Biometric Technology Today
ISSN (online): 1873-1880

The Role of Biometrics in Courtroom Evidence: Admissibility and Challenges

Dr. Amol Sapatnekar[1], Fulsundar Amita Purushottam[2], Vikas Haribhau Satonkar[3], Mandan Mishra[4], Dr. Namrata Kharate[5], Dr.Lalita Kiran Wani[6]

[1]Symbiosis Law School (SLS) Symbiosis International (Deemed University) (SIU) Vimannagar, Pune, Maharashtra, India.

[2]Sandip University Nashik, Nashik, Maharashtra, India. fulsundar.purushottam@sandipuniversity.edu.in

[3]Sandip Institute of Engineering & Management, Nashik, Maharashtra, India. vikas.satonkar@siem.org.in

[4]Sandip University Sijoul, Madhubani, Bihar, India. mandan.mishra@sandipuniversity.edu.in

[5]Vishwakarma Institute of Technology, Pune, Maharashtra, India. namratakharate1@gmail.com

[6]Bharati Vidyapeeth's College of Engineering, Lavale,Pune, Maharashtra, India. Email: lalita.wani@gmail.com

Abstract: Biometric technologies have emerged as powerful tools in modern legal systems, offering methods for identifying individuals based on unique physiological and behavioral traits. As these technologies become increasingly integrated into law enforcement, their role in courtroom evidence continues to expand, raising important questions about their reliability and admissibility. The proposed work examines the role of biometric evidence in courtroom settings, focusing on its admissibility and the challenges associated with its use. Biometric technologies, such as fingerprint recognition, facial recognition, iris scanning, and voice analysis, have become increasingly prominent in legal proceedings due to their potential for providing accurate, objective identification. However, questions arise regarding the reliability of these technologies, their legal admissibility, and the privacy and ethical concerns they raise. This paper explores the legal frameworks governing biometric evidence, examining standards such as the Frye and Daubert rules. Also, it analyzes key challenges, including technological limitations, error rates, and the potential for data manipulation. By reviewing relevant case studies and comparing international legal approaches, the paper aims to provide a comprehensive understanding of the current and future implications of biometric evidence in legal contexts. Recommendations for improving legal and ethical standards are also discussed to enhance its courtroom reliability.

Keywords: Biometric Evidence, Admissibility Standards, Courtroom Technology, Legal Framework, Privacy and Ethical Concerns.

Introduction

Biometric technology has become an integral part of modern law enforcement and legal processes, offering unique methods of identifying individuals based on their physiological or behavioral characteristics. Common biometric systems include fingerprint identification, facial recognition, iris scanning, and voice pattern analysis. These methods are widely used for personal identification and verification because they provide unique and relatively stable traits that are difficult to replicate or alter[1]. With advances in technology, biometric data has found increasing applications in criminal investigations, border security, and other law enforcement operations. Its usage has also extended into civil contexts, where identity verification is required, such as in financial transactions and access control systems.

The incorporation of biometric data as evidence in legal proceedings has introduced significant advantages. Unlike traditional evidence, such as witness testimonies, biometric data offers a higher degree of precision and objectivity. When properly collected and analyzed, it provides reliable and concrete proof, which is less prone to human error or manipulation. Due to its evidential strength, biometric data has gained traction in criminal trials, where it can

confirm the identity of suspects, establish presence at crime scenes, or refute allegations[2], [3]. The growing reliance on this technology in the courtroom is reflected in its increasing prevalence in legal cases worldwide.

The present works explore the role of biometric evidence within courtroom settings, with a particular focus on its admissibility and the challenges it presents. Key questions addressed include the reliability of biometric data, the legal standards required for its use in courts, and the ethical and technological issues that may arise. Through an analysis of current practices and case studies, this research will highlight the complexities of integrating biometrics into legal proceedings.

Biometric Technologies and Their Use in Law Enforcement

Biometric technologies offer several methods for identifying individuals by analyzing unique physical and behavioral characteristics. Fingerprint recognition is one of the oldest and most reliable methods, widely used in both criminal investigations and civil applications. DNA analysis provides highly accurate identification, particularly in cases involving forensic evidence. Facial recognition technology has gained prominence, often used in surveillance and suspect identification. Iris and retinal scans offer precise biometric data due to the unique patterns in individuals' eyes, while voice analysis is employed to verify identity through vocal patterns. These technologies provide law enforcement with diverse and reliable tools for identifying suspects and verifying identities[4], [5].

