Indian Journal of Science and Technology

Supplementary Article

ATM Terminal Design using Biological Technology

V. Khanaa[1]* and Krishna Mohanta[2]

[1]Dean, Information Technology, Bharath University, Chennai-600073, India; drvkannan62@yahoo.com
[2]Department of CSE, Sri Sai Ram Engg. College, Leo Nagar, Chennai-600044, India; krishnamohanta@gmail.com

Abstract

The traditional Automatic Teller Machine (ATM) terminal customer recognition systems only rely on bank cards, passwords, and such identity verification methods which measures are not perfect and functions are too single.

For solving the bugs of traditional ones, using a Biological Technology in new ATM terminal customer recognition systems (i.e.) fingerprint Mechanism. The chip of S3C2440 is used for the core of microprocessor in ARM9, furthermore, an improved enhancement algorithm of fingerprint image increase the security that customer use the ATM machine.

Keywords: ATM Terminal, ARM9, Fingerprint Recognition, Image Enhancement, Gabor Filtering.

1. 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 24 hours service for customer. Nowadays, using the ATM (Automatic Teller Machine) which provides customers with the convenient banknote, trading becomes easier.

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.

In recent years, with the help of algorithm, 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 [1–5].

2. The Characteristics of the System Design

The embedded ATM client authentication system is based on fingerprint recognition which is designed after analyzing existing ATM system. The S3C2440 chip is used as the core of this embedded system which is associated with the technologies of finger print 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 exceptions happen, 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.

*Corresponding author:
V. Khanna (drvkannan62@yahoo.com)

- Message alarming: the message can be send to the relevant staff's mobile phone without any noise, in order to carry onemergency processing.
- Police network connection: The system can call the police via the police network.
- Two discriminate analysis methods:

Besides the fingerprint recognition, the mode of password recognition can be also be used.

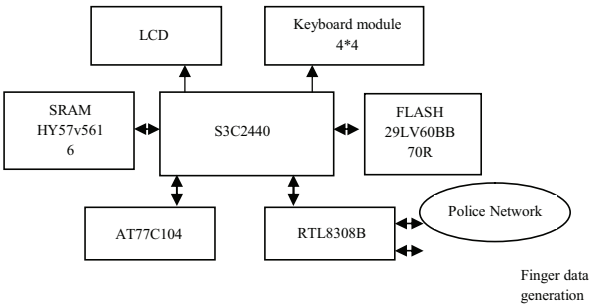

Figure 1. The Block Diagram of Hardware.

3. Design of Hardware and Software

The hardware is designed by the rules of embedded system, and the steps of software consisted of three parts. The more details are as follows.

3.1 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 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 grey-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 fingerprint recognition. It has a 500dpi resolution, anti-press, anti-static, anticorrosion [6–10].
- Ethernet switch controller

RTL8308B can provide eight 10/100 Mbps RMII Ethernet ports, which can connect police network and remote fingerprint data server. Before using the ATM terminal, the client's fingerprint feature will beconnected 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.

3.2 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 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 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 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.

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. This product embeds true hardware based 8-way navigation and click functions . The fingerprint information will be temporarily stored in SRAM and upload to the remote fingerdata server to compare through bank network. The result of process will be controlled by main chip (S3C2440).

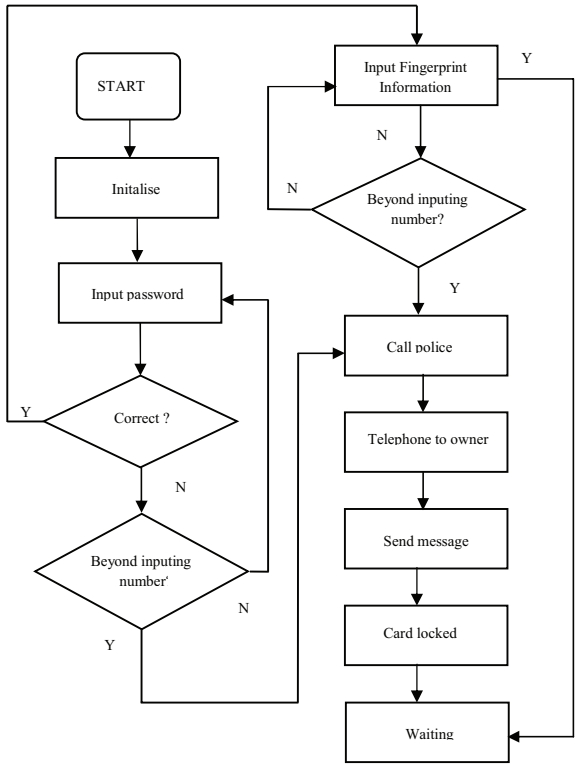

Figure 2. The Overall Flowchart of Software.

