ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

Volume - 5, Issue - 2, March – April - 2019, Page No. 143 - 146

Biometric Recognition

[1]Geetanjli Bakshi, [2]Pradeep Jha, [3]Shilpi Mishra, [4]Sudhanshu Vashistha, [5]Hari Mehta

[1]B.Tech Student, Department of CSE, Arya College of Engineering and Research Centre, Jaipur

[2,3,4,5]Assistant Professor, Department of CSE, Arya College of Engineering and Research Centre, Jaipur

Abstract

In this paper an overview of the main topics related to biometric security technology is going to be discussed. In comparison to traditional method, biometric recognition is safe and easy. In 2017, over half billion stolen accounts in the world and almost 17.8 million violated domains are taken into consideration. In today's scenario, technology is improving day by day which lead to the emergence of various new technologies and authentication system. By American analysis company Tatrica, $69.8 billion is the turnover of companies in the biometric sector in 2025 with an annual growth rate of 22.9%. Threats are increasing day by day which continuously pushing companies to adapt new technologies.

Keywords: Immutability, Individuality, verification, validation

Introduction

The word Biometrics is derived from the Greek words "bios" means life and "metrikos" means measure. It is a science which involves the statistical analysis of biological characteristics. We will use the short term "biometrics" to refer to "biometric recognition of people". It is a hardware based system which is used for data acquisition which integrate the software components which allow, with the help of mathematical algorithms which perform data analysis and reconstruct the identity of a person. Biometric refers to something you are or something you do, there is no need to remember any token.

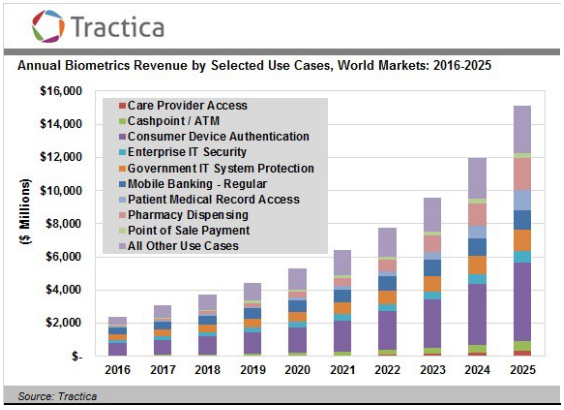

Fig 1: Annual Biometric Revenue

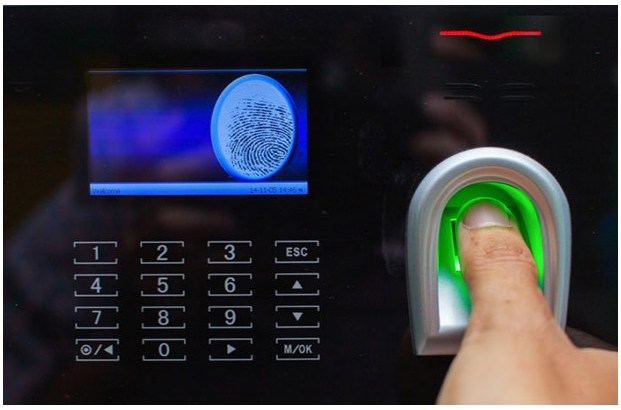

Fig 2: Biometric example

From fingerprint to facial and vocal recognition:

Along with fingerprint, facial and vocal recognition are also come into account. Now fingerprint has become widely used security system around the world. Its foundation has two peculiarities:

- **Immutability**: The characteristics of the prints do not change over time;
- **Individuality**: The imprint is unique from individual to individual.

The biometric System on iris scanning is growing considerably. The coloured portion of the eye results in a univocal code for every individual and hence allows the recognition. **Vocal recognition** made its first entry in 1952 with a system that recognizes spoken figures. BY introducing various voice assistants the analysis company Strategy Analytics estimated that the **hardware devices** (such as Alexa and Google Home) will exceed 15 million sales by 2022 compared to 3 million sold in 2017.

