An Idea for Smart Card Authentication Using Fingerprint Matching Algorithm

Sujeet More

Department of Computer science, Visvesvaraya Technological University, Belgaum

Abstract- In recent technology smart card (Debit Card/Credit Card) is used for many of the activities such as marketing, online transactions, in ATMs etc. But due to theft/cracking of smart card passwords there would be an unusual loss of property. Hence in this paper i introduce some combinational techniques of securing the smart card using a biometric algorithm. This algorithm uses fingerprint recognition as a reliable method among biometric feature recognition technology which is widely applied in personal identification for the purposes of high degree of security that can be used to authenticate and secure the transactions using smart card.

Index Terms- Smart Card, Fingerprint Matching, Authentication.

I. Introduction

Fingerprint recognition is widely used reliable method among biometric feature recognition technology for personal identification for the purposes of high degree of security. In most applications, some additional requirements, for example, the high verification or recognition speed, small size of storage space for features, and enough accuracy have to be met. Consequently, it is not practically possible to store the total fingerprint as a feature into a template owing to the limitation of storage space and processing speed. As a result, we have to extract the most reliable features in the fingerprint.

The use of fingerprint verification for smart cards is a salient example among the various applications of fingerprint identification technology. Smart cards, a kind of IC cards, are being adopted in many application cases, such as mobile phones, credit cards, which require high degree of security. Fingerprint verification technology can meet this security requirement. However, smart cards are much inferior to personal computers or workstations in the capacity of storage space and processing speed because they inherently consist of the DSP (digital signal processor) or single chip microprocessor. Therefore, it is essential to save the storage space for features and speed up the processing on designing a fingerprint verification system that can be applied in smart cards.

A. Fingerprint Biometrics Steps

In Order to perform Automatic Fingerprint Identification System (AFIS) several techniques have been applied, different authors propose many different algorithms but the steps followed for fingerprint identification are similar as follows:

1. Capture of the fingerprint.
2. Pre-processing, to eliminate the redundant information and to adopt the sample to next block requirements.
3. Feature Extraction, where minutiae pores or any information related with the justness of the fingerprint is obtained.
4. Matching of the features obtained with the template previously computed in the enrollment phase. This matching will provide percentage of similarity that will be used to determine whether the user is same as enrolled user.

II. ALGORITHM

A. Computation of Orientation Field of Template Fingerprint

Orientation field is the set of directions of those pixels located in the ridges, which is stable feature information, independent of fingerprint capture equipments and distinct with respect to that of a different finger. A. R. Rao has proposed an algorithm to estimate the orientation at every pixel of texture images. In this paper, we utilize this algorithm to estimate the orientation field.

The steps to estimate the orientation field in are as follows:

1) Divide the input fingerprint image into blocks of size W×W.

2) Compute the gradients *x G* and *y G* at each pixel in each block.

3) Estimate the local orientation of each block using the following formula:

$$\theta(i,j)=\frac{1}{2}\tan^{-1}\left(\frac{\sum_{u=i-W/2}^{i+W/2}\sum_{v=j-W/2}^{j+W/2}2G_x(u,v)G_y(u,v)}{\sum_{u=i-W/2}^{i+W/2}\sum_{v=j-W/2}^{j+W/2}\left(G_x^2(u,v)-G_y^2(u,v)\right)}\right)$$

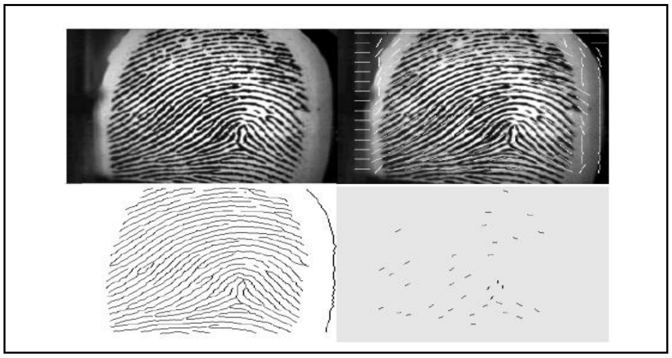
where W is the size of each block, and x G and y G are the gradient magnitudes in x and y directions respectively. Then,θ (i, j) is regularized into the degree range of – 90* ~ +90* . Finally, we obtain the orientation field image consisting of orientations at every pixel.

B. Minutiae Extraction

Minutiae extraction intends to identify minutiae and record their attributes including coordinates, directions and types, into the template. It is difficult to reliably extract minutiae from the input fingerprint, especially from the low-quality fingerprints. The performance of the minutiae extraction algorithm highly depends on the quality of the input images. However, in reality, about 10% of acquired fingerprints are of poor quality due to variations in impression or skin condition, ridge configuration, acquisition devices, and non cooperative attitude of subjects, etc. For those poor images, some spurious minutiae may exist even after fingerprint enhancement and post-processing. It is necessary to develop an algorithm to work with these spurious minutiae.

C. Fingerprint Matching

Matching is a crucial step of fingerprint recognition. To improve the accuracy, some approaches were taken to improve the accuracy of similarity measure by employing new features which can distinguish the genuine match from the impostor match. In the matching process, we employ the algorithm belonging to the light category according to FVC protocol, which is less memory and time consuming comparing with the on-line algorithms. Firstly, we get the raw similarity measure between two minutiae sets. Then, similarity of ridge width between two fingerprints was calculated, and was combined with the similarity of minutiae sets. Finally, we judge whether the match between two templates belongs to the genuine match or the impostor match by a fuzzy calculation of the quality contrast between both fingerprints image, and complete the matching process by calculating the final similarity measure with the global statistical features.



