Privacy Protection using Random Combination of Fingerprints

Abstract

The aim of this paper is to protect the information in database by combining two different fingerprint images into a new identity. This is done in two phases a) Enrollment and b) Authentication. In Enrollment phase the minutiae position from one finger and the orientation position from another finger are extracted. These two images are being combined into a new template. It is done by using a special technique called Watermarking. Once the enrollment is over the furnished information will be stored in the server as template. In Authentication phase the fingerprint matching uses two stage query processing. The images obtained from two queries are being combined and checked with the stored template. Only if both the images are matching the access is granted to the user or else an error message is sent by the server. Since the combined template is visually realistic it is difficult for the hacker to break the security by separating the two fingerprint images. Compared with the existing system, our proposed system creates a new virtual identity when two fingerprints are chosen at random. The usage of invisible watermarking technique will increase the security by hiding the original information.
Privacy Protection using Random Combination of Fingerprints


Index Terms

Computer Science
Security

Keywords

Combination Minutiae Watermarking Privacy protection Orientation