ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Combination Fingerprint Template Generation Using Multi-Biometrics System

K. Kannan,S. Meiyarasan, M. Rajesh, S.Muthusamy

UG Scholar, Department of CSE, Surya Engineering College, Erode, Tamilnadu , India.

UG Scholar, Department of CSE, Surya Engineering College, Erode, Tamilnadu , India.

UG Scholar, Department of CSE, Surya Engineering College, Erode, Tamilnadu , India.

Assistant Professor, Department of CSE, Surya Engineering College, Erode, Tamilnadu , India.

ABSTRACT: We propose here a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity. In the enrollment, two fingerprints are captured from two different fingers. We extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored in a database. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template. By storing the combined minutiae template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen. Furthermore, because of the similarity in topology, it is difficult for the attacker to distinguish a combined minutiae template from the original minutiae templates. With the help of an existing fingerprint reconstruction approach, we are able to convert the combined minutiae template into a real-look alike combined fingerprint. Thus, a new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based finger print matching algorithms. The experimental results show that our system can achieve a very low error rate with FRR 0.4% at FAR 0.1%. Compared with the state-of-the-art technique, our work has the advantage in creating a better new virtual identity when the two different fingerprints are randomly chosen.

I. INTRODUCTION

Network security consists of the policies and practices adopted to prevent and monitor access, misuse, modification, or denial of a computer network and network accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator Users choose or are assigned an ID and password or other authenticating information

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals.
The literature on automatic fingerprint verification includes a variety of methods that are broadly categorized into minutiae-based, image-based, and hybrid techniques. that allows them access to information and programs within their authority.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

II. PROBLEM STATEMENT &OBJECTIVE

- Traditional encryption is not sufficient for fingerprint privacy protection because encryption is required before the fingerprint matching, which exposes the fingerprint to the attacker.
- Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint.
  To generate minutiae based template from a two different fingerprint template.

Project Objective:

The main objective of this system is to prevent an attacker to compromise privacy of users or biometric data and not necessarily to the art by passing of the biometric authentication itself.

III. EXISTING SYSTEM

- Most of the existing techniques make use of the key for the fingerprint privacy protection, which creates the inconvenience.
- They may also be vulnerable when both the key and the protected fingerprint are stolen.
- The user identity may also be compromised when both the key and the protected thinned fingerprint are stolen.
- To implement fuzzy fault on the minutiae, this is vulnerable to the key-inversion attack.
- Two separate databases are maintained that is not possible for same applications.
- Decryption is needed for this approach

IV. PROPOSED SYSTEM

- A novel system for protecting fingerprintprivacy by combining two different fingerprints into a newidentity.
- During the enrollment, the system captures two fingerprintsfrom two different fingers.
- A combined minutiaetemplate generation algorithm to create a combined minutiaetemplate from the two fingerprints.
- In such a template, the minutiae positions are extracted from one fingerprint, while the minutiae directions depend on the orientation of the other fingerprint and some coding strategies.
- The template will be stored in a database for the authentication which
- Requires two query fingerprints.
- A two-stage fingerprint matching process is further proposed for matching the two query fingerprints against a combined minutiae template.
- By using the combined minutiae template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen.
- In addition, the combined minutiae template share a similar topology to the original minutiae templates, it can be converted into a real-look alike combined fingerprint by using an existing fingerprint reconstruction approach.
- The combined fingerprint issues a new virtual identity for two different fingerprints, which can be matched using minutiae based fingerprint matching algorithms.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

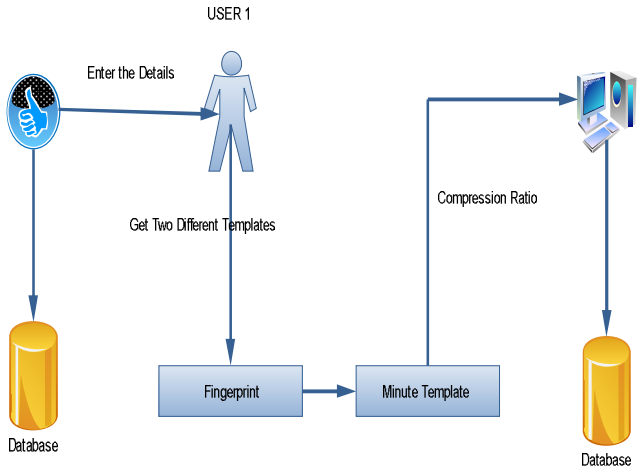
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

SYSTEM ARCHITECTURE:

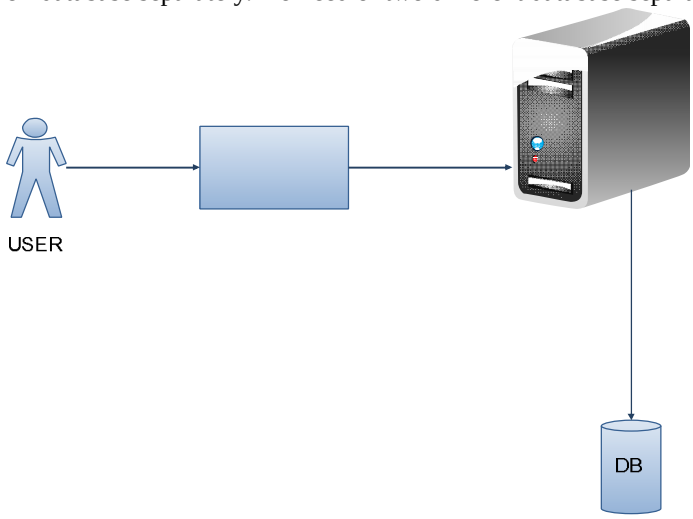


MODULES
LIST OF MODULES

- User Enrollment
- Compressed Template Generation
- Server Authentication
- Access User Information

USER ENROLLMENT

This Module mainly used for user registration process and they need to provide information such as username, password, address, phone number, image, fingerprint info, Security question, answer, locker details and the server can maintain the details in their database separately. No need of two different database separately.