III. EXPERIMENTAL RESULTS

In our experiments database consists of fingerprint impressions of 640 bytes of storage are required for a 508×480 fingerprint image and 896 byte for an 832×768 fingerprint image. For those images, our algorithm will regulate the blocks to the size of 64×64 due to their large resolution 500 dpi (dots per inch). Consequently, our algorithm will require about 200~300 bytes for the features of minutiae and orientation fields (assuming there are 20~60 minutiae in a fingerprint), which is smaller than that of the method. So, our algorithm is very appropriate for applications in IC cards or chips.

The performance of a biometric system can be shown as a Receiver Operating Characteristic (ROC) curve that plots the Genuine Accept Rate against the False Accept Rate (FAR) at different thresholds on the matching score. For example, at a 1% FAR, the hybrid matcher gives a Genuine Accept Rate of 92%, while the other gives genuine accept rate of 70%-80%. The results of our experiments reveal that our algorithm is very efficient in preventing the error of false matching. That is to say, our algorithm greatly reduces the FAR, except that we reduce the constraint of the orientation field in computing matching score.

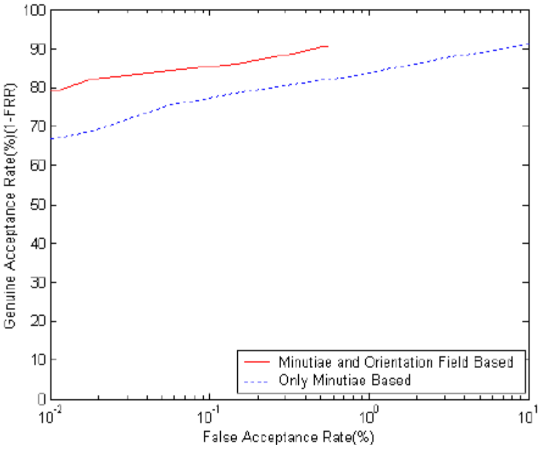


Figure 2: ROC Curve

IV. CONCLUSION

In this paper, we have proposed an improved minutia-based pattern matching algorithm, which achieves good performance in both efficiency and accuracy neither sacrificing the processing speed nor greatly increasing the size of storage space for features. The primary advantage of the proposed method is its small size in storing extra features and easy implementation.

Another advantage of our algorithm is its more precise registration scheme, which supports the fingerprint rotation scale to 2π. Through the orientation field and computation of Ps (p, q), we can, to some extent, tackle the trouble that the number of matched minutiae between two identical fingerprints is comparable with that of occasionally matched minutiae between two different fingerprints. Therefore, our method can achieve good performance without classification to fingerprints, which also helps to authenticate IC cards.

REFERENCES

[1] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, “An Identity Authentication System Using Fingerprints,” Proc. IEEE, Vol.85, No.9, pp.1365-1388, 1997.

[2] A.N. Marana, A.K. Jain, “Ridge-based Fingerprint Matching Using Hough Transform,” Computer Graphics and Image Processing, 2005. SIBGRAPI 2005. 18th Brazilian Symposium on, pp: 112-119, 2005.

[3] D. Maio and D. Maltoni, “Direct Gray-scale Minutiae Detection in Fingerprints,” IEEE Trans. Pattern Analysis and Machine Intelligence, Vol.19, No.3, pp.27-39, 1997.

[4] J. Yang, L. Liu and T. Jiang, "An Improved Method for Extraction of Fingerprint Features," To appear in the Proc. of the Second International Conference on Image and Graphics, Anhui, P.R. China, August, 2002.

[5] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, "A Real-Time Matching System for Large Fingerprint Databases", IEEE Trans. Pattern Analysis and Machine Intelligence, Vol.18, No.8,pp. 799-813,1996.

[6] Synthetic Fingerprint Generator [Online]. Available: http://biolab.csr.unibo.it/Research.asp

[7] S.H. Lee, C.H. Lee, and J.H. Kim, "Model Based Fingerprint Quality Estimation of Fingerprint Images," in Proc. International Conf. on Biometrics (ICB06), HongKong, China, pp: 229-235, 2006.

[8] X.J. Chen, J. Tian, and X. Yang, "A New Algorithm for Distorted Fingerprints Matching Based on Normalized Fuzzy Similarity Measure," IEEE Trans. Image Processing, vol. 15, no. 3, pp: 767–776,2006.

[9] X.J. Chen, J. Tian, J.G. Cheng, and X. Yang, "Segmentation of Fingerprint Images Using Linear Classifier," EURASIP Journal on Applied Signal Processing(EURASIP JASP), no.4, pp: 480-494, 2004.

[10] Y.L. He, J. Tian, L. Li, and X. Yang, "Fingerprint Matching Based on Global Comprehensive Similarity," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 28, no. 6, pp. 850–862, 2006.

AUTHORS

First Author – Auth Sujeet More, Department of Computer science, Visvesvaraya Technological University, Belgaum, sujeetmore7@gmail.com