International Journal of Mobile Computing and Multimedia Communications
Volume 14 • Issue 1

Biometric Authentication Methods on Mobile Platforms:

An Introduction to Fingerprint Strong Feature Extraction

Agnitè Maxim Wilfrid Straiker Edoh, University of Abomey-Calavi, Benin*
Tahirou Djara, University of Abomey-Calavi, Benin
https://orcid.org/0000-0002-8591-6610
Abdou-Aziz Sobabe Ali Tahirou, University of Abomey-Calavi, Benin
Antoine Vianou, Université d'Abomey-Calavi, Benin

ABSTRACT

In this work, the authors propose a new biometric authentication system on mobile devices, enhancing security at these terminals and preserving user privacy. The proposed system uses a method of extracting strong features from minutiae with refinement of the method with regard to the further elimination of false minutiae by the calculation of geometric information (orientations and distances between minutiae) to obtain true terminations and stronger bifurcations facilitating the recognition of individuals. A series of tests carried out using a recognition and authentication application allowed us to achieve a false rejection rate of 13.81% and a false acceptance rate of almost zero (0.021%). The authors also propose a security model using hash functions and a random number to make the recognition system revocable, more difficult to compromise and thus reducing the risk of usurpation.

KEYWORDS

Biometric Authentication, Fingerprint, Minutiae Extraction, Mobile Devices, Recognition, Strong Features

INTRODUCTION

With the current digitization of most administrative services, e-government, mobile payments, remote healthcare, the advent of COVID 19 where exchanges must be done mostly online and so on, and because of the large number of identity-theft cases, the authentication step is often considered the weakest link in computer security (Belguechi, 2015). For the authentication of an individual, the password is by far the most widespread method despite its obvious lack of security (password cracker, eavesdropping, etc.) and its very limited ease of use when the user wishes to access a multitude of services (use of several passwords for several applications).

DOI: 10.4018/IJMCMC.334130

*Corresponding Author

Biometric authentication, which is used to recognize an individual based on physiological or behavioral characteristics, is an interesting alternative. For example, it is extremely rare to lose one's fingerprints, unlike passwords. It is also easier for users to put their fingers on a sensor or to capture their faces than to enter a password. As far as smartphones are concerned, the means of biometric authentication are various, such as fingerprints, facial captures, graphic patterns, voice, gait, or even keyboard speed. However, users are not usually aware that they are storing their enduring physiological or behavioral characteristics on unsecured platforms (i.e., on cell phones or cloud storage), threatening the privacy of their biometric patterns and identities.

In recent years, biometric authentication has attracted much attention from academics and industries. The more people trust biometric authentication systems, especially on their personal devices such as smartphones, the more they reveal their identities to third parties. Due to the enduring characteristics of biometrics such as fingerprints, face, or behavioral traits, the increasing use of biometrics will increase the risk of identity theft. Therefore, secure, robust, privacy-preserving authentication systems are required to prevent unauthorized access to sensitive and personal information stored on mobile devices.

The main objective of this work is to strengthen biometric authentication methods on mobile phones, particularly by fingerprint. This objective has two sub-objectives: to provide methods to avoid identity theft with regard to fingerprint authentication and to strengthen authentication to avoid information leakage from the biometric model.

In this work, we present a novel privacy-preserving biometric authentication system for mobile users. The proposed system, unlike other research efforts, leverages the hardware security of smartphones and demonstrates its potential for secure authentication with faster and more accurate performance and low resource consumption. This work makes the following contributions: a new strong-minutiae extraction method for the elimination of false minutiae and completeness of the security model of authentication of mobile platforms by fingerprint by proposing a secure authentication system based on the strong-characteristics method and encryption using a random number and hash functions for information transformation after studying some of the authentication schemes used in the mobile-device domain for secure and fast authentication with respect to fingerprints.

LITERATURE REVIEW

Traditional Authentication Methods on Mobile Devices

The most popular authentication methods are PIN and password, pattern-lock, and physiological authentication.

Password and PIN Authentication

A major difference between desktop and mobile authentication is that mobile users are not restricted to a particular location and settings; therefore, users are free to use their mobile devices to access and use password-protected services (e.g., online banking and email services) anytime and anywhere (Maydebura et al., 2013). In the process of these authentications, user credentials are verified at the beginning of the session. If the verification is successful (e.g., the correct password or PIN is entered), access is granted; otherwise, access is denied (Fig. 1). The session remains valid until the user logs out or closes the session.

Pattern-Lock Authentication

Pattern-based authentication is also a popular form of authentication on many mobile devices today. These authentication methods involve a user entering a pattern in order to authenticate. This typically involves connecting dots to complete the pattern, as shown in Fig. 1. If the wrong pattern is entered, the device will not authenticate the user, and if the pattern is increasingly incorrect, the device uses a

Related Content