

Biometrics: Challenges and Opportunities (Keynote)

Vincenzo Piuri 

Computer Science Department, Università degli Studi di Milano
vincenzo.piuri@unimi.it

Biometric technologies and applications are pervasively permeating our everyday life.

Biometrics for user authentication, once typically used for restricting access to critical (physical or digital) environments, are now making their ways in everyday life applications and services, from the emerging fast-paced adoption of biometric passports and face boarding at the airports to the widespread use of face and fingerprint recognition for unlocking smart phones.

Biometrics are also seamlessly at the basis of many of the services and applications of today's smart society, from governmental and business services to leisure. Video cameras are increasingly being adopted in public places to respond to security needs or providing services in smart cities. Smart cars monitor the drivers facial expressions and movements to react in case of sleepy drivers. IoT and smart assistant devices and applications rely on voice recognition for user interactions. Advanced entertainment and e-commerce applications can acquire and process user facial or body postures for emotion and sentiment analysis. Adding to the examples, which show the richness of applications relying on biometrics when interacting with users, biometrics technologies are also behind other services operating offline and downstream, such as the longly debated automatic user tagging from images in social network applications.

The widespread adoption of biometrics, the enormous amount of biometrics data gathered, collected and processed, as well as advancements in artificial intelligence open new challenges and opportunities in the field of biometrics and biometric data processing. The importance and criticality of biometrics are also testified by their explicit mention and particular consideration in the Artificial Intelligence Act just approved by the European Parliament.

These advancements in applications call for novel biometric solutions, able to operate in new and emerging scenarios seamlessly and balancing the need of catering advanced services based on biometrics with the rightful desire for an ethical, secure, and privacy-respectful use of biometrics.

In this talk, I will illustrate the main biometrics techniques discussing their characteristics (e.g., universality, uniqueness, permanence, performance, and circumvention), strengths, limitations, and applications. I will also discuss challenges and research directions, with particular focus on opportunities from the application of AI.

Keywords: Biometrics · Privacy · Artificial Intelligence

Acknowledgements. This work was supported in part by the EC under projects EdgeAI (101097300) and GLACIATION (101070141), and by project SERICS (PE00000014) under the MUR NRRP funded by the EU - NGEU. Views and opinions expressed are however those of the authors only and do not necessarily reflect those

of the European Union or the Italian MUR. Neither the European Union nor the Italian MUR can be held responsible for them.

References

1. Abukmeil, M., Ferrari, S., Genovese, A., Piuri, V., Scotti, F.: A survey of unsupervised generative models for exploratory data analysis and representation learning. *ACM Comput. Surv.* **54**(5), 1–40 (2021)
2. Chen, C.F., Moriarty, B., Hu, S., et al.: Model-agnostic utility-preserving biometric information anonymization. *Int. J. Inf. Secur.* (2024). <https://doi.org/10.1007/s10207-024-00862-8>
3. Donida Labati, R., et al.: Biometric recognition in automated border control: a survey. *ACM Comput. Surv.* **49**(2), 24:1–24:39 (2016)
4. Donida Labati, R., Genovese, A., Piuri, V., Scotti, F., Vishwakarma, S.: I-SOCIAL-DB: a labeled database of images collected from websites and social media for iris recognition. *Image Vis. Comput.* **105**(104058), 1–9 (2021)
5. Genovese, A., Muñoz, E., Piuri, V., Scotti, F.: Advanced biometric technologies: emerging scenarios and research trends. In: Samarati, P., Ray, I., Ray, I. (eds.) *From Database to Cyber Security*. LNCS, vol. 11170, pp. 324–352. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-04834-1_17