

Real Time Sms-Based Hashing Scheme for Securing Financial Transactions on Atm Terminal

P. Prem Kishan¹, Neerugatti Vishwanath², Vasudheva Reddy Nandigama³, Sk. Khamuruddeen⁴, Anirudh Kasibhatla⁵, D.Pavani⁶, G.Swetha⁷

¹(Assistant professor, Department of ECE, ST. MLR INSTITUTE OF TECHNOLOGY Laxma Reddy College, Hyderabad)

²(Assistant professor, Department of ECE, ST. Peters Engineering College, Hyderabad)

³(Assistant professor, Department of ECE, ST. MLR INSTITUTE OF TECHNOLOGY Laxma Reddy College, Hyderabad)

⁴(Assistant Professor, Department of ECE, HITAM, Hyderabad, India)

⁵(B. Tech III year, Department of ECE, HITAM, Hyderabad, India)

⁶(B. Tech III year, Department of ECE, HITAM, Hyderabad, India)

⁷(Associate Professor, Department of ECE, ACTS, Hyderabad)

Abstract- The purpose of this project is to increase the security that customer use the ATM machine. 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, so to rectify this problem we are implementing this project. Now a days 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, 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.

Keywords-ATM terminal; ARM9; fingerprint recognition; image enhancement; Gabor filtering

I. INTRODUCTION

With the development of computer network technology and e-commerce, the self-service banking system has got extensive popularization with the characteristic offering high-quality 24hours service for customer. Nowadays, using the ATM (Automatic Teller Machine) which provides 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, 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.

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.

Telephone alarming: Once an exception happens, such as log in as the fake identity, the system will start the phone alarm to inform client and bank staff as soon as possible.

Message alarming: the message can be send to the relevant staffs mobile phone without any noise, in order to carry on emergency processing.

Police network connection: The system can call the police via the police network.

Two discriminant analysis methods: Besides the fingerprint recognition, the mode of password recognition can be also used for the system.

III. 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:

- LCD module: The OMAP5910 is used in this module as a LCD controller, it supported 1024*1024 image of 15 gray-scale or 3375 colors.
- Keyboard module: It can be used for inputting passwords.
- Alarming module: TC35i alarming module is based on GSM technology implement which can call the credit card owner and send message to relevant staffs without any sound.
- 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.
- Fingerprint recognition module: Atmel Company's AT77CI04B be used as a fingerprint recognition. It has a 500dpi resolution, anti-press, anti-static, anti- corrosion.
- Ethernet switch controller: RTL8308B can provides eight 10/1 00 Mbps RMI Ethernet ports, which can connect police network and remote fingerprint data server.

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.

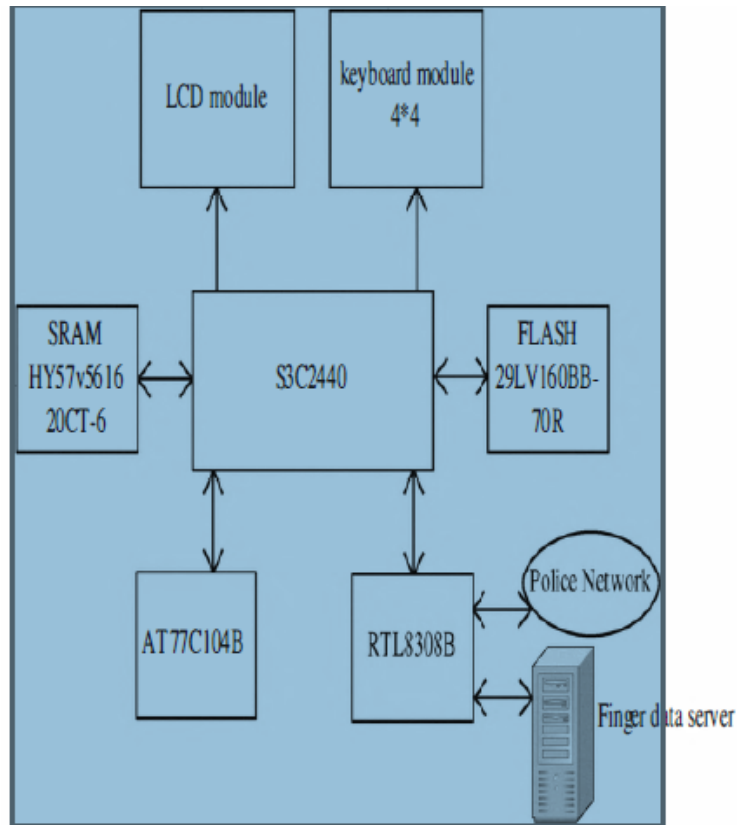


Figure 1. The block diagram of hardware

B. Software design

The design of software is very important for this embedded system. 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 A TM system, GSM communication and so on, and then each module reset for ready to run commands.

