

Chapter 1

Biometric Intelligence in the War Against Cybercrime and Identity Fraud

Kavita Kanwar

 <https://orcid.org/0009-0000-6661-891X>

Poornima University, Jaipur, India

Nikhil Kumar Goyal

 <https://orcid.org/0009-0007-4532-8033>

Poornima University, Jaipur, India

ABSTRACT

This chapter discusses the principles that underlie biometric systems, summarizes the usual strategies employed in digital identity frauds, such as deepfakes, spoofing and creating synthetic identity and reviews the strengths and weaknesses associated with the use of biometric in cyber investigation. Case studies in the real world depict the application of biometrics in criminal justice, border control as well as verification on mobile identity. Meanwhile the chapter discusses ethical, legal and privacy concerns of biometric data capture and application with examples of international laws like GDPR and HIPAA. Last, it discusses emerging trends such as AI-based biometric security, decentralized digital identity and privacy-respecting biometric protocols, and provides an in-depth perspective on the future of the cross-section of biometrics, cybersecurity, and biometric-based identity protection.

DOI: 10.4018/979-8-3373-4972-5.ch001

Copyright © 2026, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

1. INTRODUCTION

1.1 Biometrics in the Digital Age

The digital era has brought about an unparalleled number of demands of technology on identity authentication, information retrieval and safe transaction. Through this progression, biometric technologies have assumed prime integration into verifying persons through basis of their respective physiological and behavioral characteristics. Biometrics (such as fingerprints, facial characteristics, patterns in the iris, or even signs in the voice) can be used as a source of high confidence in identity confirmation to a greater extent than the usual passwords, ID cards, etc. They are especially useful when applied to the domain of digital access control and security because of their non-transportability properties, in addition to their infeasibility to forge (Adjerid & Kelley, 2018).

The increased dependence on biometrics in smartphones, banks, airport security, and even national identification systems is evidence of the increased faith in technologies. Biometrics does not only facilitate the authentication of its users, but it also plays a larger role in the field of cyber forensics and investigation. These two capabilities (preventative and investigational) mean that biometrics can be considered a staple to most digital security efforts today.

Nonetheless, the growth of the use of biometrics also brings along difficult questions dealing with the storage of data, surveillance and the consent of individuals. Due to the expected promotion of biometric systems in the common part of infrastructure, the risks of data losses, abuses, and unlawful surveillance rise. What makes the biometric identifiers so unique and undetermined is the absolute cause of their notoriety when compromised (Alsaadi & Tubaishat, 2015).

1.2 Rise of Cybercrime and Identity Theft

Cybercrime has become an advanced, unified menace which takes advantage of weak spots in digital networks, systems and even human nature. Digital identity theft is one among its numerous forms and is one of the most common and destructive forms. Hackers sell the stolen credentials to perpetrators so that they can utilize them to perpetrate fraud, gain access to sensitive information, or pretend to be a victim, which has long-term effects. As more and more personal information is kept on the Internet, the surface area of such attacks also increases.

Conventional authentication—username and passwords in this case have been found insufficient to counter the current threats in cyberspace. These certificates are simple to be phished, guessed, or leaked by means of information breaches. Because of this, even low-tech attackers are able to get unauthorized access to systems. The

28 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/biometric-intelligence-in-the-war-against-cybercrime-and-identity-fraud/402963

Related Content

Learning with Privileged Information for Improved Target Classification

Roman Ilin, Simon Streltsov and Rauf Izmailov (2014). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 50-66).

www.irma-international.org/article/learning-with-privileged-information-for-improved-target-classification/130620

Mobile Ad Hoc Network Routing Protocols for Intelligent Transportation Systems

Hamza Zembrane, Youssef Baddi and Abderrahim Hasbi (2021). *International Journal of Smart Security Technologies* (pp. 35-48).

www.irma-international.org/article/mobile-ad-hoc-network-routing-protocols-for-intelligent-transportation-systems/272100

Indoor Localization, Tracking and Fall Detection for Assistive Healthcare Based on Spatial Sparsity and Wireless Sensor Network

Mohammad Pourhomayoun, Zhanpeng Jin and Mark L. Fowler (2013). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 72-83).

www.irma-international.org/article/indoor-localization-tracking-and-fall-detection-for-assistive-healthcare-based-on-spatial-sparsity-and-wireless-sensor-network/93055

2D Image Matrix-Based Discriminator

David Zhang, Xiao-Yuan Jing and Jian Yang (2006). *Biometric Image Discrimination Technologies: Computational Intelligence and its Applications Series* (pp. 258-286).

www.irma-international.org/chapter/image-matrix-based-discriminator/5927

Intrusion Detection Using Deep Belief Network and Extreme Learning Machine

Zahangir Alom, Venkata Ramesh Bontupalli and Tarek M. Taha (2015). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 35-56).

www.irma-international.org/article/intrusion-detection-using-deep-belief-network-and-extreme-learning-machine/146244