International Journal of Distributed Artificial Intelligence
Volume 11 • Issue 1 • January-June 2019

Biometric Systems in Mobile Devices
A Study

Sukhdev Singh, Kurukshetra University, Kurukshetra, India
Chander Kant, Kurukshetra University, Kurukshetra, India

ABSTRACT

Growth of mobile devices uses has favored the user experience with different digital platforms, from basic activities such as sending messages, phone calls, taking pictures for social networks, email, bank account management, and commerce. These are some examples of daily tasks performed from mobile devices, which makes it essential to provide security of information. Therefore, privacy of stored information has become a main point in the development of mobile devices. This article presents research about the impact that mobile devices have in people's lives and the presence of biometric systems in this kind of device. Papers related with biometrics on mobile devices were examined to find which devices have integrated biometric systems; in addition to identifying biometric features used to authenticate people and find out what mobile platforms were created for. It was found that the smartphone is the device with more biometrics systems, and fingerprints are the most used feature; also, that the Android operating system is the most widely used mobile platform for these purposes.

KEYWORDS

Biometrics, Mobile Devices, Operating Systems

INTRODUCTION

Currently the use of mobile devices has been exciting enormous boom due, to a greater extent, to the weight and size of these devices, which offers the possibility to take them practically anywhere; to its ability to connect to the internet and other devices; besides its costs are accessible. Due to the advance technological, mobile devices handle different types of information such as: personal, health, banking, and labor, among others; this implies that your level of security must be sufficient to maintain the privacy of device content. Various security mechanisms have been used in the protection of the information of the devices mobile phones, including passwords and patterns. However, there is a risk that the user may forget them or that someone else stolen and uses them (Yang & Bal, 2012). To deal with this situation there are other means that provide the possibility to protect the content of the device more reliable way than typical methods; and these are biometric systems (Tao & Veldhuis, 2010; Ben-Asher, Sieger, Ben-Oved, Kirschnick, Meyer, & Moller, 2011).

Biometric Systems

Biometric systems use automated methods to recognize or verify a person's identity based on physical characteristics (face, fingerprint, iris and finger knuckle print), or behavioral characteristics (voice, signature, gait) (Jain, Ross, & Prabhkar, 2004). A biometric recognition system consists of the following stages as shown in Figure 1:

DOI: 10.4018/IJDAI.2019010102

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

- Acquisition: the biometric feature is acquired from user through a device.
- Pre-processing: the acquired data are processed to locate the used biometric pattern, which involves remove information that does not belong to the biometric characteristic.
- Extraction of characteristics: the results extract by the previous stage from user's characteristics are converted into numerical characteristics.
- Classification: the extracted characteristics are compared to the previously stored pattern.
- Take decision: this phase is used to make the final decision about the identity of the user.

Biometric Traits

The identity of a person can be known through its features or biometric characteristics, whether physical and behavioral. The physical features include, for example: the face, the fingerprint, the iris, the retina, hand geometry, finger knuckle print and the ear. The behavioral traits contain: the voice, the writing, gait, the way in which user puts pressure on the screen or keyboard of the device (keystroke), among other.

Biometric Systems in PDA

The number of people using PDA (Personal Digital Assistant) is smaller as compared to those who use devices like smart phone (10 million PDA's: hundreds of millions of smart phones). However, it must maintain the safety of the devices and an alternative to this is to include biometric systems in the PDAs for provide protection to user information. Among the biometric features mostly used in these types of devices are found: writing and keystrokes (Clark, Furnell, & Reynolds, 2012; Zoebisch & Vielhauer, 2003).

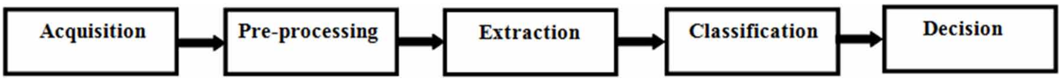
Biometric Systems in Smart -phones and Tablets

Currently, smartphones are the most used mobile devices (Clark, Furnell, & Reynolds, 2012); maintain the privacy of user's content has become a sensitive topic and company are responsible for producing the such application and devices which remain safe and secure. The biometric systems integrated into these devices are an alternative for the safety of these. Among the most used biometric features in these mobiles are: the face, the fingerprint, the iris, the voice, and keystroke. To implement these biometric features there are some parts of the device are: the keyboard, the accelerometer, the global positioning system (GPS), the camera and the microphone (Yang & Bal, 2012; Saevanee, Clarke, & Furnell, 2012; Vildjiounaite, Makela,, Lindholm, Kyllönen, & Ailisto, 2007; Trewin, Swart, Koved, Martino, Singh, & BenDavid, 2012; Derawi, Nickel, Bours, & Busch, 2010; Derawi, Yang, & Busch, 2012; Ijiri, Sakuragi & Lao, 2006; Seo, Kim, & Kim, 2012; Kang, 2010; Kurkovsky, Carpenter, & MacDonald, 2010; Kwapisz, Weiss, & Moore, 2010).

Biometric Systems in Smart Watches

The biometric systems incorporated in mobile phones are mainly focused on smart phones and tablets devices, however a new opportunity with the use of smart watches. The smart watches gain popularity among people thanks to the fact that they present a new way of interacting with the applications because the technology of a mobile device is literally within reach of the hand; besides that they have programs such as: messaging, multimedia, weather prediction, likewise have applications dedicated to monitoring the state of health of the user, among others. As the consumption of these devices, manufacturers

Figure 1. Phases of a biometric system



5 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/biometric-systems-in-mobile-devices/248479

Related Content

Exploiting the Overlapping of Higher Order: Entities within Multi-Agent Systems

Hosny A. Abbas (2014). *International Journal of Agent Technologies and Systems (pp. 32-57).*

www.irma-international.org/article/exploiting-the-overlapping-of-higher-order/122471

An Unmanaged Intersection Protocol and Improved Intersection Safety for Autonomous Vehicles

Kurt Dresner, Peter Stoneand Mark Van Middlesworth (2009). *Multi-Agent Systems for Traffic and Transportation Engineering (pp. 193-217).*

www.irma-international.org/chapter/unmanaged-intersection-protocol-improved-intersection/26939

Detecting Generic Music Features with Single Layer Feedforward Network using Unsupervised Hebbian Computation

Sourav Dasand Anup Kumar Kolya (2020). *International Journal of Distributed Artificial Intelligence (pp. 1-20).*

www.irma-international.org/article/detecting-generic-music-features-with-single-layer-feedforward-network-using-unsupervised-hebbian-computation/265563

Virtual Worlds and the Implication for Accountants: The Case of Second Life

Jorge A. Romero (2009). *International Journal of Agent Technologies and Systems (pp. 45-50).*

www.irma-international.org/article/virtual-worlds-implication-accountants/3871

Towards Distributed Association Rule Mining Privacy

Mafruz Ashrafi, David Taniarand Kate Smith (2007). *Application of Agents and Intelligent Information Technologies (pp. 245-271).*

www.irma-international.org/chapter/towards-distributed-association-rule-mining/5116