Before using A TM terminal, the password and fingerprint is required. First need to enter owner's password, if password is successful then the system is required the owner's fingerprint. If all the recognition is right, the system would enter into the waiting status. In addition, the number of times that recognition of fingerprint and password are restricted to 3. If more than 3 times, the system will call the police through police network, telephone to the owner and send message to relevant staff. Then locked the owner's credit card. The overall flow chart of software is shown in figure 2.

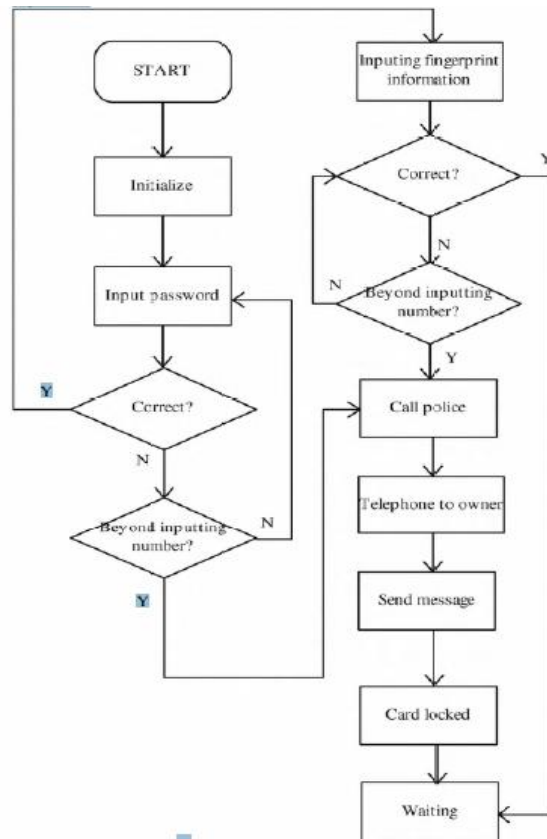


Figure 2. The overall flow chart of software

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 be used for acquiring the image of fingerprint. These products 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).

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 3.

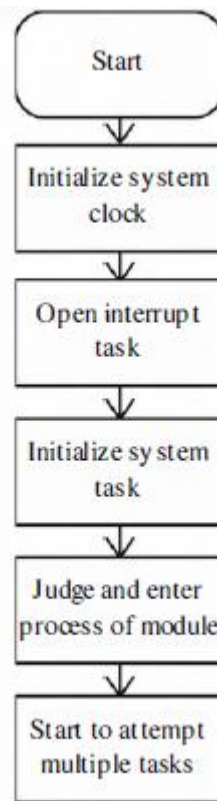


Figure 3. The flow chart of fingerprint recognition

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 ones 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. There is a lot of noise in fingerprint image, the image enhancement was the precondition for recognition of fingerprint characteristics. The algorithm of fingerprint recognition based on the algorithm of Gabor and direction filter was used. Finger print 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. Fingerprint enhancement algorithm based on direction filter has a faster processing capabilities, but it was not good to handing the large noise areas. so combination of these two algorithms could obtain better effects. The algorithm based on direction filter was used in the clear area, and based on Gabor filter was used in the recoverable region.

a) The Gabor filter algorithms

For each point, according to its frequency, direction, using formula(1) calculate the Gabor filter coefficients, calculate the filter values of each point and then ,move to the next point, repeat the process above.

$$h(x, y, \theta, f) = \exp \left[-\frac{1}{2} \left(\frac{x'^2}{\delta_x^2} + \frac{y'^2}{\delta_y^2} \right) \right] \cos(2\pi f x') \quad (1)$$

Besides,

$$x' = x \sin \theta + y \cos \theta \quad (2)$$

$$y' = x \cos \theta - y \sin \theta \quad (3)$$

b) The direction filter algorithms

For each point, according to its frequency, direction, using formula (4) on the clear fingerprint image area.