Application in Criminal Investigations

Biometric evidence plays a critical role in criminal investigations, aiding in identifying suspects, verifying alibis, and linking individuals to crime scenes. Fingerprints lifted from crime scenes or DNA recovered from personal items have been crucial in securing convictions. Facial recognition technology, increasingly used by police departments, assists in identifying suspects from video footage, often expediting investigations. These applications have significantly impacted the criminal justice system by enhancing the accuracy of investigations and reducing wrongful arrests[6].

Use in Civil Cases

Beyond criminal law, biometric technologies are used in civil cases, particularly in matters requiring identity verification. Biometric data is commonly utilized in personal dispute cases, such as inheritance claims or property rights, where confirming an individual's identity is vital. Additionally, biometric verification is used in various administrative contexts, including immigration processes, voter registration, and financial transactions, where identity fraud prevention is essential.

Legal Framework for the Admissibility of Biometric Evidence

The admissibility of scientific evidence in courts has evolved over time, with two key rulings shaping its foundation: the Frye standard and the Daubert ruling. The Frye standard, established in Frye v. United States (1923), requires that scientific evidence must be "generally accepted" by experts in the relevant field to be admissible. This standard, however, lacked flexibility in dealing with newer forms of scientific evidence, including biometric technologies[7], [8].

In 1993, the Daubert ruling (Daubert v. Merrell Dow Pharmaceuticals) modified the Frye standard by introducing a more rigorous set of guidelines for admissibility. The Daubert criteria focus on whether the scientific technique has been tested, peer-reviewed, has a known error rate, and follows established standards. Both the Frye and Daubert rulings remain relevant to biometric evidence, as courts assess whether these advanced technologies meet the criteria for reliability and general acceptance.

Country/Region	Admissibility Standard	Key Requirements for Biometrics
United States	Daubert Standard	Reliability, peer review, testability, error rates, general acceptance
United Kingdom	Civil Evidence Act 1995	Relevance, reliability, expert testimony on validation

European Union	ECHR, GDPR Compliance	Legal basis for data collection, proportionality, fairness, necessity
India	Indian Evidence Act 1872	Relevance, corroboration by expert testimony, reliability of data collection methods

Biometric evidence must meet specific legal criteria to be admitted in court, varying by jurisdiction. In the U.S., courts follow the Daubert standard, focusing on the reliability and scientific soundness of the method. The U.K. emphasizes the relevance of the evidence, relying heavily on expert validation. In the E.U., compliance with data protection laws such as the General Data Protection Regulation (GDPR) is necessary, ensuring biometric data is collected and used lawfully. India's legal framework focuses on the reliability and corroboration of evidence, often necessitating expert testimony[9].

Expert testimony plays a vital role in the admissibility of biometric evidence. Forensic experts are required to present and validate the biometric data used in legal cases. Their role includes explaining the technical aspects of biometric identification, discussing the method's reliability, and addressing any potential error rates or limitations. Without expert testimony, courts may struggle to assess the scientific credibility of biometric evidence. These experts provide the necessary bridge between the complex technology and its legal relevance, ensuring that biometric evidence meets the standards of admissibility.

Challenges in the Use of Biometrics as Courtroom Evidence

Biometric evidence, while useful, poses several challenges in legal contexts. These challenges must be carefully considered to ensure the integrity and fairness of its use in courtrooms[8], [10].

Table 1 Challenges in the use of Biometrics

Challenge	Description	Impact
Reliability and Accuracy	Biometric systems can produce false positives, false negatives, and exhibit error rates depending on the technology used.	Could lead to wrongful convictions or acquittals based on inaccurate or unreliable data.
Data Manipulation/Mishandling	Biometric data can be vulnerable to tampering or incorrect handling during collection or processing.	Undermines the credibility of the evidence presented in court.
Privacy and Ethical Concerns	The collection and use of biometric data raise significant concerns over individual privacy rights and adherence to legal privacy frameworks.	Can lead to potential violations of privacy laws and ethical standards, raising doubts about the legality of the evidence.
Technological Limitations	Factors like lighting conditions, aging, and physical changes can affect the accuracy of biometric technologies such as facial recognition.	Reduces the reliability of the data, especially when conditions are not optimal for accurate readings.

