IJOCIT

*Review Paper*

# ATM Security based on Fingerprint Biometric and SVM

**Alireza Farhang** [1,*]
**Hassan Rashidi** [2]

**Abstract**

For the traditional 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, the author designs new ATM terminal customer recognition systems. In this paper we focus on use of SVM classifier in fingerprint recognition on ATM security.

**Keywords:** Automated Terminal Machine (ATM), Fingerprint Biometric, Support Vector Machine (SVM), Security.

[1] Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran
[2] Department of Mathematics and Computer Science, Allameh Tabataba'i University, Tehran, Iran
[*] Corresponding Author: Farhang.alireza@yahoo.com

## 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 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.[3]

In this paper, we propose a fingerprint classifier based on Support Vector Machine (SVM), a relatively new technique to train classifier that is well founded in statistical learning.

## 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 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 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. 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.[4]

### 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 follow:

- LCD module: The OMAP5910 is used in this module as a LCD controller, it supported 1024*1024 images of 15 gray-scale or 3375 colures.
- Keyboard module: It can be used for inputting passwords.
- 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.

- 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 be connected to the remote fingerprint data server to match fingerprint data with the master's[1,2], 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.
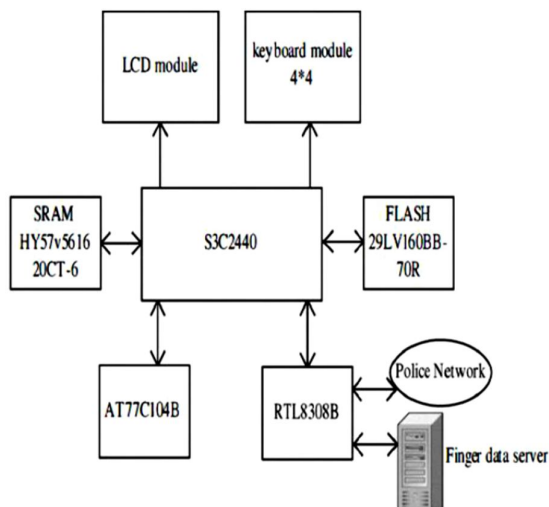


Figure 1. The Block Diagram of Hardware

### B. Software Design

The design 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. [9].
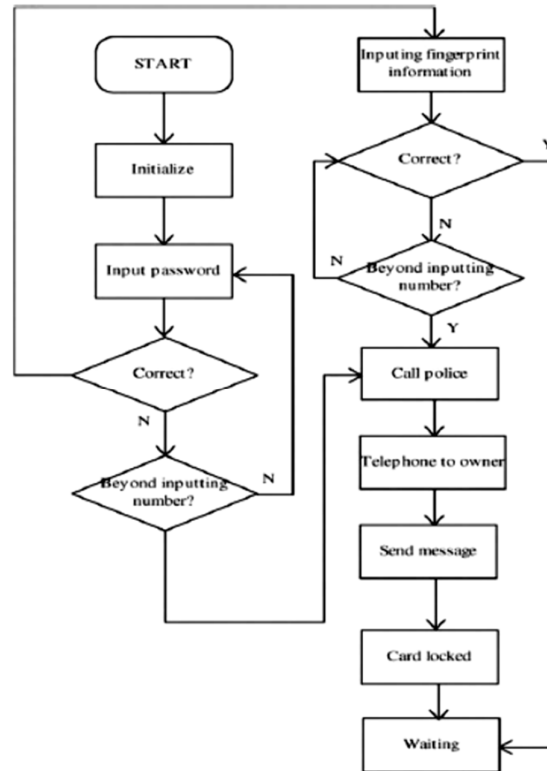


Figure 2. The Overall Flow Chart of Software

In the process of inputting fingerprint, the AT77C104B 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 embeds 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).[12] 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 figure3.

The initializing process means that set 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.
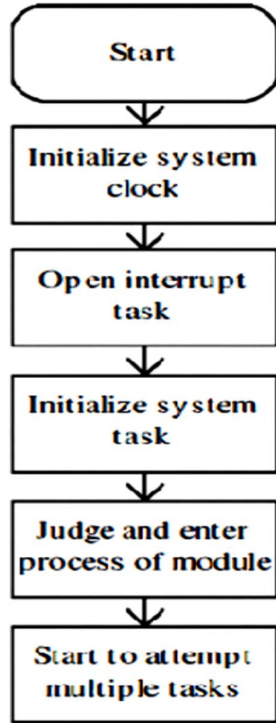


Figure 3. The Flow Chart of Fingerprint Recognition

## 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.

*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.

*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.

