PhD THESIS SUMMARY

INFORMATION SECURITY USING BIO-CRYPTOGRAPHIC TECHNIQUES

Author: Ing. Marius-Alexandru VELCIU
E-mail: alexandruvelciu@gmail.com , Tel: 0745037750
PhD Supervisor: Prof. Dr. Ing. Victor-Valeriu PATRICIU

The study within the present paper is focused on the topic area of Bio-cryptography, aiming to highlight the main advantages conferred, to the detriment of tranditional biometric systems, and to research and implement methods of increasing the security level conferred by its encryption algorithms and reducing their computational complexity.

The 1st chapter presents the general framework of bio-cryptographic systems, followed by a brief review of thesis main objectives and its summary.

As part of *the 2nd chapter*, biometric systems roles and their architecture are presented, followed by main evaluation methods description, including error rates. The final of the chapter aims to emphasize biometric systems importance, in contrast with the main vulnerabilities they tend to exhibit.

The 3rd chapter describes the main bio-cryptographic operating modes, which allow cryptographic keys generation / regeneration, locking / unlocking or binding (also known as Biometric Encryption, the most representative and reliable bio-cryptographic systems operating mode).

The 4th chapter presents the most well known biometric encryption algorithm, the Fuzzy Vault bio-cryptographic scheme. In addition, an implementation of this scheme for Voice biometrics is proposed and evaluated, based on cepstral analysis method, used for speech parameterization.

The 5th chapter presents the main ways for evaluating bio-cryptographic algorithms. In its first part, Fuzzy Vault scheme specific parameters are described, including the order of magnitude for diffusion points, followed by the description of a method for evaluating Fuzzy Vault bio-cryptograms strength against brute-force attacks, reviewing the experimental results too. In addition, bio-cryptographic algorithms speed of execution is evaluated, directly related to the computational complexity of the mathematical processing they exhibit.

Within *the 6th chapter*, two methods for reducing Fuzzy Vault scheme computational complexity are proposed, the first one focused on the usage of Reed-Solomon error-correcting codes during the exhaustive polynomial reconstruction stage, and the second one based on the usage of shared bio-cryptograms, in order to eliminate the need for using diffusion points during the enrollment stage.

Chapter 7 tampers the Fuzzy Vault scheme vulnerability against correlation attacks and proposes an effective method to reduce it, the usage of biometric salted hashing.

The 8th chapter of the paper describes the main types of bio-cryptographic infrastructures, both for medium-scale and large-scale use, and proposes the usage of such a model to secure access to a shared storage environment. In the end, a bio-cryptographic protocol for secure messages exchange is presented, along with the possibility of its application in the mobile computing, in order to secure access to files on a mobile device or to encrypt conversations between two speakers.

Within the 9th chapter, a bio-cryptographic framework for securing Android-based mobile devices is proposed, relying on integrated fingerprint sensor and symmetric encryption. Basically, a key locking / unlocking bio-cryptographic system architecture is built, where access to Android Keystore is granted through biometric authentication. In addition, TrustZone technology is taken into consideration for usage within the proposed framework, which materialized in the development of an application that allows files and directory encryption on-demand.

Paper ends with a review of the conclusions, which summarizes the entire topic addressed in this paper, together with the selective Bibliography, the entire material consulted during the research process.