Abstract

The popularity of biometrics and its widespread use introduces privacy risks. Template security is a critical issue in biometric systems because biometric templates cannot be easily revoked and reissued. While multibiometric systems overcome limitations such as non-universality and high error rates that affect unibiometric systems, they require storage of multiple templates for the same user. Securing the different templates of a user separately is not optimal in terms of security. Hence, we propose a scheme for securing multiple templates of a user as a single entity. We derive a single multibiometric template from the individual templates and secure it using the fuzzy vault framework. We demonstrate that a multibiometric vault provides better recognition performance and higher security compared to a unibiometric vault. One of the main vulnerabilities of a biometric system is the exposure of a user's biometric template information. Access to a user's template can lead to (i) creation of physical spoofs (ii) replay attacks, and (iii) cross-matching across different databases to covertly track a person. Furthermore, unlike passwords or tokens, compromised biometric templates are not revocable. Due to these reasons, template security is essential to protect both the integrity of the biometric system and
the privacy of the users. Although a number of approaches have been proposed to secure templates, most of these schemes have been designed primarily to secure a single template.

References


Index Terms

Computer Science
Fuzzy Systems
Keywords

Keywords are your own designated keywords which can be used for easy location of the manuscript using any search engines.