Abstract

Protecting the privacy of the fingerprint in authentication systems has become a major issue nowadays 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 generating a new identity. During enrolment, the system captures left and right thumb impressions 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 fingerprint are 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 the same algorithms for the pre-processing and post-processing of fingerprint images.
Fingerprint Combinations for Privacy Protection: A Performance Analysis

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 KholmatovSabanci University, "Combining Multiple Biometrics to Protect Privacy", in Proc. ICPR- BCTP Workshop, Cambridge, U. K., Aug.
2004.

Index Terms

Computer Science
Security

Keywords
Privacy Combinatione Fingerprint Protection Minutiae Orientation