Research Journal of Computer and Information Technology Sciences ISSN 2320 – 6527
Vol. **5(5),** 6-8, July **(2017)** *Res. J. Computer and IT Sci.*

Short Communication

Advanced security with fingerprint and palmprint recognition

Deepa Soni
Bhilai Institute of Technology, Durg, CG, India
deepa.soni04@gmail.com

Available online at: www.isca.in
Received 8th April 2017, revised 5th July 2017, accepted 18th July 2017

Abstract

A requisite to authenticate ourselves to machines is increasing day by day in today's meshed society. It is must that only the legitimate user will be able to perform any action on our networked society also it is necessary that a strong system should be introduced to verify individuals at that time biometric identification comes to light. Well known biometric approaches are palmprint and fingerprint recognition technology. Instead of using palmprint recognition or fingerprint recognition system separately for personal authentication we can use both fingerprint and palmprint recognition together to provide enhanced level of confidence for personal verification and identification.

Keywords: Biometric recognition, Fingerprint, Palmprint, Creases, Superficial lines, Decentralized, encrypted databases.

Introduction

Biometric recognition systems are advisable for high security applications because of privacy concerns. Our palm surface usually has principal lines and secondary creases. Principal lines are thumb crease (thenar crease), five finger crease (proximal palmar crease) and three finger crease (distal finger crease). Principal lines are formed before we born and superficial lines are formed after we born.

Even identical twins have different palmprint. We are considering principle lines for personal identification and fingerprints. Generally it is believed that pattern of each finger of everyone is unique. In fingerprint we check for minutiae of each finger, where ridges and lines end or where ridges split into two ridges are called minutiae. So we recommend to use this multi-model (integration of palmprint and fingerprint) recognition system for better security[1-2].

Methodology

The basic methodology involved in the project is as followed, we will have two option to select Registration for new user and Verification of registered user. Figure-1 (from Biometric Recognition: security and Privacy concerns[3]) shows the general overview of the methodology.

First block is for registration process; for registration an interface will be provided to user at the interface a scanner is there to scan the fingerprint and palm print a quality checker will check the quality of prints which has been taken from the user here minutiae and creases is the feature of fingers and palm, hash code is generated from extracted features of palm and fingers then stored in the databases. In verification process the user who want to verify himself has to scan his hand and a hash code is generated from the scanned prints then that hash code is compared with the previously stored one hash of that user if hash is matched then the requester is a legitimate user otherwise not a legitimate user[3-5].

Figure-2 contains flow chart of the working process is shown in flow chart and description is as followed:

This system has two module first is registration and second one is verification.

Registration: Step-1: A contactless recognition system scans (read) minutiae (where ridges of fingers and lines end or ridges splits in two) from fingers and creases from palm (automated palmprint recognition system[6]).

Step-2: from scanned fingerprints and palmprint, a hash code is generated and stored to the different databases.

Verification: Step-1: Scans minutiae from fingers and creases from palm through optical sensor.

Step-2: After scanning process, a hash code is generated from scanned biometric.

Step-3: Firstly hash code of scanned palmprint and previously stored hash code of palmprint is compared. i. If both hash codes are not matched then the request of verification is cancelled, ii. Else request is forwarded for next step.

Step-4: Comparison between the hash code of scanned fingerprint and previously stored hash code of fingerprint is performed. i. If hash codes are not matched then the request of verification is cancelled, ii. Else verification process is complete and all assigned privileges of that user are granted.

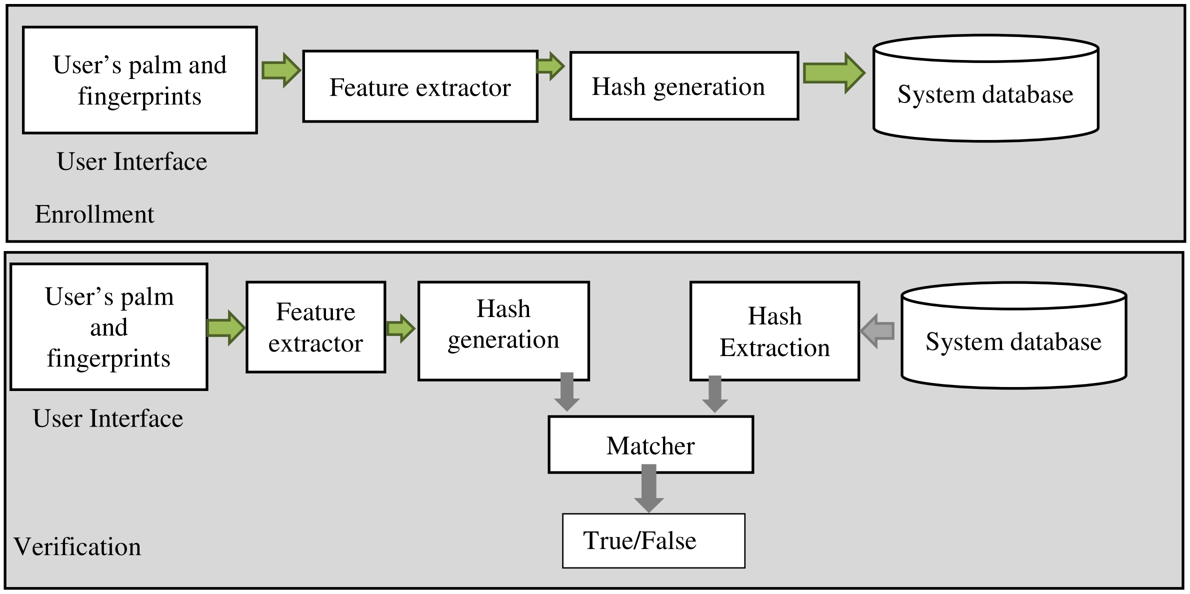

Figure-1: Block diagram of methodology.