*Support Vector Machine (SVM)*

A fingerprint image is a digital representation of a fingerprint pattern acquired though a scanner. Machine learning algorithms, such as neural network, classification trees ,K-nearest neighbor classifiers and linear discriminant analyses ,are mainstream methods in fake fingerprint detection .Among these methods ,the support vector machine (SVM) is the most widely used .Therefore, we also select SVM as the classification method in our characteristic valuation network, Support vector machines (SVM) perform pattern recognition for two-class problems by determining the separating hyperplane1 with maximum distance to the closest points of the training set, also the SVM classifier presents better performance in almost all the tested configurations[14]. If the data is not linearly separable in the input space, a non-linear transformation $\Phi$ (0) can be applied which maps the data points $X \in R^n$ into a high (possibility infinite) dimensional space H which is called feature space. The data in the feature space is then separated by the optimal hyper plane as described above.[10] The mapping $\Phi$ (0)  is represented in the    Support Vector Machine classifier by a    Kernel function K(0,0) which defines an  inner product in H, i.e. $K(x,t) = \phi(x).\phi(t)$ The decision function of the SVM has the form :

$$f(x) = \sum_{i=1}^{l} \alpha_i y_i K(X_i, X)$$

Where    $l$    the number of data points, and $y_i \in \{-1,1\}$ is the class label of training point $x_j$. Coefficients $\alpha_i$ in Eq. can be found by solving a quadratic programming problem with linear constraints. The support vectors are the nearest points to the separating boundary and are the only ones for which $\alpha_i$ in Eq. Proposed algorithm

maintains a candidate Support Vector set. It initializes the set with the closest pair of points from opposite classes like the Direct SVM algorithm. As soon as the algorithm finds a violating point in the dataset it greedily adds it to the candidate set. It may so happen that addition of the violating point as a Support Vector may be prevented by other candidate Support Vectors already present in the set. We simply prune away all such points from the candidate set. To ensure that the KKT conditions are satisfied we make repeated passes through the dataset until no violators can be found. Thus Using support vector machine (SVM) fingerprint match has been improved. SVM has improved false rejection ratio (FRR) as well as false acceptance ratio (FAR).Besides that the accuracy of system has also been enhanced. Initially without using the classification algorithms, the training time was less because training of data was not done. But with the use of a classification algorithm like support vector machine, although training time has been increased but there has been significant improvement in the overall performance of fingerprint classification and verification.

## 4. Conclusion

The design of ATM terminal system based on fingerprint recognition took advantages of the stability and reliability of fingerprint characteristics, the recent results in pattern recognition have shown that support vector machine (SVM) classifiers often have superior recognition rate in comparison to other classification methods. Additional, the system also contains the original verifying method 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 more safe, reliable and easy to use.

## References

[1] Lin Hong, Wan Yifei, Anil Jain. (1998), "Fingerprint image enhancement: algorithm and performance evaluation", *IEEE Transactions on Pattern Analysis and Machine intelligence*. 1998, Vol. 20, No. 8, pp. 777-789.

[2] E Saatci, V Tavsanogh., (2002), "Fingerprint image enhancement using CNN gabor-Cpe filter", Proceedings of the 7th IEEE International Workshop on Cellular Neural Networks and their Applications pp. 377-382.

[3] Cheng J, Tian J., (2004), "Fingerprint enhancement with dyadic scale-space", *Pattern Recognition Letters*, Vol. 25, No.11, pp. 1273-1284.

[4] Chen H, Tian J., (2005), "A fingerprint matching algorithm with registration pattern inspection", *Journal of Software*, Vol. 16, no.6, pp. 1046-1050.

[5] Jun Zhou, Guangda Sua, Chun hongJiang. (2007), "A face and fingerprint identity authentication system based on multi-route detection", *Nero-computing*, Vol. 70, pp. 922-931.

[6] Cortes and V. Vapnik, (1995), "Support-Vector Networks", *Machine Learning*, Vol. 3, No. 20, pp.273-297.

[7] Maltoni, D. Maio, A.K. Jain and S. Prabhakar, (2003), "*Handbook of Fingerprint Recognition*" *Springer*, New York.

[8] Youssef ELMIR (2012), "Support vector machine based fingerprint identification" CTIC university d' Adrar,Algérie..

[9] Ballan M, Sakarya F, (1997), "A fingerprint classification technique using directional images", In: Proceedings of the Conference Record of the Thirty-First Asilomar Conference on Signals Systems and Computers.

[10] Support Vector Machines for Classification and Regression, S.R. Gunn, *Technical Report*.

[11] Nello Cristianini and John Shawe-Taylor, (2000), An Introduction to Support Vector Machines and Other Kernel-based Learning Methods, *Cambridge University Press*.

[12] Y. Zhou, Y. Fang, and Y. Zhang, (2008), "Securing wireless sensor networks: A survey," *IEEE Communications Surveys and Tutorials*, Vol. 10, No. 4, pp. 6–28.

[13] M. Pontil and A. Verri., (1998), " Support vector machines for 3-d object recognition", *IEEE Trans. PAMI*, pp. 637–646.

[14] Hung, Q., Chang, Sh., Liu, Ch., Niu, B., Tang, M., Zhou, Zh., (2015), "An evaluation of fake fingerprint databases utilizing SVM classification" *Pattern Recognition Letters*, pp. 610-617.

IJOCIT

WWW.IJOCIT.ORG