ABSTRACT

The biometrics have been used as a solution for access control systems for many years, but the simple use of biometrics can not be considered as final and perfect solution. There are many risks that should not be ignored. Most problems are related to the transmission path between the system where the users require access and the servers where the captured biometric data is stored. Various types of attacks can be made by impostors who want to use the system improperly. Besides the technical aspects, there is the social aspect. There is a growing concern of users about both data storage and the misuse of their biometrics, which is an unique identifier and, being invariant in time , may be lost forever if compromised. The fact that several companies keep their biometric data in different servers is causing discomfort to users because it makes their biometric data more susceptible to attacks. In this thesis, the use of smart cards is adopted as a possible solution to the above problems. Smart cards prepared for multi-applications are used to perform biometric comparisons internally. Thus, it would not be necessary to use different servers because biometric features will always be on a single card in the possession of the owner. It was developed and implemented three different algorithms using different biometric identification characteristics: fingerprint, palmprint and iris. Considering the used memory, average execution time and accuracy, palm print biometrics obtained the best results, achieving minimum error rates and processing time lower than half a second.

Keywords: Biometrics. Smart cards. Minutiae. PalmCode. IrisCode