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

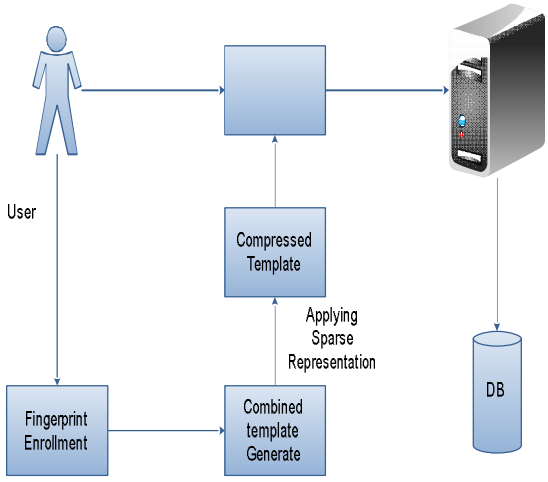
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

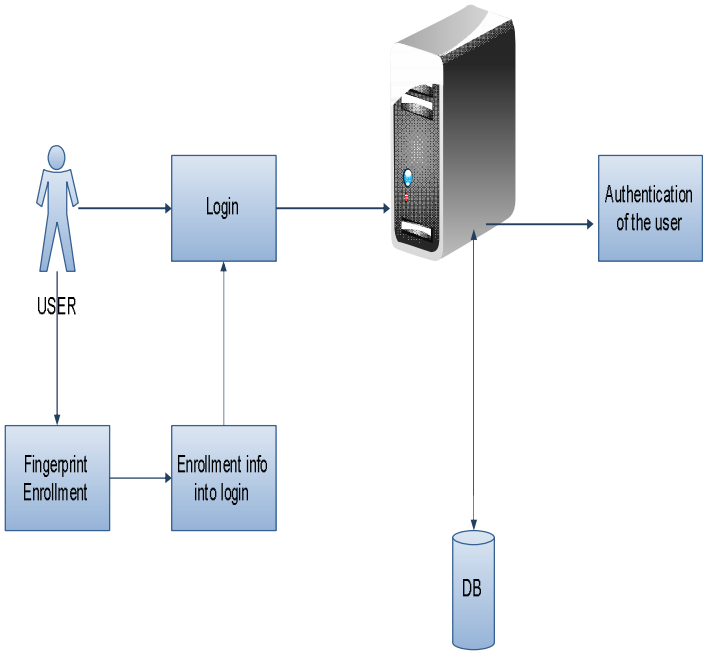
COMPRESSED TEMPLATE GENERATION

User provides a two different fingers and the combination is generated from the combined fingerprint for a given whole fingerprint, divide it into small blocks called patches. Use the method of sparse representationto obtain the coefficientsthe effects on actual fingerprint matching or recognition is investigated.



SERVER AUTHENTICATION

This module mainly used to authenticate the user login info details provided by the user will be match with an existing database and especially fingerprint info. The Fingerprint enrollment process again the two points are extracted and then the matching the two templates with the database if it matches then the user is an authenticated person can access the details. Otherwise; user is not an authenticated user deny accessing the details.



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Access User Information

The user can access their information if they want to view the details and the updation they want to do their information means they provide their updation info to the server and in turn server can update the user information. The users access the details at anytime. This will provide a high enough security to the user details. The user data will be more and more secure unauthorized user can't able get the details.

IV. CONCLUSION

A novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints will be generated and stored in a database. To make the combined minutiae template look real as an original minutiae template, three different coding strategies are introduced during the combined minutiae template generation process. In the authentication process, two query fingerprints from the same two fingers are required. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Our combined minutiae template has a similar topology to an original minutiae template. Therefore, we are able to combine two different fingerprints into a new virtual identity by reconstructing a real-look alike combined fingerprint from the combined minutiae template. The experimental results show that our system achieves a very low error rate with FRR at FAR. It is also difficult for an attacker to break other traditional systems by using the combined minutiae templates. Compared with the state-of-the-art technique, our technique can generate a better new virtual identity (i.e., the combined fingerprint) when the two different fingerprints are randomly chosen. The analysis shows that it is not easy for the attacker to recover the original minutiae templates from a combined minutiae template or a combined fingerprint.

V. FUTURE ENHANCEMENT

The authentication of user information by using the Security question and answer provided by the user during registration in case of wounded fingerprint information it will be changed and updated the database it will provide more security to the user data.

REFERENCES

1. C. Gottschlich, B. Tams, and S. Huckemann, "Perfect fingerprint orientation fields by locally adaptive global models," IET Biometrics, pp.183-190, 2017.
2. S. Li and A. C. Kot, "Privacy protection of fingerprint database," IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.
3. Ross and A. Othman, "Visual cryptography for biometric privacy," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81,Mar. 2011.
4. S. Li and A. C. Kot, "A novel system for fingerprint privacy protection," in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), Dec. 5–8, 2011, pp. 262–266.
5. K. Nandakumar, and A. K. Jain, "Biometric template transformation: A security analysis," in Proc. SPIE, Electron. Imaging,Media Forensics and Security, San Jose, Jan. 2010.
6. N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach.Intell., vol. 29, no. 4, pp. 561–72, Apr. 2007.
7. W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in Proc. Biometrics Symp., Sep. 2007, pp. 34–39.
8. B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication
9. featuring fingerprint data and tokenised random number," Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.
10. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants," Pattern Recognit., vol. 39, no. 7, pp. 1359–1368, 2006.
11. B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug. 2004