area, will used for acquiring the image of fingerprint. This product embed true hardware based 8-way navigation and click functions. 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).

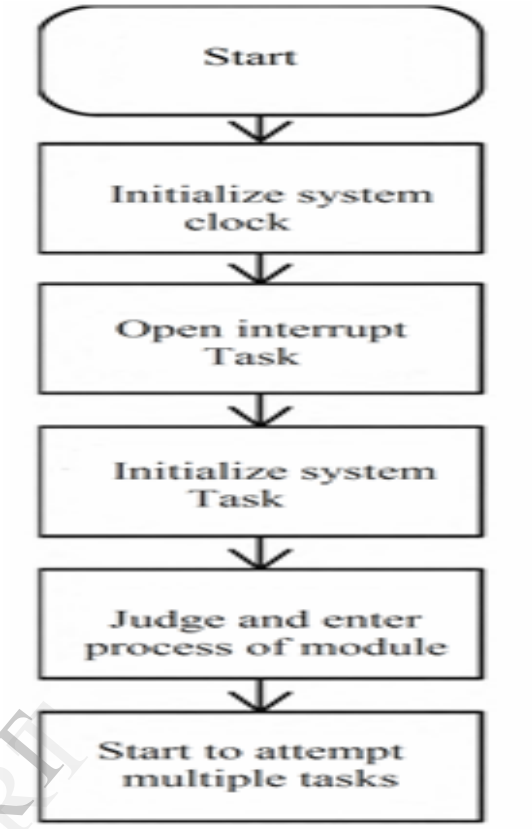


Figure 5. The flow chart of fingerprint recognition

The initializing process means that set the hardware and software and then start the multiple mission module, each module will be started according to the priority processes. At first, initialize the system clock, and execute the codes of open interrupt and the open interrupt task. Then, the system would judge and enter process of module. finally, the system would start to attempt multiple tasks. The initializing flow chart is shown in figure 5.

C. The design of fingerprint recognition algorithm

The design of algorithm based on fingerprint recognition is so vital for the whole system. We would approach two steps to process the images of fingerprint.

1) The detail of fingerprint recognition process**.**

The first step was the acquisition of fingerprint image by above device mentioned in the algorithm, and the results could be sent to the following process. secondly, pre-processing the images acquired. After obtain the fingerprint image, it must be pre-processing. Generally, pre-processing of one's is filtering, histogram computing, image enhancement and image binarization. Lastly, the characteristic value was extracted, and the results of the above measures would be compared with the information of owner's fingerprint in the database so as to verify

whether the character is matched, and then the system returned the results matched or not.

2) The design of fingerprint image enhancement

Fingerprint recognition module is an extremely important part of the system, the high-quality images was the major factors of influencing the performance in the system. The algorithm of fingerprint recognition based on the algorithm of Gabor and direction filter was used. fingerprint enhancement algorithm based on Gabor filter could be better to remove noise, strengthen the definition between the ridge and valley, it could significantly improve the image enhancement processing capacity, but this algorithm was slow in dealing with the high capacity requirements.

7.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 also pioneered a low-cost alternative to voice calls, the Short message service. GSM is a digital mobile telephone system that is widely used in Europe and other parts of the world.

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.

A. 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.

B.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).

8.Conclusion

Secured access to ATM using fingerprint recognition and GSMtook advantages of the stability and reliability of fingerprint characteristics. Additional, the system also contains the original verifying methods which was 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 is safe, reliable and easy to use.

REFERENCES

1. “Integrated Electronics: Analog and Digital Circuits and System” by Jacob Millman and Christos C.Halkias.
2. “The 8051 Microcontroller and Embedded Systems” by Muhammad Ali mazidi, Janice GillipseMazidi and RolinD.McKinlay
3. “Digital Image Processing” byRafael C. Gonzalez and Richard E. Woods
4. http://www.wikipedia.org
5. http://www.ece.ubc.ca
6. http://www.electrodesales.com