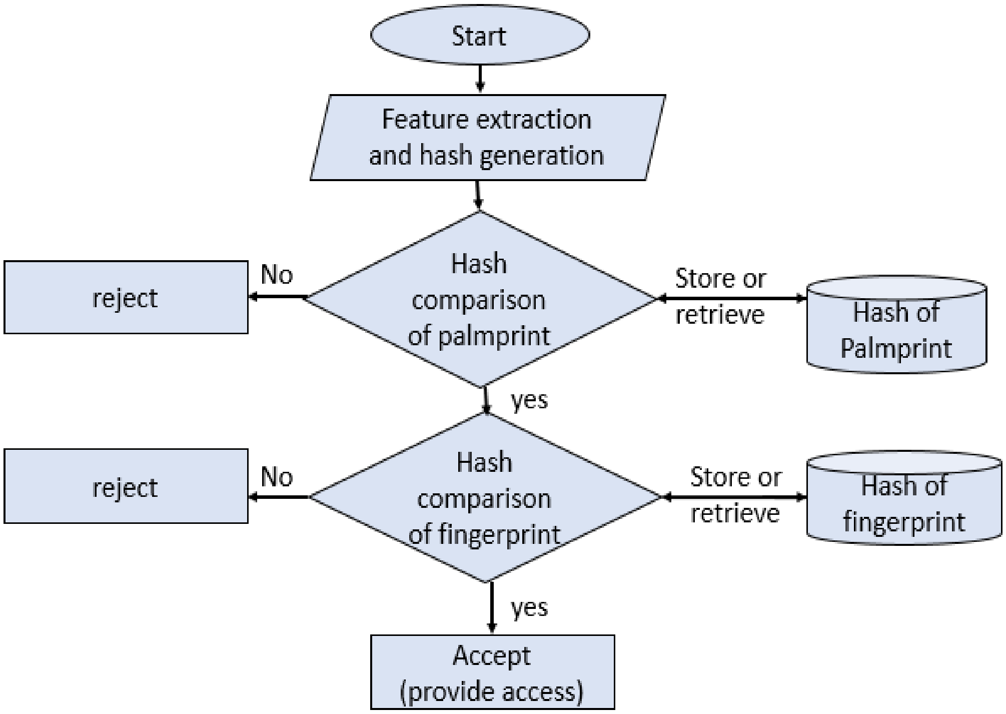

Figure-2: Flow Chart of palmprint and finger print recognition.

The technique we have adopted for securing our database by making it decentralized and encrypted[7]. If our database is decentralized then it will be more secure than centralized one. Hackers are more attracted towards centralized databases. Here we have stored fingerprint and palmprint in separate database so that if anyone gets access on a single database then the other information will be save, here we have stored hash of minutiae and creases so if anyone gets it then he will not be able to do anything with that hash.

Conclusion

From this analysis we observe that this system will be strong enough to recognize a person based on biometric characteristics. Proposed multimodal-biometric system is more secure than previous fingerprint recognition system and integrating hashing function technique along with system will prevent a thief to acquire a person's biometric.

Decentralized database of the system will be reliable system and more satisfactory for the time being also its implementation cost is low and simple to implement.

References

1. Maltoni D., Maio D., Jain A.K. and Prabhakar S. (2009). Handbook of Fingerprint Recognition - Second Edition Springer, London,.

2. Jain A.K., Bolle R. and Pankanti S. (1999). Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers..

3. Prabhakar Salil, Pankanti S. and Jain A.K. (2003). Biometric Recognition: Security and Privacy Concerns. *IEEE Security and Privacy,* 33-42, DOI: 10.1109/MSECP.2003.1193209.

4. Maio Dario, Maltoni Davide, Cappelli Raffaele, Wayman James L. and Jain Anil K. (2002). FVC2002: Second Fingerprint Verification Competition. Proc. Int'l Conf. Pattern Recognition, IEEE CS Press, 3, 811-814.

5. Kour Jaspreet, Vashishtha Shreyash, Mishra Nikhil, Dwivedi Gaurav and Arora Prateek (2013). Palmprint recognition system. *International Journal of Innovative Research in Science, Engineering and Technology*, 2(4), 1006-1009.

6. Connie Tee, Beng Jin Andrew Teoh, Kah Ong Michael Goh and Chek Ling David Ngo (2005). An automated palmprint recognition system. *Image and Vision Computing*, 23, 501-515.

7. Jules A. and Sudan M. (2002). A Fuzzy Vault Scheme Proc. IEEE Int'l Symp. Information Theory, IEEE Press, 408.