Engineering technology open access Journal
ISSN: 2641-8185

Juniper Publishers
key to the Researchers

Mini Review
Volume 1 Issue 3 - April 2018
DOI: 10.19080/ETOAJ.2018.01.555562

Eng Technol Open Acc

Biometric Techniques: A Mini-Review

Huang L[1]* and Xinzhe C[2]

[1]*Department of Engineering technology, Metropolitan State University of Denver, USA*

[2]*Department of computer Engineering, Colorado State University, USA*

Submission: January 31, 2018; **Published:** April 02, 2018

***Corresponding author:** Lin Huang, Engineering and Engineering Technology, Metropolitan State University of Denver, USA, Email: lhuang1@msudenver.edu

Abstract

Biometrics is the body measurement and statistical analysis of people's unique biological traits. It has been applied for identification and access control. This mini-review paper will provide you with comparison of the biometric technologies based on different biological traits for identification and authentication. In addition, this paper also discusses the challenge and controversy in the area of biometric person recognition.

Keywords : Biometrics; Recognition; Security; Technology

Introduction

With the development of Engineering and Technology, it is becoming extremely important and critical to reduce the threats in privacy, personal safety and public security in 21st century. Biometrics is the technology of measuring and analyzing biological data of human subjects involved for person authentication or identification purposes. Its progress in recent years has brought in many civilian, military and government applications. It is believed that biometric technology is the most ideal solution to ensure the security and privacy of our personal information, and let us have confidence in identification systems [1].

Biometrics apply for different biological traits, such as fingerprints, irises, retinas, signatures, voices, faces, etc. (Figure 1) to recognize a person [2]. There are many debates about the merits and demerits of different biometric systems. This paper presents the description and advantages/disadvantages of the most popular ones listed in Table 1.

Table 1: Different Biometric Solution Comparison.

Technology	Pros	Cons
Face Use geometry of distinguishing face features [3]	1. Easy to collect 2. Cheap sensor 3. Less enrollment time needed 4. Many vendors and products available	1. Impacted by age, injury, plastic surgery or more temporary changes such as sunglasses, make-up or growing a beard [4] 2. Hard to distinguish identical twins [2] 3. Privacy concerns when using a surveillance system [5] 4. Affected by the quality of the camera, the control of the surroundings and algorithm [5]
Fingerprint Use minutiae	1. Less enrollment time needed 2. Ease acquisition 3. Unique fingerprints to each person 4. Small fingerprint sensor 5. Many vendors and product choices available	1. Injury interfering with the scanning process 2. Low people acceptance rate 3. Fingerprint scanners are too fidgety for everyday use 4. Incompatible technologies and standards among vendors/products

Iris Analyze the pattern of blood vessels on the retina	1. Internal organ that is well protected against damage and wear 2. Remarkably stable with less data storage 3. Non-intrusive 4. Used at a certain distance (contactless) 5. Fast matching speed of matching 6. Extreme resistance to false matches 7. Considered to be most accurate of all biometrics	1. Incompatible with the very substantial investment 2. Effective distance limited to a few meters 3. Not reliable when the person is not standing still 4. Susceptible to poor image quality 5. Suffering with higher failure enrollment rates 6. Special lighting required 7. Special scanner required
Voice Analyze speech idiosyncrasies	1. Reliable and easy to use 2. Cheap sensor 3. High public acceptance rate 4. No contact required	1. Easily recorded by someone else 2. Big file storage 3. Affected by environmental factors such as background noise
Palmprint Based on ridges and bifurcations, scars, creases [6]	1. Simple in feature extraction 2. Short processing time 3. High resolution not required 4. Not sensitive to noise	1. More processing time 2. Bad performance if fingers are widely spread 3. Not very reliable method
Hand Geometry Use dimensions and shape of the hand, palm size, finger length and width, knuckle's distance [7]	1. Simple, relatively easy to use 2. Inexpensive 3. Easier to collect data 4. Environmental factors friendly 5. Usually less intrusive than other technology	1. Not unique 2. Not used in identification systems 3. Not ideal for growing children 4. Large data size to store
Signature The activity such as stroke order, pressure applied and the speed	1. Extremely difficult to mimic the behavior of signing 2. Low False Acceptance Rates (FAR) 3. Not perceived to be invasive.	1. People may not always sign in a consistent manner
Keystroke Based on the typing rhythm/pattern	1. No special hardware needed Difficult to mimic the behavior	2. Less reliable 3. Typing rhythm varies considerably in between days and even within the same day 4. Applicable legislation is sufficiently unclear 5. Higher FAR and FRR due to higher variations in behavior

