

Advancements in Biometric Sensors: Revolutionizing Identification and Security Systems

Flemingo Kiming*

Department of Biostatistics, University of Dhaka, Dhaka, Bangladesh

Abstract

Advancements in biometric sensors were already shaping the landscape of identification and security systems. However, it is essential to note that further developments might have occurred since then. Here's a brief overview of the potential advancements up to that point. Biometric sensors, such as fingerprint scanners, iris scanners, and facial recognition systems, have seen significant improvements in accuracy and reliability. This ensures more precise identification and reduces the chances of false positives and false negatives.

Keywords: Biometric sensors • Biometric technology • Behavioral biometric

Introduction

Biometric technology has long been a fascination for science fiction enthusiasts, but in recent years, it has become an integral part of our daily lives, revolutionizing identification and security systems. Biometric sensors utilize unique physical and behavioral traits of individuals to establish their identity, replacing traditional password-based authentication with more secure and convenient methods. From unlocking smartphones to safeguarding sensitive facilities, these advancements have made our lives safer and more efficient. In this article, we explore the remarkable advancements in biometric sensors and their impact on identification and security systems. Behavioral biometric sensors, on the other hand, focus on individual behavioral traits. These include voice recognition sensors, which analyze speech patterns, and signature recognition sensors, which assess unique writing styles. These sensors monitor subtle behavioral patterns that remain relatively consistent over time [1,2].

Literature Review

One of the most significant breakthroughs in biometric sensors has been the improvement in accuracy. Early biometric systems were plagued by high error rates, resulting in false positives and negatives. However, with advancements in technology, modern biometric sensors have become incredibly accurate. Fingerprint scanners, iris recognition, and facial recognition systems have achieved a level of precision that rivals traditional identification methods. This enhanced accuracy ensures that only authorized individuals gain access, reducing security breaches and unauthorized entry attempts. This streamlines the user experience and minimizes the risk of fraudulent activities. Healthcare is another area benefiting from biometric sensors. Patient identification using biometrics reduces medical errors and ensures accurate recordkeeping. Biometric sensors in hospitals and clinics help prevent identity theft and ensure proper administration of medications and treatments.

Wearable biometric devices for continuous authentication

To further enhance security, the concept of multimodal biometrics has gained popularity. Multimodal biometrics involve combining two or more biometric

Address for Correspondence: Flemingo Kiming, Department of Biostatistics, University of Dhaka, Dhaka, Bangladesh, E-mail: kiming46@edu.in

Copyright: © 2023 Kiming F. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Received: 27 March, 2023, Manuscript No. jbmbs-23-101636; **Editor assigned:** 29 March, 2023, Pre QC No. P-101636; **Reviewed:** 12 April, 2023, QC No. Q-101636; **Revised:** 17 April, 2023, Manuscript No. R-101636; **Published:** 25 April, 2023, DOI: 10.37421/2155-6180.2023.14.156

modalities to create a more robust identification process. For instance, a system might use both fingerprint and facial recognition to authenticate a user. By doing so, the chances of identity fraud are significantly reduced, as an intruder would need to replicate multiple biometric traits simultaneously, making it an almost insurmountable challenge. Advancements in miniaturization and cost reduction will make biometric sensors more accessible for widespread adoption. In response to the COVID-19 pandemic, contactless biometric technologies emerged as a game-changer. Traditional fingerprint scanners required physical contact, which raised concerns about hygiene and germ transmission. To address this, touchless fingerprint scanners and facial recognition systems were developed. Users can now authenticate themselves without touching any surfaces, promoting hygiene in public spaces while maintaining security [3].

Discussion

The integration of AI and machine learning algorithms has been a game-changer for biometric sensors. AI algorithms can analyze vast amounts of data, recognize patterns, and adapt to changes in biometric traits. This not only improves the accuracy of identification but also allows the system to learn and adjust to new environmental factors or potential threats. AI-powered biometric systems can detect anomalies and suspicious activities, making them invaluable in security applications. However, it is crucial to address privacy concerns and ensure robust security measures to protect the integrity of biometric data. Another significant advancement in biometric sensors is the capability of real-time authentication. Users no longer have to wait for their identity to be verified, as modern systems can provide instant responses for access control and security purposes. Whether it's unlocking a smartphone or accessing secure facilities, real-time authentication ensures a seamless and efficient user experience [4-6].

Conclusion

Advancements in biometric sensors have transformed identification and security systems, offering unparalleled accuracy, convenience, and security. From fingerprint scanners to facial recognition and wearable devices, biometrics has become an integral part of our lives. These advancements have not only made our daily interactions more secure but also found applications in finance, healthcare, law enforcement, and other industries. As technology continues to evolve, we can expect biometric sensors to play an even more significant role in shaping a safer and more connected future. However, it is crucial to strike a balance between security and privacy, ensuring that these advancements benefit society without compromising individual rights.

Acknowledgement

We thank the anonymous reviewers for their constructive criticisms of the manuscript. The support from ROMA (Research Optimization and recovery in the

Manufacturing industry), of the Research Council of Norway is highly appreciated by the authors.

Conflict of Interest

The authors declare that there was no conflict of interest in the present study.

References

1. Shopon, Md, Sanjida Nasreen Tumpa, Yajurv Bhatia and KN Pavan Kumar, et al. "Biometric systems de-identification: Current advancements and future directions." *J Cybersecur* 1 (2021): 470-495.
2. Tiwari, Shradha, J. N. Chourasia and Vijay S. Chourasia. "A review of advancements in biometric systems." *IJIRAE* 2 (2015): 187-204.
3. Munir, Rumaisah and Rizwan Ahmed Khan. "An extensive review on spectral imaging in biometric systems: Challenges & advancements." *J Vis Commun Image Represent* 65 (2019): 102660.
4. Ross, Arun and Anil Jain. "Biometric sensor interoperability: A case study in fingerprints." In *International Workshop on Biometric Authentication* (2004): 134–145.
5. Wang, Hee Seung, Seong Kwang Hong, Jae Hyun Han and Young Hoon Jung, et al. "Biomimetic and flexible piezoelectric mobile acoustic sensors with multiresonant ultrathin structures for machine learning biometrics." *Sci Adv* 7 (2021): eabe5683.
6. Aboalsamh, H. "Recent advancements in biometrics: Vein and fingerprint authentication." In *14th WSEAS International Conference on Computers (Part of the 14th WSEAS CSCC Multiconference)* (2010): 459-462.

How to cite this article: Kiming, Flemingo. "Advancements in Biometric Sensors: Revolutionizing Identification and Security Systems." *J Biom Biosta* 14 (2023): 156.