Opinion
Volume 13:2, 2022

Journal of Biometrics & Biostatistics

ISSN: 2155-6180

Open Access

Current Advancements of Biometric Systems De-identification

Nujeti Bindhu*

Department of Computer Science, Vignan's University, Andhra Pradesh, India

Introduction

We live in a culture where people's personal and social lives, professional affiliations, hobbies, and interests all become part of their public profile. Social network accounts or digital identities are a good example of how diverse aspects of a person's life become publicized. Decision making, information fusion, artificial intelligence, pattern recognition, and biometrics all benefit from the complicated relationships between online personalities and our actual world. In the information security arena, numerous research have examined intelligent algorithms and information fusion techniques. Machine learning and deep learning breakthroughs have created new ways to extract new knowledge from publicly available data, posing new concerns to user privacy. The performance of existing biometric identification systems can be impacted by merging de-identification with various types of auxiliary information that may be provided directly or indirectly, according to this review paper. The de-identification of biometric data to ensure user privacy is discussed analytically. This article also includes an overview of existing and emerging biometric research, as well as several unresolved problems of critical importance to information privacy and security experts. In an increasingly linked society, the answers to these concerns may aid in the creation of new biometric security and privacy preservation solutions [1,2].

Description

Privacy is a critical social and political issue with a diverse set of enabling and supporting technology and processes. Multimedia, big data, communications, data mining, social networks, and audio-video surveillance are some of these. De-identification became one of the key strategies for preserving the privacy of multimedia content, alongside traditional methods of encryption and discretionary access controls. De-identification is the process of changing or replacing personal identifiers in order to hide particular information from public view. Despite the compelling need for approaches that safeguard personal privacy while providing adequate biometric trait recognition, de-identification has not been a primary focus of biometric research [3].

In the literature on the subject, there is no consensus on a single definition of what de-identification is. De-identification, for example, is defined as "the act of concealing personal identifiers in personal information or replacing them with suitable surrogates to avoid the disclosure and use of data for purposes unrelated to the reason for which the data were originally obtained." "De-identification" is defined as "the reversible process of deleting or hiding any personally identifiable information from individual records in a way that reduces the danger of inadvertent revelation of individuals' identities and information about them." It entails the providing of additional information to allow, for example, an authorised entity to retrieve the original identifiers." While the fundamental purpose of de-identification is to safeguard user data privacy, how it is implemented varies dramatically depending on the application domain or the system's commercial value. In the sections that follow, we deconstruct the differences between de-identification strategies, build a taxonomy of de-identification techniques, and offer novel types of de-identification based on supplementary biometric data [4,5].

Conclusion

The field of biometric de-identification is substantially unexplored, with numerous intriguing research opportunities. The impact of the original data perturbation on primary biometric identification and auxiliary biometric estimates can be examined further. Furthermore, the development of realistic solutions for privacy-preserving video surveillance systems could arise from the construction of revolutionary deep learning architectures for sensor-based biometric de-identification. The acceptable level of biometric data obscurity while preserving other biometric data is up for debate. It was presented a comprehensive review of all de-identification approaches based on the modalities used and the sorts of biometric features that remained intact. Analytical conversations were held on ways to preserve physiological, behavioural, and social-behavioral biometric data in diverse applications. The study offered novel de-identification paradigms based on current breakthroughs in the biometric security domain: social biometric de-identification, sensor-based de-identification, emotion-based de-identification, and psychological traits de-identification.

References

1. Padilla-López, José Ramón, Alexandros Andre Chaaraoui, and Francisco Flórez-Revuelta. "Visual privacy protection methods: A survey." *Expert Syst Appl* 42 (2015): 4177-4195.
2. Ribaric, Slobodan, Aladdin Ariyaeeinia, and Nikola Pavesic. "De-identification for privacy protection in multimedia content: A survey." *Signal Process Image Commun* 47 (2016): 131-151.
3. Jain, Anil, Lin Hong, and Sharath Pankanti. "Biometric identification." *Commun ACM* 43 (2000): 90-98.
4. Sultana, Madeena, Padma Polash Paul, and Marina Gavrilova. "Social behavioral biometrics: An emerging trend." *Int J Pattern Recognit Artif Intell* 29 (2015): 1556013.
5. Meng, Li, Zongji Sun, and Odette Tejada Collado. "Efficient approach to de-identifying faces in videos." *IET Signal Process* 11 (2017): 1039-1045.

****Address for Correspondence:** *Nujeti Bindhu, Department of Computer Science, Vignan's University, Andhra Pradesh, India, E-mail: bindu.simh@gmail.com*

Received: 30 January, 2022, Manuscript No. jbmbs-22-64663; **Editor assigned:** 01 February, 2022, PreQC No. P-64663; **Reviewed:** 15 February, 2022, QC No. Q-64663; **Revised:** 20 February, 2022, Manuscript No. R-64663; **Published:** 26 February, 2022, DOI: 10.37421/2155-6180.2022.13.93

How to cite this article: Bindhu, Nujeti. "Current Advancements of Biometric Systems De-identification." J Biom Biostat 13 (2022): 93.