A secure and private fingerprint-based authentication system

Qinghai Gao
Department of Security Systems, Farmingdale State College, SUNY
GaoQJ@farmingdale.edu

Abstract

In this paper we propose a secure and private fingerprint-based authentication system. First the user of the system ought to register his or her fingerprints to a server database of fingerprint-minutiae templates, which are generated from the original fingerprint images and then are inserted with a number of foreign minutiae. Upon authentication the same live fingerprint will be measured again to regenerate a template, which will then be matched against the stored templates. The regenerated template will be discarded once the match is done. The new system is secure and private because of the insertion of large numbers of foreign minutiae to the database templates and no other template will be stored. Our testing results show the proposed system is promising.

Introduction

Biometric authentication system works in two stages: enrollment and authentication. At both stages, a raw image is obtained with some instruments by measuring a live biometric. The raw image is then used for feature generation. Features extracted are often transformed into a template, which contains less data than the raw image. The template generated at authentication will be matched against the enrolled template. If the score is greater than a system defined threshold, the matching is considered successful, otherwise unsuccessful. The main objectives of biometric recognition are user convenience and better security. We believe that wider applications of biometric technologies are inevitable and necessary. However, biometric applications have raised a series of issues that prevent its wide acceptance. Among them the security and privacy issues [1-6] of biometric information are regarded as more important than other issues.

In literature a few methods [7-9] has been proposed to address these issues by perturbing the original minutiae of fingerprint templates. In this paper we propose an authentication system that protects the security and privacy of biometric information. Specifically, the system is a client-server system in which the enrolled fingerprint templates will be modified with the insertion of large number of foreign minutiae before they are stored in the server database. And the modified templates will be used directly, i.e., without removing the inserted foreign minutiae upon authentication. If the fingerprints are stolen by a hacker, he would have more difficulty to differentiate the genuine minutiae from the foreign minutiae. Thus, the biometric templates are secured. No other biometric information needs to be stored because the new template generated at authentication will only be used temporarily to obtain a matching score and then be discarded.

The rest of the paper is organized as the following. In section 2 we test matching an original template (without any foreign minutiae) against the same template inserted with increasingly larger number of foreign minutiae. In section 3 we test matching an original template against a database of fingerprints in which every fingerprint has been inserted with certain number of foreign minutiae. Section 4 summarizes the paper.

Matching templates with foreign minutiae

In this section we test matching an original template against the same template inserted with increasingly larger number of foreign minutiae. Nine fingerprints were randomly selected from the first fingerprint database of Fingerprint Verification Competition 2004[10] for the testing, as given in Table 1. Note that the first row (labeled with "#Min") is the numbers of minutiae in each fingerprint. The 119 minutiae in *FP1* will be used as the sources of foreign minutiae to be inserted into other fingerprint minutiae templates. Also note that the cells in the left bottom of the table are left empty due to symmetrical matching.

Table 1 Fingerprints and their original matching scores

#Min	**119**	**117**	**113**	**107**	**93**	**72**	**55**	**25**	**21**
FP#	*FP1*	*FP2*	*FP3*	*FP4*	*FP5*	*FP6*	*FP7*	*FP8*	*FP9*
FP1	837	10	17	15	7	14	6	3	0
FP2		1018	15	14	10	12	8	3	3
FP3			1011	16	12	10	7	3	3
FP4				1007	9	8	9	3	3
FP5					509	9	10	3	0
FP6						489	7	3	3
FP7							499	3	3
FP8								100	0
FP9									131

From *FP1* we randomly select 10, 20, …, or 110 minutiae and then insert them into the original minutiae templates of other fingerprints to obtain a new template. On each step, match the new template against the corresponding original template to obtain a matching score. The matching results are plotted in Fig.1.

From Fig. 1 we can see that for nearly every fingerprint, as we step-wised insert foreign minutiae into a template, the matching scores remain stable at the beginning. For example, for *FP4* the matching scores stay nearly the same after 10 to 30 foreign minutiae are inserted; for *FP5* the matching scores remain at 509 after 10 to 60 foreign minutiae are added.

We can also see from Fig.1 that the original number of minutiae plays a role on how many foreign minutiae can be inserted without significantly affecting the matching score. Unlike *FP5* which has 95 minutiae, *FP9* only has 21 original minutiae. Therefore, the matching score starts going down after 30 foreign minutiae are inserted and reaches the lowest score after 60 minutiae are inserted. The generic conclusion is that a fingerprint with more minutiae can tolerate more foreign minutiae.

