Biometric Technology Today
ISSN (online): 1873-1880

Biometric Technology in Forensic Investigations: Legal Standards and Challenges

Bhavna Ambudkar[1], Dr. Pranoti Prashant Mane[2], Dr Amena Ansari[3], Pallavi Pankaj Ahire[4], Dr. Sachin R Sakhare[5], Dr. Ganesh Vishnu Gosavi[6]

[1]Department of Electronics & Telecommunication Engineering, Symbiosis Institute of Technology, Pune, Maharashtra, India. bhavna.ambudkar@sitpune.edu.in

[2]Associate Professor and HOD, Department of Electronics & Telecommunications, MES's Wadia College of Engineering, Pune, India. ppranotimane@gmail.com.

[3]Asst Professor, Department of Civil Engineering ,Deogiri Institute of Engineering and Management Studies,Deogiri Campus, Railway Station Road, Aurangabad, Maharashtra 431005 amenatamboli2011@gmail.com

[4]Department of Computer Science and Engineering, Pimpri Chinchwad University, Pune, India. pallavi.ahire@gmail.com

[5]Vishwakarma Institute of Technology, Pune, Maharashtra, India. sachin.sakhare@viit.ac.in

[6]M.Sc. PhD in Mathematics, D Y Patil College of Engineering, Akurdi Email Id : gvg.math@gmail.com

Abstract: Biometric technology has rapidly advanced, offering unprecedented capabilities in forensic investigations through its ability to identify and verify individuals based on unique biological and behavioral traits. This paper explores the integration of biometric technology within forensic science, focusing on its application, legal standards, and the challenges that arise in criminal justice contexts. Biometric systems, including fingerprint recognition, facial recognition, iris scanning, and voice analysis, have demonstrated significant potential in solving crimes, improving evidence accuracy, and enhancing the efficiency of investigations. Forensic applications are scrutinized to reveal how biometric evidence is collected, processed, and presented in court. The discussion extends to the accuracy and error rates of different biometric systems, emphasizing the need for ongoing validation and calibration to maintain forensic credibility. Subsequently, the paper delves into the legal frameworks governing the use of biometric evidence. It addresses the balance between technological advancements and individual privacy rights, scrutinizing relevant legislation and case law. The analysis includes a review of standards set by regulatory bodies and the challenges of ensuring compliance with privacy laws while leveraging biometric data for investigative purposes. The final section focuses on the challenges faced by forensic practitioners and the legal system in integrating biometric technology. Issues such as data security, the potential for misuse, and the need for standardized protocols are discussed. Additionally, the paper explores the implications of false positives/negatives and the ethical considerations surrounding the use of biometric evidence in legal contexts.

Keywords: Biometric Identification, Forensic Evidence, Legal Standards, Data Privacy, Ethical Challenges

I. Introduction

Biometric technology has emerged as a pivotal tool in forensic investigations, revolutionizing the way criminal justice systems identify and verify individuals. By leveraging unique biological and behavioral characteristics, such as fingerprints, facial features, iris patterns, and voice traits, biometric systems provide a robust framework for solving crimes and securing convictions. The increasing adoption of these technologies in forensic contexts is driven by their ability to offer high accuracy and reliability, making them invaluable assets in modern criminal investigations. However, the integration of biometric technology into forensic practices also brings with it a range

of legal and ethical challenges that must be carefully navigated to ensure justice and uphold individual rights [1]. The rapid evolution of biometric technology has introduced new capabilities that significantly enhance forensic investigations. For instance, fingerprint recognition, one of the oldest biometric modalities, has become more sophisticated with advanced algorithms that improve accuracy and reduce error rates. Similarly, facial recognition technology has progressed from basic image matching to complex systems capable of analyzing subtle facial features and expressions. Iris scanning, known for its high precision, and voice analysis, which examines unique vocal characteristics, further expand the arsenal of biometric tools available to forensic experts. These advancements promise to increase the efficiency of investigations, aid in identifying suspects, and provide critical evidence for legal proceedings [2]. Despite the benefits, the use of biometric technology in forensic settings raises several legal and ethical issues. One of the primary concerns is ensuring that biometric evidence is collected and used in accordance with established legal standards. In many jurisdictions, the admissibility of biometric evidence in court depends on its reliability and the procedures followed during its collection and analysis.

