TECHNOLOGY

Method and Apparatus for Authenticating Biometric Scanners

OVERVIEW

Background

Using biometrics for authentication of people to systems provides convenience. When authenticating to mobile devices, such as smartphones, tablets and laptops, however, security problems may arise because this authentication typically takes place in unsupervised environments (e.g., at home). Since a mobile device can be easily stolen, an attacker with physical access to it can launch a powerful attack by manipulating the data which is acquired and transmitted by the biometric sensor. Furthermore, the biometric information has a low degree of secrecy as it can be captured by an unintended recipient and even without user's consent. Because the biometric characteristics are difficult to change and cannot be revoked, their compromise may lead to more serious consequences than, for example, a compromise of a password. Finally, regardless of all efforts to keep user's biometrics private, the widespread use of biometric technologies are set to make the biometric information essentially publicly available, with the face photos being public even today.

Innovative Technology

Using biometric information for identifying individuals typically involves two steps: biometric enrolment and biometric verification.

In order to overcome security problems associated with biometric scanners, researchers at the University of Maryland have developed methods and apparatuses which enhance the security of biometric scanners and systems by authenticating the scanner itself in addition to authenticating the submitted biometric information. By requiring authentication of both the information and the original scanner, the submission of counterfeit images can be detected, thereby preventing authentication of the counterfeit biometric image.

This technology uses unique, persistent, and unalterable characteristics of the sensors. It is also accurate, computationally efficient, and robust. Since it does not require any hardware modifications, it can be added to systems already put into service.

Advantages

- Does not require hardware modifications
- Customers can upgrade their system software, firmware and/or hardware
- Small computational burden to scanner system
- Suited for any system that uses biometric authentication
- Provides easy and user-friendly security to end-users

Applications

- Fingerprint authentication
- Computer, laptop, and cell phone security
- Banking applications
- Mobile commerce

• Health care records access

CONTACT INFO

UM Ventures
0134 Lee Building
7809 Regents Drive
College Park, MD 20742
Email: umdtechtransfer@umd.edu
Phone: (301) 405-3947 | Fax: (301) 314-9502

Additional Information

INSTITUTION

University of Maryland, College Park

LICENSE STATUS

Available for exclusive or non-exclusive license

CATEGORIES

- Information Technology

EXTERNAL RESOURCES

- US Patent 8,942,430
- US Patent 8,942,438
- US Patent 9,141,845
- US Patent 9,208,370

IS-2011-043