Biometric Cryptosystems: Towards a Light and Precise Remote Authentication. (2021) Recent Advances in Computer Science and Communications, 14 (7), pp. 2087-2102. https://doi.org/10.2174/2666255813666191223115223

Authors:

Atef Bentahar, Abdallah Meraoumia, Hakim Bendjenna, Salim Chitroub, Abdelhakim Zeroual

Abstract

Background: Remote authentication in current networks such as IoT that connects many end-devices of low capacity must be light, accurate and scalable without threatening security. In general, biometrics is the most reliable way to authenticate users because of its efficient results in many applications.

Objective: The biometric data is expressed by a feature vector that should be extracted and secured by reliable techniques. This paper proposes a suitable extraction and encryption scheme with the aim to make the authentication light, accurate, scalable and secure.

Methods: As extraction technique, principal component analysis with a nonlinear block average quantization is used to reduce the feature vector length with the aim to increase the rapidity and the scalability. As encryption technique, the fuzzy commitment and the fuzzy vault with Hamming and Reed-Solomon codes are used to increase security. These cryptosystems are tested with multibiometric modalities to make the validation more credible.

Results: Experimental results are analyzed, validated and compared to other works according to several conventional and new recognition rates. Analysis is also done in terms of computation time to validate the lightness of our findings. It is shown that the proposed scheme finds a compromise between the coveted features.

Conclusion: Our biometric cryptosystems ensure a secure, light, precise and scalable remote authentication. These properties can be achieved by using the PCA technique with nonlinear coefficient quantization and fuzzy schemes with the appropriate correcting-code.