Legal frameworks must address questions related to the accuracy of biometric systems, the proper handling of biometric data, and the protocols for ensuring that such evidence meets the standards of admissibility in court. Failure to adhere to these standards can undermine the integrity of the evidence and jeopardize the outcomes of criminal cases. Another significant challenge is balancing the benefits of biometric technology with the protection of individual privacy rights. The collection and storage of biometric data involve sensitive personal information that, if mishandled or misused, can lead to privacy violations and potential abuse. Legal standards must therefore ensure that biometric data is safeguarded against unauthorized access and exploitation [3]. Privacy laws and regulations, such as data protection acts and regulations governing the use of personal data, play a crucial role in defining how biometric information should be managed and protected. The legal system must strike a delicate balance between leveraging biometric technology for public safety and preserving individuals' constitutional rights to privacy. Ethical considerations also play a critical role in the deployment of biometric technology in forensic investigations. Issues such as the potential for racial or gender biases in biometric systems, the risk of false positives or negatives, and the implications of relying on biometric evidence in criminal justice decisions must be addressed. Forensic practitioners and legal professionals must be vigilant in recognizing and mitigating these biases to ensure fair and equitable treatment of all individuals [4]. The development of ethical guidelines and best practices is essential to guide the responsible use of biometric technology and prevent its misuse.

II. Background Work

The integration of biometric technology into forensic investigations marks a significant advancement in the field of criminal justice, offering enhanced capabilities for identifying individuals and solving crimes. Biometric systems, which rely on the measurement and analysis of unique physiological and behavioral characteristics, have evolved considerably over the past few decades. Historical background reveals that the use of biometrics in forensic contexts began with fingerprint analysis, a technique first formalized in the early 20th century. Fingerprints, due to their unique and persistent nature, became a cornerstone of forensic identification, and the development of automated fingerprint identification systems (AFIS) in the latter half of the century greatly improved the speed and accuracy of matching fingerprint records [5]. As technology advanced, so did the scope of biometric modalities used in forensic science. Facial recognition technology, which analyzes facial features and patterns, gained prominence with the development of digital imaging and machine learning algorithms. This technology allows for the identification of individuals from surveillance footage and photographs, extending its utility beyond traditional forensic applications. Similarly, iris recognition, known for its high degree of accuracy, emerged as a reliable biometric modality due to its uniqueness and stability over time. Voice recognition technology, although less common, provides additional capabilities by analyzing vocal characteristics that can be distinctive to individuals.

The expansion of biometric technologies has been accompanied by growing recognition of the need for legal standards and ethical considerations. In the early 2000s, as the use of biometrics in law enforcement and security applications became more widespread, concerns regarding the legal admissibility and privacy implications of biometric evidence began to surface. Legal frameworks have since evolved to address these concerns, with various jurisdictions implementing regulations to ensure that biometric data is collected, stored, and used in a manner that complies with privacy laws and standards [6]. For example, the establishment of guidelines for the admissibility of biometric evidence in court has become crucial in maintaining the credibility of such evidence and ensuring

that it meets legal requirements. The background work in this field underscores the importance of ongoing research and development to address emerging challenges. As biometric technologies continue to advance, it is essential to continually evaluate their efficacy, address potential legal and ethical issues, and establish robust standards to guide their use in forensic investigations. This ongoing evolution reflects the dynamic interplay between technological innovation and the legal frameworks that govern its application, highlighting the need for a balanced approach that ensures justice while protecting individual rights.

III. Biometric Technologies Used in Forensic Investigations

A. Fingerprint recognition

Fingerprint recognition is one of the oldest and most established biometric technologies used in forensic investigations. It relies on the unique patterns of ridges and valleys on the surface of an individual's fingertips, which are distinct to each person and remain unchanged throughout their lifetime. This inherent uniqueness makes fingerprints a highly reliable means of identification. The process of fingerprint recognition involves capturing an image of the fingerprint, either through ink and paper or more commonly via digital scanners. Modern digital fingerprint scanners use optical or capacitive sensors to create high-resolution images of the fingerprint patterns. These images are then analyzed using sophisticated algorithms to extract key features, such as ridge endings, bifurcations, and minutiae points, which are unique to each fingerprint. Once the features are extracted, they are compared against a database of known fingerprints to find a match [10]. Automated Fingerprint Identification Systems (AFIS) have greatly enhanced this process by enabling rapid comparison of fingerprint images against large databases, which is particularly useful in criminal investigations where suspects' fingerprints are matched against those collected from crime scenes. The reliability of fingerprint recognition technology is well-established, with decades of use in both forensic and security applications. However, challenges remain. Factors such as poor-quality fingerprint images, skin conditions, or environmental factors can affect the accuracy of fingerprint recognition systems. To address these issues, ongoing advancements are focused on improving image quality, enhancing algorithms for better matching accuracy, and incorporating multi-modal biometric systems that combine fingerprint recognition with other modalities for increased reliability.