$$h(x, y) = \sum_{u=-3}^3 \sum_{v=-3}^3 G(x+u, y+v) g(u, v) \quad (4)$$

$$h(x, y, \theta, f) = \exp \left[-\frac{1}{2} \left(\frac{x'^2}{\delta_x^2} + \frac{y'^2}{\delta_y^2} \right) \right] \cos(2\pi f x') \quad (1)$$

Besides,

$$x' = x \sin \theta + y \cos \theta \quad (2)$$

$$y' = x \cos \theta - y \sin \theta \quad (3)$$

b) The direction filter algorithms

For each point, according to its frequency, direction, using formula (4) on the clear fingerprint image area.

$$h(x, y) = \sum_{u=-3}^3 \sum_{v=-3}^3 G(x+u, y+v) g(u, v) \quad (4)$$

$G(u, v)$ is normalized after the fingerprint image, $g(u, v)$ as a template filter coefficient.

Proposed image block average M , the calculation using image block average gray level range, if the mean was small, the variance was small, that is not to restore area; if the mean moderate, have a great variance, the smaller the ratio of mean and variance, it could be regard as the clear area; if the mean moderate, variance and they were smaller than the ratio of non-recovery area, it could be regard as confusion region. Image block average calculated as follows: The fingerprint image was divided into $w \times w$ area, using equation (5), (6) in each of a gray-scale mean and variance, And the statistics is greater than the number of M , marked as m and less than the number of M , marked as n .

$$\text{if } |m - n| > w^2, \bar{M} = \begin{cases} \bar{M} - \theta & m < n \\ \bar{M} + \theta & m \geq n \end{cases} \quad (5)$$

θ is very small,

$$M(n, m) = \frac{1}{w^2} \sum_{u=1}^w \sum_{v=1}^w h[w(n-m)+u, w(m-m)+v] \quad (6)$$

$$N(n, m) = \frac{1}{w^2} \sum_{u=1}^w \sum_{v=1}^w \{h[w(n-m)+u, w(m-m)+v] - M(n, m)\}^2 \quad (7)$$

IV. CONCLUSIONS

The design of ATM terminal system based on fingerprint recognition took advantages of the stability and reliability of fingerprint characteristics, a new biological technology based on the image enhancement algorithm of Gabor and direction filter. Additional, the system also contains the original verifying methods which was inputting owner's password. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was build on the technology of embedded system which makes the system more safe, reliable and easy to use.

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.
- [1] Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition,2004,37: 543-553.
- [2] Cheng J, Tian J. Fingerprint enhancement with dyadic scale-space. Pattern Recognition Letters, 2004,25(11): 1273-1284.
- [3] Chen H, Tian J. A fingerprint matching algorithm with registration pattern inspection. Journal of Software,2005,16(6): 1046-105.
- [4] Smits G FJordaan E M.Improved SVMRegression using Mixtures of Kernels[A]. Proceedings of the 2002 International Joint Conferenceon Neural Networks[C]. Hawaii: IEEE. 2002. 2785-2.
- [5] FU Zhenghua, LI Yongjun, Tian Mi(2007). "The embedded monitoring system based ARM". JOURNAL OF INSTRUMENT TECHNOLOGY, Vol. 07,No. Ipp. 01-2.
- [6] Jun Zhou, Guangda Sua, Chun hongJiang. A face and fingerprint identity authentication system based on multi-route detection. Neurocomputing 70 (2007)922-931.

AUTHORS:



1.P.Prem Kishan working as an Assistant Professor in MLRIT, His area of interest is VLSI & Signal processing.



2.Neerugatti Viswanath working as Assistant Professor in ST. Peters college of Engineering, Hyderabad and his area of interest is signal processing and communication engineering.



3. MR.VASUDHEVA REDDY NANDIGAMA working as an Assistant Professor in MLRIT, His area of interest is VLSI & Signal processing.



Mr.SK. Khamuruddeen working as an Assistant Professor in Hyderabad Institute of Technology & Management, His area of interest is VLSI & System Design.



Mr. ANIRUDH KASIBHATLA B. Tech III year, Department of ECE, HITAM area of interest Communications,VLSI.



Ms.D.PAVANI B.Tech III year, Department of ECE, HITAM area of interest Communications,VLSI.



Mrs. G.Swetha as an Associate Professor in ACTS, her area of interest is communications, VLSI & Antenna theory.