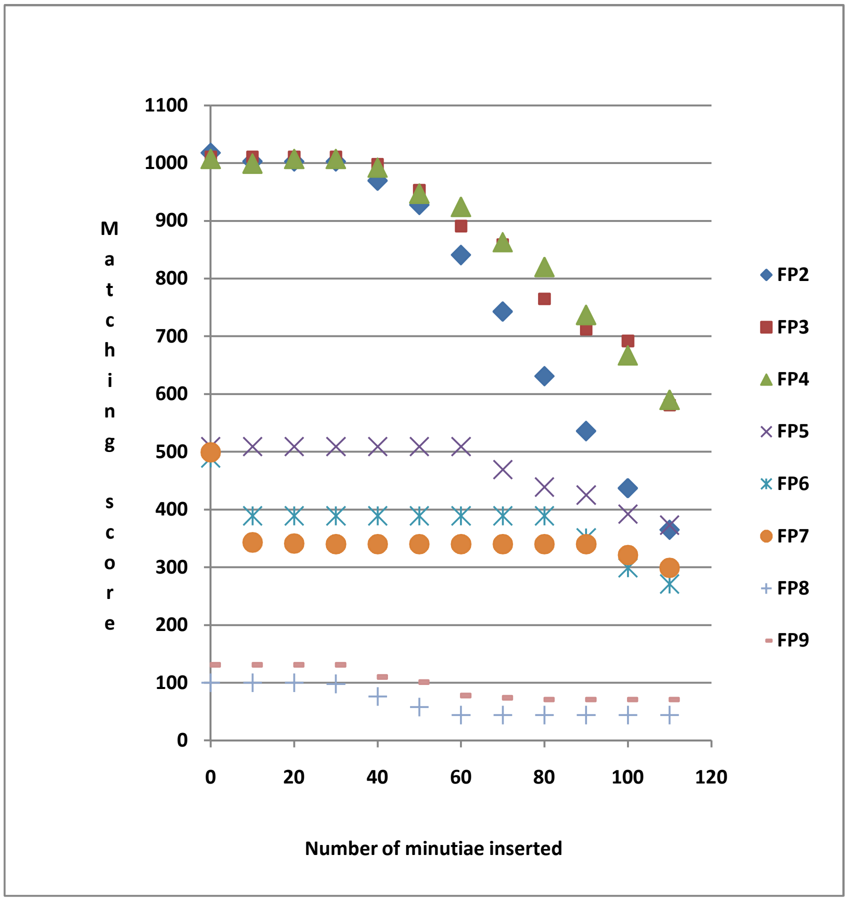

Fig.1 Matching results after inserting foreign minutiae

Inserting foreign minutiae into database

In this section we test matching an original template against a database of fingerprints in which every fingerprint has been inserted with certain number of foreign minutiae. Since fingerprint templates in the database will be stored in the server, inserting foreign minutiae can protect the security and privacy of the original fingerprint templates. The goal of the testing is to see if inserting foreign minutiae would increase the false matching rates (FMR), i.e., some fingerprints which do not match originally may become a match after inserting foreign minutiae.
For every fingerprint templates in the database we insert a different set of foreign minutiae. We step-wised add more foreign minutiae to every fingerprint templates. At each step we match a randomly selected fingerprint against the database. The results are plotted in Fig. 2, which shows the results of inserting 0, 10, 20 30, 40 and 50 foreign minutiae. From Fig.2 by comparing the *DB+0* graph (Top-left) with other graphs we can see that inserting foreign minutiae has negligible effects on the matching scores. Thus inserting foreign minutiae to the database does not increase the FMR.