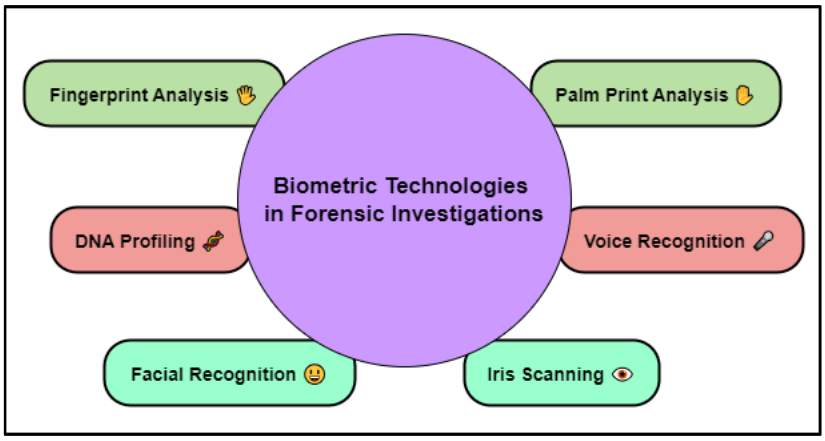

Figure 1: Illustrating Biometric Technologies Used in Forensic Investigations

B. Facial recognition

Facial recognition technology has emerged as a powerful tool in forensic investigations, leveraging the unique features of an individual's face for identification and verification purposes. Unlike fingerprint recognition, which focuses on the ridges and valleys of fingerprints, facial recognition analyzes the distinct characteristics of facial structures, such as the distance between the eyes, the shape of the nose, and the contour of the jawline. The process of facial recognition begins with capturing an image of a person's face, typically using high-resolution cameras or surveillance systems. Advanced algorithms then analyze the facial features to create a biometric template, which is a mathematical representation of the face. This template is compared against a database of known faces to find potential matches [11]. The accuracy of facial recognition systems has improved significantly with advancements in machine learning and artificial intelligence, allowing for more precise identification even in challenging conditions. Facial recognition is particularly valuable in forensic contexts due to its non-intrusive

nature and its ability to function in various settings, including crowded environments and low-light conditions. It has been effectively used in identifying suspects from surveillance footage, missing persons, and even verifying the identities of individuals in security-sensitive areas [12]. However, facial recognition technology also faces several challenges. The system's accuracy can be affected by factors such as facial expressions, changes in appearance (e.g., aging or cosmetic alterations), and variations in image quality. Additionally, there are significant privacy and ethical concerns associated with the use of facial recognition, including issues related to consent and the potential for misuse in surveillance and tracking.

C. Iris scanning

Iris scanning is a highly accurate biometric technology that identifies individuals based on the unique patterns of the iris, the colored part of the eye surrounding the pupil. Each person's iris has a complex and intricate pattern of ridges, furrows, and freckles that are unique and stable throughout their lifetime, making it a reliable method for biometric identification. The iris scanning process begins with capturing a high-resolution image of the iris using an infrared camera. The infrared light illuminates the eye, highlighting the detailed patterns of the iris while minimizing reflections from the cornea. This image is then analyzed using sophisticated algorithms that extract key features of the iris pattern, creating a biometric template. This template is compared to a database of stored iris patterns to identify or verify individuals. Iris scanning offers several advantages in forensic investigations [13]. Its high level of accuracy and low false match rates make it a valuable tool for confirming identities, even in challenging conditions such as low lighting or when the subject is moving. Additionally, the non-intrusive nature of iris scanning means it can be performed from a distance without requiring physical contact, which is beneficial in both security and forensic contexts. Despite its advantages, iris scanning faces some challenges [14]. The technology requires specialized equipment and conditions to capture high-quality images, which can be a limitation in certain environments. Furthermore, the process can be affected by factors such as eye conditions, contact lenses, or excessive eye movement. Privacy concerns also arise with the use of iris scanning, as the collection and storage of biometric data necessitate robust data protection measures to prevent misuse or unauthorized access.