While biometrics offer precise identification, their integration into courtroom procedures faces multiple challenges. These issues need to be addressed to maintain trust in the use of biometric evidence, balancing technological capabilities with legal and ethical considerations.

Case Studies: Admissibility and Challenges in Real Courtrooms

Biometric evidence, while increasingly common, often faces scrutiny in courtroom settings. The following case studies illustrate in table-2 the challenges and legal nuances involved in using biometric evidence such as fingerprints and facial recognition in criminal trials[9], [11].

Table 2 Major case studies illustrates challenges

Case Study	Description	Key Challenges	Outcome
Case Study 1: Fingerprint Evidence	A prominent case where fingerprint evidence was challenged involved a suspect whose partial fingerprint was found at a crime scene, but doubts arose regarding its collection and analysis.	Reliability of partial fingerprints and the chain of custody for evidence handling.	The court ruled that the fingerprint evidence was inadmissible due to questionable handling and analysis.
Case Study 2: Facial Recognition	In a criminal trial, facial recognition technology was used to identify a suspect from surveillance footage. The defense questioned the technology's accuracy in poor lighting conditions.	Accuracy issues with facial recognition in suboptimal conditions, such as poor lighting or facial obstructions.	The evidence was admitted but with cautionary instructions to the jury about its potential inaccuracies.
Comparative Analysis	Various jurisdictions, such as the U.S., U.K., and E.U., apply different standards for biometric evidence, leading to varying admissibility outcomes based on local laws and expert testimony.	Differences in legal frameworks and the weight given to expert testimony across jurisdictions.	Jurisdictions with stricter evidence handling laws are more likely to exclude or limit the use of biometrics.

These case studies highlight the complexities surrounding the admissibility of biometric evidence. While such technologies can be powerful tools, their use in court must be carefully scrutinized to ensure accuracy and fairness, with varying legal standards affecting their acceptance across different regions.

Recommendations for Enhancing the Admissibility of Biometrics in Court

To ensure the effective and fair use of biometric evidence in courtrooms, several key recommendations can be implemented. These focus on standardizing protocols, strengthening legal frameworks, and safeguarding privacy and ethical considerations[12].

Developing Standardized Protocols

- Consistency in Data Collection: Establishing clear guidelines for the collection, storage, and processing of biometric data is essential to ensure consistency. Uniform protocols across jurisdictions will help in reducing discrepancies in evidence handling.
- Certification of Biometric Technologies: Biometric tools should be independently certified for reliability and accuracy before they are used in legal contexts, with regular audits to maintain these standards.
- Training for Law Enforcement and Legal Professionals: Comprehensive training programs should be instituted to ensure law enforcement officials and legal professionals are proficient in using and evaluating biometric technologies.

Strengthening Legal Frameworks

- Clear Legal Standards: Legal frameworks must evolve to keep pace with advancements in biometric technologies. Clear and updated legal standards should be introduced to ensure that biometric evidence is admissible and used appropriately.
- International Harmonization of Laws: In light of cross-border legal challenges, efforts should be made to harmonize biometric data laws and admissibility standards across countries to ensure consistency in international cases[13].

Safeguarding Privacy and Ethical Considerations

- Data Privacy Protections: Stronger data protection measures must be put in place to ensure that individuals' biometric data is handled in compliance with privacy laws. This includes limiting access to the data and implementing strict consent requirements.
- Ethical Oversight: Independent ethical oversight bodies should be established to review the use of biometric technologies in legal proceedings, ensuring they do not infringe on civil liberties or privacy rights.

Enhancing the admissibility of biometric evidence in court requires a multifaceted approach involving standardized protocols, robust legal frameworks, and stringent privacy safeguards. These measures will ensure that biometric technologies can be utilized effectively while maintaining fairness and protecting individual rights.

Conclusion

Biometric evidence plays a significant and increasingly vital role in courtroom proceedings, offering precision and objectivity in identifying individuals. However, challenges persist regarding its reliability, privacy implications, and legal admissibility. False positives, technological limitations, and the potential for data manipulation all pose risks to its effective use in legal contexts. Additionally, privacy concerns and ethical dilemmas arise from the collection and use of biometric data, necessitating stringent legal safeguards and frameworks. The importance of expert testimony to validate the technology further emphasizes the complexity of presenting biometric evidence in court.

