Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 100 (2015) 169 – 176

Procedia Engineering

www.elsevier.com/locate/procedia

25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM 2014

Security of Biometric Systems

Milan Adámek*, Miroslav Matýsek, Petr Neumann

Faculty of AppliedInformatics, Tomas Bata University in Zlin, Czech Republic

Abstract

There are many ways how to identify people and to provide their authorization of access to a specific area. This article describes the reliability of biometric systems that are commonly used to identify of people. The article aims to highlight the ways in which to disturb the security of biometric systems. There are describes techniques that can impair the reliability of equipment for fingerprinting. To test the reliability of the fingerprint was made series of measurements; the results are presented in the article.

Peer-review under responsibility of DAAAM International Vienna

Keywords: Fingerprint sensor; biometric systems; reliability; attack; fake fingerprint

1. Introduction

Currently growing demand to increase the safety of not only persons, objects and data, but also the reliability of the identification of persons. Traditional identification technologies (check identity documents, standard access systems based on subject or password authentication) are now at their limits. To increase the reliability of the identification of the person contributes biometric identification. Biometric identification is understood as a discipline that is interested in describing and measuring of anatomical - physiological features and behavioral traits. Commonly used methods of biometric systems include identification of fingerprint, palm, face, iris of the eye. Commonly used methods of biometrics include fingerprint identification, palm, face, iris of the eye.

* Corresponding author. Tel.: +420576035220; fax: +420576035555.
E-mail address: adamek@fai.utb.cz

Peer-review under responsibility of DAAAM International Vienna
doi:10.1016/j.proeng.2015.01.355

Typical areas where biometric identifications are used include:

- Criminology
- Tourism (Customs clearance and passport control)
- Control of movement of persons, counter-terrorism measures, monitoring the crowds
- Attendance and access systems
- Data protection, PC and other data sources
- Electronic banking, online payment transactions and more [1].

The general structure of a biometric identification system is shown in Fig. 1.

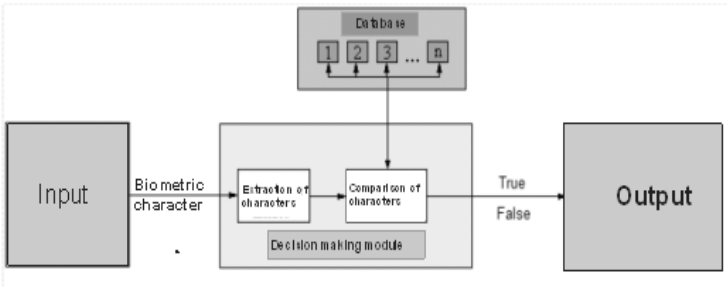

Fig. 1. Structure of a biometric identification system [2].

The basic component of a biometric identification system is a sensing module that ensures scanning of biometric characters. The major part is the decision-making module that compares the biometric features defined in the database. The output of the biometric identification system is the communication interface or lock allowing access to the space provided.

2. Access control systems using fingerprints

A fingerprinting is one of the best known biometric identification method. Usually the fingerprints are used in criminology, now they are widely used in commercial security. This method is based on the identification of the friction ridges of fingers (papillary lines). There are three basic patterns of classification of papillary lines, which are shown in Fig. 2.

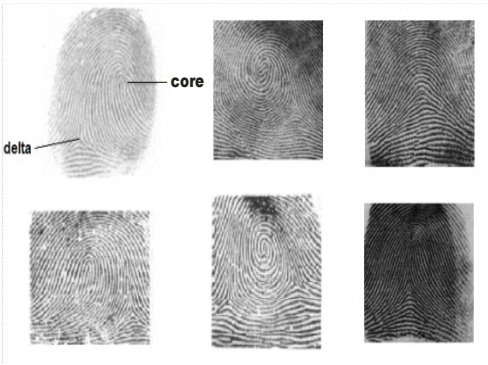

Fig. 2. Basic patterns (from left loop, swirl, arch) [2].