Perspective
Volume 13:2, 2022

Journal of Biometrics & Biostatistics

ISSN: 2155-6180 Open Access

Adoptable and Secure Biometrics in Smart Devices

Andre Michaud*

Department of Technology, Sloan School of Management, Cambridge, Massachusetts, USA

Introduction

A biometric system is a type of recognition system that determines the validity of a user's physiological or behavioural characteristics. The enrollment module and the identification module are the two steps of the biometric system. The enrollment module's job is to teach the system how to recognise a specific person by scanning their physiognomy and creating a digital image of them. This digital depiction serves as a comparison template. The identification module is in charge of recognising a specific individual by capturing their traits and turning them into the same digital format as the template. The identity module is split into two parts: identification and verification [1,2]. The system asks, "Who is X?" and tries to match "X" to every template in the database during the identification stage. The verification stage, on the other hand, requires the system to confirm that a user who claims to be "X" answers and solves the question "Is this X?"

Description

The digital age has brought with it a plethora of interactive devices, ranging from smartphones to smart appliances, all of which provide critical services to their users [3]. These gadgets can also communicate with one another through the internet, constituting the Internet-of-Things, a network of internet-connected devices (IoT). Around the world, there were an estimated 22 billion IoT devices in use, with that figure expected to rise to 50 billion by 2030. The IoT market's quick growth has ushered in new applications and services, such as smart fitness tracking and home automation that improve people's quality of life. Many smart cities across the world are using IoT-based applications and services to provide people with community- and city-level smart services including smart mobility and smart grids [4].

With widespread usage in smartphones and smart devices for user identification, fingerprint technology has become nearly universal. Unlike face biometrics, which present privacy concerns, iris detection has a low degree of freedom, and voice authentication has a poor level of resilience, fingerprints have a high level of societal acceptance due to their uniqueness and convenience. The need to track vital signs, automate daily tasks, and improve quality of life promotes the growth of various smart devices in today's digital world. According to Gartner, a typical family house will include 500 smart objects by 2022. Smart gadgets will undoubtedly continue to rely on biometrics to protect the smart environment, with the fingerprint being the first choice as the key to a user's personal data [5].

Conclusion

The eigenface technology is unique in that it alters the lighting of the shown face by employing different scales of light and dark in a precise pattern. Because of the different light and dark areas computed on the face, the presented image no longer seems like a face. However, the pattern formed by the shaded areas is crucial because it depicts and calculates how the distinct characteristics of the face are identified and the symmetry of the face. The pattern is estimated to a degree of eigenfaces, or eigenvectors, which is dictated by the size of facial features or the presence of facial hair. When calculating a face, different numbers of eigenvectors might be used to facilitate reconstruction. The usual approach employs roughly 150 eigenfaces, yet it is possible to accurately rebuild the face using only 40.The history and current achievements of facial biometrics and the security elements it handles, as well as the hopeful future following that, we discuss the various uses of facial biometrics, both current and hypothetical. Then we go over and try a few of the available mobile apps that use facial biometrics. Finally, we look at security, investigating why present verification and authentication methods are insecure and proposing new approaches that we believe are more safe.

References

1. Pankanti, Sharath, Ruud M. Bolle, and Anil Jain. “Biometrics: The future of identification.” *Computer* 33 (2000)**:** 46-49.

2. Haller, Matthew I., and Butrus T. Khuri-Yakub. “A surface micromachined electrostatic ultrasonic air transducer.” *IEEE Trans Ultrason Ferroelectr Freq Control* 43 (1996): 1-6.

3. Lu, Yipeng, Hao-Yen Tang, Stephanie Fung, and Bernhard E. Boser, et al. “Pulse-echo Ultrasound imaging using an AlN piezoelectric micromachined ultrasonic transducer array with transmit beam-forming.” *J Microelectromech Syst* 25 (2016): 179-187.

4. Wang, Tao, Takeshi Kobayashi, and Chengkuo Lee. “Micromachined piezoelectric ultrasonic transducer with ultra-wide frequency bandwidth.” *Appl Phys Lett* 106 (2015): 013501.

5. Chen, Yuan-Quan, Yu-Xing Li, Yan Chen, and Zhen-Yi Ju, et al. “Large-scale and high-density pMUT array based on isolated sol-gel PZT membranes for fingerprint imaging.“ *J Electrochem Soc* 164 (2017): B377-B381.

How to cite this article: Michaud, Andre. “Adoptable and Secure Biometrics in Smart Devices.” J Biom Biostat 13 (2022):92.

***Address for Correspondence:** Andre Michaud, Department of Technology, Sloan School of Management, Cambridge, Massachusetts, USA; E-mail: srp2@srpinc.org*

Received: 30 January, 2022, Manuscript No. jbmbs-22-64662; **Editor assigned:** 01 February, 2022, PreQC No. P-64662; **Reviewed:** 15 February, 2022, QC No. Q-64662; **Revised:** 20 February, 2022, Manuscript No. R-64662; **Published:** 26 February, 2022, DOI: 10.37421/2155-6180.2022.13.92