As biometric technologies continue to evolve, so will the legal frameworks that govern their use in courtrooms. It is essential for courts to adapt to these advancements by developing more comprehensive standards for admissibility. Future innovations in biometrics, such as more accurate facial recognition algorithms or enhanced DNA analysis techniques, will likely impact the reliability of evidence. These developments will require ongoing legal review to ensure they meet the necessary evidentiary and ethical standards. The balance between advancing technology and protecting individual rights will be crucial as biometric evidence becomes more prevalent in the judicial process.

References

[1] P. Faraldo Cabana, "Technical and Legal Challenges of the Use of Automated Facial Recognition Technologies for Law Enforcement and Forensic Purposes BT - Artificial Intelligence, Social Harms and Human Rights," A. Završnik and K. Simončič, Eds. Cham: Springer International Publishing, 2023, pp. 35–54.

[2] S. Nixon, P. Ruiu, C. Trignano, and M. Tistarelli, "Forensic Biometrics: Challenges, Innovation and Opportunities BT - Driving Forensic Innovation in the 21st Century: Crossing the Valley of Death," S. Francese and R. S. P. King, Eds. Cham: Springer International Publishing, 2024, pp. 165–194.

[3] G. K. Goswami and S. Goswami, "Three Decades of DNA Evidence: Judicial Perspective and Future Challenges in India BT - DNA Fingerprinting: Advancements and Future Endeavors," H. R. Dash, P. Shrivastava, B. K. Mohapatra, and S. Das, Eds. Singapore: Springer Singapore, 2018, pp. 181–205.

[4] B. Y. J. C. Puracal and A. B. Kaplan, "Science in the Courtroom: Challenging Faulty Forensics," *The Champion, NACDL.org*, p. 16, 2020.

[5] K. Quezada-Tavárez, P. Vogiatzoglou, and S. Royer, "Legal challenges in bringing AI evidence to the

criminal courtroom," *New J. Eur. Crim. Law*, vol. 12, no. 4, pp. 531–551, Nov. 2021, doi: 10.1177/20322844211057019.

[6] S. Carr, A. Gallop, E. Piasecki, G. Tully, and T. J. Wilson, "Chapter 5: Clarifying the 'reliability' continuum and testing its limits: biometric (fingerprint and DNA) expert evidence," Cheltenham, UK: Edward Elgar Publishing, 2018.

[7] P. Roberts and M. Stockdale, *Forensic Science Evidence and Expert Witness Testimony: Reliability through Reform?* Cheltenham, UK: Edward Elgar Publishing, 2018.

[8] H. S. Bakhtiar, "The Evolution of Scientific Evidence Theory in Criminal Law: A Transformative Insight," *Media Iuris*, vol. 7, no. 2, pp. 221–240, 2024, doi: 10.20473/mi.v7i2.51095.

[9] G. Edmond, "Latent science: A history of challenges to fingerprint evidence in Australia," *Univ. Qld. Law J.*, vol. 38, no. 2, pp. 301–365, Dec. 2019, [Online]. Available: https://search.informit.org/doi/10.3316/ielapa.031713335707908.

[10] B. S. A. Nasser, M. M. Saleh, and S. S. Abu-naser, "Genetic Fingerprinting and Its Admissibility in Criminal Evidence," no. July, 2024.

[11] R. Stoykova, "Digital evidence: Unaddressed threats to fairness and the presumption of innocence," *Comput. Law Secur. Rev.*, vol. 42, p. 105575, 2021, doi: https://doi.org/10.1016/j.clsr.2021.105575.

[12] G. Edmond, "Latent justice? A review of adversarial challenges to fingerprint evidence," *Sci. Justice*, vol. 62, no. 1, pp. 21–29, 2022, doi: https://doi.org/10.1016/j.scijus.2021.10.006.

[13] M. O. Ezegbogu and P. I.-O. Omede, "The admissibility of fingerprint evidence: An African perspective," *Can. Soc. Forensic Sci. J.*, vol. 56, no. 1, pp. 23–41, Jan. 2023, doi: 10.1080/00085030.2022.2068404.