A Biometric Template Security Approach to Fingerprints Based on Polynomial Transformations

Authors : Ramon Santana

Abstract : The use of biometric identifiers in the field of information security, access control to resources, authentication in ATMs and banking among others, are of great concern because of the safety of biometric data. In the general architecture of a biometric system have been detected eight vulnerabilities, six of them allow obtaining minutiae template in plain text. The main consequence of obtaining minutia templates is the loss of biometric identifier for life. To mitigate these vulnerabilities several models to protect minutiae templates have been proposed. Several vulnerabilities in the cryptographic security of these models allow to obtain biometric data in plain text. In order to increase the cryptographic security and ease of reversibility, a minutiae templates protection model is proposed. The model aims to make the cryptographic protection and facilitate the reversibility of data using two levels of security. The first level of security is the data transformation level. In this level generates invariant data to rotation and translation, further transformation is irreversible. The second level of security is the evaluation level, where the encryption key is generated and data is evaluated using a defined evaluation function. The model is aimed at mitigating known vulnerabilities of the proposed models, basing its security on the impossibility of the polynomial reconstruction.

Keywords : fingerprint, template protection, bio-cryptography, minutiae protection

Conference Title : ICCB 2018 : International Conference on Clinical Biostatistics

Conference Location : Vancouver, Canada

Conference Dates : August 09-10, 2018