Fig 3: Voice recognition

Advantages:

- It is quite standard, although moving to a different country, facility, etc.
- It is a simple and economical method.
- It cannot be lost, forgotten, guessed, stolen, shared, etc.
- It is quite easy to check if one person has several identities.
- It can provide a greater degree of security than the other ones.

Disadvantages

- It can be stolen**.**
- A fake one can be issued.
- It can be shared.
- One person can be registered with different identities.
- It can be guessed or cracked.
- Good passwords are difficult to remember.
- It can be shared.
- One person can be registered with different identities.

Verification and validation

Biometric systems is operated in two modes: identification and verification.

Identification: In this, the identity isn't claimed by the user. the automated system mechanically determines the user's identity. If the user belongs to a bunch of predefined users, then this can be a closed game definition, however the noted (learned) user cluster by system is definitely smaller than the quantity of individuals World Health Organization will attempt to enter. the final scenario that a system has got to manage with users not within the info is named open identification. Adding the "None of the above" choice to the closed cluster definition permits USA to possess AN open group definition. System performance are often evaluated victimisation the speed of identification.

verification: In this, the aim of the system is to examine if the person is that the one World Health Organization claims to be. As a result, the user should give AN identity and also the system merely accepts or rejects users supported verification. Most of the time, the operation methodology is named authentication or discovery. Performance system performance are often evaluated victimisation the incorrect acceptance rate (FAR, the things during which the fraudster is accepted) and also the wrong reject rate (FRR, these are things wherever the user is incorrectly rejected), noted within the theory of detection as warning and Miss, severally . Performance are often raised in one {in all|one amongst|one in every of} the characteristics of the receiving operator or in a detection error adjustment. this offers uniform treatment to any or all sorts of errors and uses a graduated table.

Fig 4: All types of biometric recognition

Conclusion

Biometric Systems have proved very successful both on the technical level and as a reservoir of expertise. They have replaced the traditional method of identification . It are often detected that fingerprint primarily based bioscience system is reliable ,accurate and secure. As per because the current electronic security systems are involved, they bank totally on personal identification to make sure that a shopper is a licensed user of a system, have a typical penetrability: the verification are often duplicated which may be sorted exploitation bioscience. In today's scenerio, bioscience are often utilized by varied organizations to extend security levels and defend their information and patents. it's not the ultimate alternative of the plenty due to its high value and legal issues like privacy issues.

References

[1] R. Clarke “Human identification in information systems: management challenges and public information issues”. December 1994. Available in http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

[2] S. Furui Digital Speech Processing, synthesis, and recognition., Marcel Dekker, 1989.

[3] A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, “The DET curve in assessment of detection performance”, V. 4, pp.1895-1898, European speech Processing Conference Eurospeech 1997

[4] A. J. Mansfield, J. L. Wayman, “Best Practices in Testing and Reporting Performance of Biometric Devices”. Version 2.01. National Physical Laboratory Report CMSC 14/02. August 2002.

[5] M. Faundez-Zanuy “Door-opening system using a low-cost fingerprint scanner and a PC”. IEEE Aerospace and Electronic Systems Magazine. Vol. 19 nº 8, pp.23-26. August 2004

[6] M. Faundez-Zanuy y Joan Fabregas “Testing report of a fingerprint-based door-opening system”. IEEE Aerospace and Electronic Systems Magazine Vol.20 nº 6, pp 18-20, ISSN: 0885-8985. June 2005..

[7] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar “Handbook of Fingerprint Recognition” Springer professional computing. 2003

[8] M. Faundez-Zanuy “Technological evaluation of two AFIS systems” IEEE Aerospace and Electronic Systems Magazine Vol.20 nº 4, pp13-17, ISSN: 0885-8985. April 2005.

[9] M. Faundez-Zanuy “Are Inkless fingerprint sensors suitable for mobile use? IEEE Aerospace and Electronic Systems Magazine, pp.17-21, April 2004