Abstract

Protecting the privacy of the fingerprint in authentication systems is become a major issue now-a-days because of the widespread use of fingerprint recognition systems. Traditional encryption and transformation techniques are shown to be more vulnerable to attacks. Therefore, fingerprint combination at the image and feature level has been proposed. This paper introduces two approaches for protecting fingerprint privacy by combining two different fingerprints into a new identity. This paper compares two systems that were introduced to protect the privacy of fingerprint. First is a novel system for fingerprint privacy protection by mixing features of two different fingerprints and thus generate a new identity. During enrolment, the system captures left and right thumb impression from a user. The new identity contains minutiae points of right thumb and has an orientation of left thumb impression. Second is a technique that combines minutiae features of two different fingerprints of a user. The minutiae points of each fingerprints is protected in the new identity. In addition minutiae filtering is done in order to remove spurious minutiae for improving the performance of both the systems. Finally the performance of each technique in terms of FRR, ERR and FAR is compared. For evaluating the performance of two techniques, this work uses same algorithms for the pre-processing and post-processing of fingerprint image.
References

- 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.
- Berrin Yanikoglu and Alisher KhomlatovSabanci University, "Combining Multiple Biometrics to Protect Privacy", in Proc. ICPR- BCTP Workshop, Cambridge, U. K., Aug.


Index Terms
Computer Science
Security

Keywords
Privacy  Combination  Fingerprint  Protection  Minutiae  Orientation