Cancelable Multi-biometric Approach using Fuzzy Extractor and Novel Bit-wise Encryption

Surabhi Garg

TCS Research

The widespread deployment of multi-biometrics to authenticate users prompts the need for biometric systems with high recognition performance. Further, the biometric data, once leaked or stolen, remains compromised forever. Hence biometric security is of utmost importance. Existing biometric template protection schemes either degrade the recognition performance or they have issues with security and speed. We propose a cancellable multi-biometric authentication approach where a novel bit-wise encryption scheme transforms a biometric template to a protected template using a secret key generated from another biometric template. It fully preserves the number of bit-errors in the original and the protected template to ensure recognition performance equivalent to the performance of the unprotected systems. We introduce Algorithm I and Algorithm II for bit-wise encryption; both are defined over cryptographic-primitives- block cipher-based encryption and keyed-hash function. We profile these algorithms on various hardware architectures to calculate the efficiency in terms of the time taken during enrolment and authentication phase. For Algorithm II, we observe that a 3.3 GHz desktop architecture takes about 18 milliseconds on an average of over 200 runs to authenticate a user. Additionally, we provide mathematical proof to show that the proposed scheme guarantees secrecy and irreversibility. The results of comparisons with the existing biometric template protection schemes on the various face and iris databases show that the proposed work provides significantly good recognition performance and efficiency, while it achieves high security. Finally, the bit-wise encryption scheme can be built over the commercial-off-the-shelf systems to achieve security with equivalent high performance.

Keywords: Multi-biometrics, cancelable biometric, bit-wise encryption, biometric security, fuzzy extractor