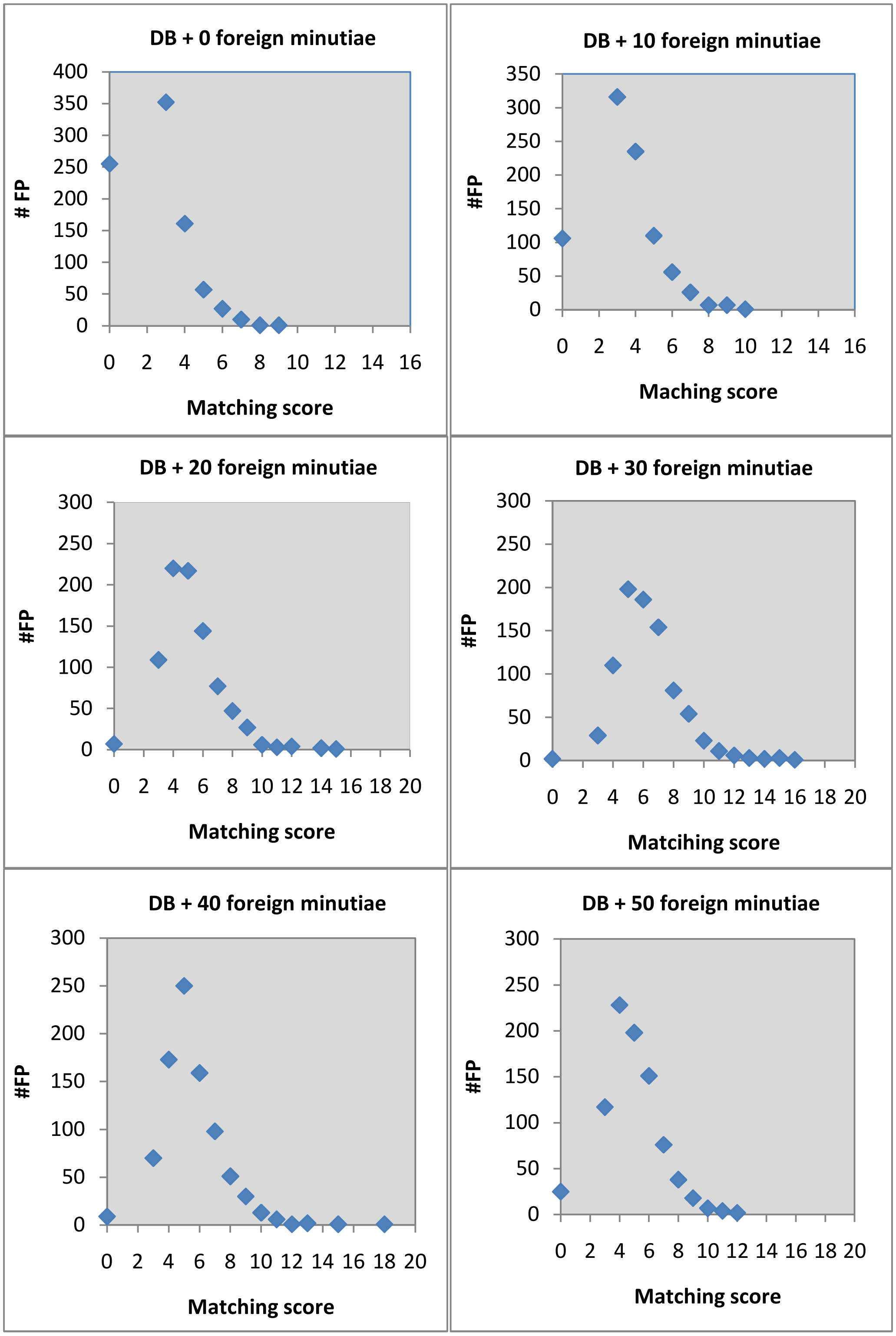

Fig. 2 Matching results for inserting foreign minutiae into database (Threshold : 40)

Conclusion

In this paper we propse a secure and private fingerprint-based authentication system, in which the fingerprint minutiae templates that are stored on the server database would be inserted with a number of foreign minutiae. These foreign minutiae will not be removed during authentication. Our first tesing shows that the templates can still matching after certain number of foreign minutiae are inserted. The number of foreign minutiae that can be added without significantly affecting matching score significantly depends on the number of original minutiae. Our second testing shows that inserting foreign minutiae into the database does not increase the false matching rate. With these results we conclude that inserting foreign minutiae is a promising method for enhancing the security and privacy of fingerprint-based authentication system.

Bibliography

[1] Wadman, M. (1999). "Biometrics group counters privacy fears". *Nature*, 398, 6727: 451.
[2] Schneier, B. (1999) "Biometrics: use and abuse". *Communications of the ACM*, 42: 136
[3] Grijpink, J. (2004). "Two barriers to realizing the benefits of biometrics: a chain perspective on biometrics and identity fraud as biometrics' real challenge", *Proc. SPIE*, 5310: 90-102.
[4] Bronstein, M. & Bronstrein, A. (2002). "Biometrics was no match for hair-raising tricks", *Nature*, 420, 6917: 739.
[5] Buhan, I. & Hartel, P. (2005). "The State of the Art in Abuse of Biometrics". Available at: http://www.coelle.org/papers/TheUseandAbuse.pdf
[6] Jain, A., Nandakumar, K., and Nagar, A. (2008). Biometric Template Security. *Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics*.
[7] Ratha, N., Chikkerur, S., Connell, J., and Bolle, R. (2007). Generating Cancelable Fingerprint Templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4): 561-572.
[8] Ratha, N., Connell, J., and Bolle, R. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(2): 614-634.
[9] Ratha, N., Connell, J., Bolle, R., and Chikkerur, S. (2006). Cancelable Biometrics: A Case Study in Fingerprints. *18th International Conference on Pattern Recognition*, pp: 370-373.
[10] Available at: http://bias.csr.unibo.it/fvc2004/