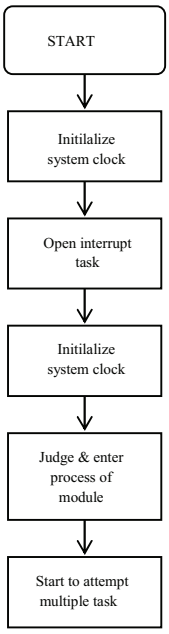

Figure 3. The Flowchart of fingerprint recognition.

The initializing process means that it sets the hardware and software and then starts the multiple mission modules, 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.

3.3 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.

3.3.1 The Detail of Fingerprint Recognition Process

The first step was the acquisition of finger print 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 obtaining the fingerprint image, it must be pre-processing. Generally, pre-processing includes is filtering, histogram computing, image enhancement and image linearization. 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.

3.3.2 The Design of Fingerprint Image Enhancement

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

Besides,

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

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

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

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 infinger print image, the image enhancement was the precondition for recognition off ingerprint characteristics. 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 ridge and valley, it could 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.

3.3.2.1 The Gabor Filter Algorithms

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

3.3.2.2 The Direction Filter Algorithms

For each point, according to its frequency, direction, using formula (4) on the clear fingerprint image area. 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 grey 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 x w area, using equation (5), (6) in each of a grey-scale mean andvariance, And the statistics is greater than the number of $\bar{M}$, marked as m and less than the number of, $\bar{M}$ marked as n.

$$\text{If} \quad |m-n| > w^2, \bar{M} = \begin{cases} \bar{M} - \theta & m \geq n \\ \bar{M} - \theta & m \geq n \end{cases} \tag{5}$$

θ is very small.

$$M(n,m) = \frac{1}{w^2} \sum_{U=1}^{w} \sum_{V=1}^{W} h\left[w(n-m)+u, w(m-m)+v \right] \tag{6}$$

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

4. 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. Additionally, 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 built on the technology of embedded system which makes the system safe; reliable and easy to use.

5. References

1. Hong L, Yifei W et al. (1998). Fingerprint image enhancement: algorithm and performance evaluation, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol 20(8), 777–789.
2. ESaatci V T (2002). Fingerprint image enhancement using CNN gabor-Cpe filter [C(0)], Proceedings of the 7th IEEE International Workshop on Cellular Neural Networks and their Applications, 377–382.
3. Gu J, Zhou J et al. (2004). A combination model for orientation field of fingerprints, Pattern Recognition, vol 37(3), 543–553.
4. Cheng J, and Tian J (2004). Fingerprint enhancement with dyadic scale-space, Pattern Recognition Letters, vol 25(11), 1273–1284.
5. Chen H, and Tian J (2005). A fingerprint matching algorithm with registration pattern inspection, Journal of Software, vol 16(6), 1046–105.
6. Smits G F, and Jordaan E M (2002). Improved SVM regression using mixtures of kernels. Proceedings of the 2002 International Joint Conference on Neural Networks, vol 3, 2785–2790.
7. Zhenghua F U, Yongjun L I et al. (2007). The embedded monitoring system based ARM, Journal of Instrument Technology, vol 7, No. I , 1–2.
8. Zhou J, Sua G et al. (2007). A face and fingerprint identity authentication system based on multi-route detection, Neurocomputing, vol 70(4–6), 922–931.
9. He Y, Tian J et al. (2003). Image enhancement and minutiae matching in fingerprint verification, Pattern Recognition Letters, vol 24(9–10), 1349–1360.
10. Wang W, Li J et al. (2008). Design and implementation of Log-Gabor filter in fingerprint image enhancement, Pattern Recognition Letters, vol 29(3), 301–308.