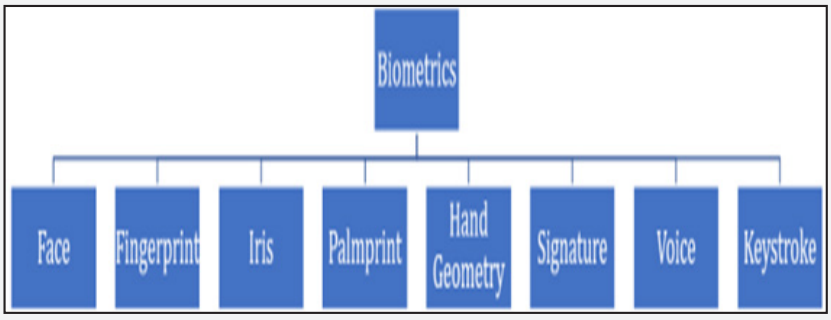

Figure 1 : Different Biometric Technologies.

How to cite this article: Huang L, Xinzhe C. Biometric Techniques: A Mini-Review. Eng Technol Open Acc. 2018; 1(3): 555562.
DOI: 10.19080/ETOAJ.2018.01.555562

Discussion

Biometric solution can be applied for a wide range of security areas, including access control, time and attendance management, surveillance, and boarder control, etc. Among those solutions, face recognition has been used in projects to identify card counters or other undesirables in casinos, shoplifters in stores, criminals and terrorists. Fingerprint recognition has been applied in US-VISIT program [8]. IAFIS system with over 47 million subjects is maintained by the FBI Criminal Justice Information Services (CJIS) and includes automated ten-print and latent fingerprint search. The Canada-US Fast Track Nexus program utilizes iris recognition to manage frequent travellers to pass through boarder.

Biometric solutions are also facing challenges. The use of biometric data might be compromised by any unauthorized party and used for other purposes which are different from the original consents or agreements. Another risk is that the biometric data can be captured during their transmission to the central database and fraudulently replicated in another transaction.

The challenge of biometrics also includes how to develop and commercialize the systems by addressing all needs for biometrics and achieving all potential benefits. Moreover, the system should work for everyone and everywhere with 100% accurate rates under all kinds of conditions and environments. Data storage should also be small with fast recognition speed. It is a tough job.

References

1. Li, Stan Z, Jain AK (2015) Encyclo pedia of Biometrics, (2nd edn), Springer, New York, USA.
2. Nagpal R, Nagpal P, Malhotra S (2012) "Biometric Techniques and Facial Expression Recognition-A Review", Journal of Global Research in Computer Science 3(11): 69-76.
3. Park U, Tong Y, Jain AK (2010) "Age Invariant Face Recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence 32(5): 947-954.
4. Deb D, Best Rowden L (2017) Jain AK "Face Recognition Performance Under Aging", in CVPR, Workshop on Biometrics, Honolulu, HI, USA .
5. Huang L, Zhuang HQ, Morgera SD (2009) "A method towards face recognition", International Journal of Intelligent Systems Technologies and Application 7(3): 282-295.
6. Jain AK, Feng J (2009) "Latent Palm print Matching", IEEE Trans. PAMI 31(6): 1032-1047.
7. Jain AK, Nandakumar K, Ross A (2016) "50 years of Biometric Research: Accomplishment, Challenge & Opportunities", Pattern Recognition Letters 79: 80-105.
8. Documents, Palm Print Recognition 121-127.

DOI: 10.19080/ETOAJ.2018.01.555562

How to cite this article: Huang L, Xinzhe C. Biometric Techniques: A Mini-Review. Eng Technol Open Acc. 2018; 1(3): 555562.
DOI: 10.19080/ETOAJ.2018.01.555562