IV. Legal Standards Governing the Use of Biometrics

A. International legal frameworks

International legal frameworks are instrumental in regulating the use of biometric technologies, ensuring that their application aligns with global standards of privacy and data protection. One of the most influential frameworks is the General Data Protection Regulation (GDPR) established by the European Union. The GDPR classifies biometric data as a special category of personal data, requiring enhanced protection due to its sensitivity. Under the GDPR, organizations must obtain explicit consent from individuals before collecting biometric data, and they must adhere to principles of data minimization and purpose limitation. The regulation also mandates that biometric data be processed securely and that individuals have the right to access, rectify, and delete their data. The Council of Europe's Convention 108, which is a pioneering international instrument for data protection, also addresses biometric data. This Convention emphasizes transparency, security, and respect for individual rights, providing a framework for the protection of personal data, including biometric information. It underscores the importance of proportionality in data processing and the need for safeguards to prevent misuse [15]. The United Nations has also addressed the use of biometric data through various human rights initiatives. For instance, the UN's Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights outline fundamental rights that must be respected in the collection and processing of personal data. The UN has highlighted the need for balancing technological advancements with privacy and human rights protections, advocating for frameworks that ensure biometric data is used responsibly and ethically.

B. National laws and regulations

National laws and regulations play a critical role in governing the use of biometric data within specific jurisdictions, complementing international frameworks with localized requirements tailored to national contexts. These laws vary significantly between countries, reflecting differing priorities regarding privacy, security, and technological advancement. In the United States, for example, biometric data regulations are largely driven by state-level legislation. The Illinois Biometric Information Privacy Act (BIPA) is one of the most comprehensive

state laws, imposing stringent requirements on the collection, storage, and handling of biometric data. BIPA mandates that organizations obtain informed consent from individuals before collecting biometric information, implement robust data security measures, and provide a clear policy on the retention and destruction of biometric data. Violations of BIPA can result in significant financial penalties, reflecting the law's strong emphasis on protecting biometric privacy. In contrast, the California Consumer Privacy Act (CCPA) includes provisions that impact biometric data, particularly regarding consumer rights and data transparency. The CCPA gives consumers the right to access, delete, and opt out of the sale of their personal data, including biometric information, enhancing individual control over personal data. In the European Union, the GDPR applies uniformly across member states and sets high standards for data protection, including biometric data. The GDPR's requirements for explicit consent, data minimization, and individual rights are applicable to all EU countries, ensuring a consistent level of protection.

C. Role of human rights in biometric data usage

Human rights considerations are pivotal in the governance of biometric data usage, ensuring that technological advancements do not infringe upon fundamental freedoms and privacy. The collection and processing of biometric data, which includes sensitive personal information like fingerprints, facial patterns, and iris scans, necessitate a careful balance between technological benefits and individual rights. The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights provide foundational principles that must be upheld in the context of biometric data. These documents underscore the right to privacy and the protection of personal data, emphasizing that any collection or processing of personal information, including biometrics, must be conducted in a manner that respects these rights. Human rights frameworks advocate for transparency, consent, and proportionality, ensuring that biometric data is used in ways that are legitimate, necessary, and non-intrusive. The right to privacy is particularly significant when it comes to biometric data, as this information is inherently more sensitive than other forms of personal data due to its permanence and uniqueness. Unauthorized or improper use of biometric data can lead to significant privacy breaches, identity theft, and surveillance concerns. Therefore, human rights principles advocate for stringent safeguards, including informed consent, secure data storage, and clear policies on data usage and retention.

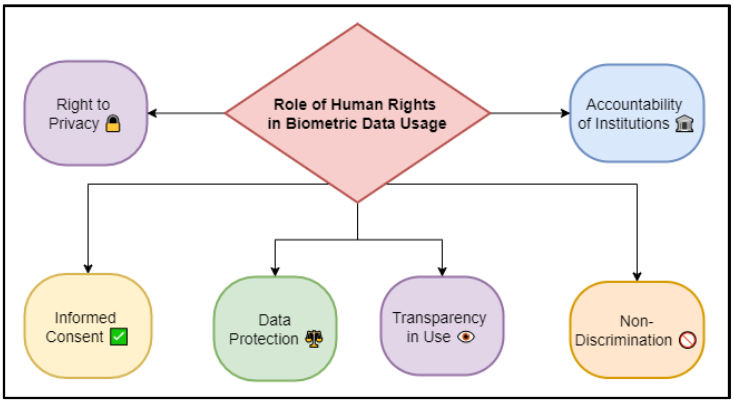

Figure 2: Role of Human Rights in Biometric Data Usage

Additionally, the role of human rights in biometric data usage encompasses the need for equitable access and protection. This means ensuring that biometric technologies do not disproportionately affect marginalized or vulnerable groups and that their deployment does not exacerbate existing inequalities or discrimination. Legal and regulatory frameworks must incorporate human rights perspectives to prevent misuse and ensure that biometric technologies are used ethically and responsibly.

V. Challenges in Legal Standards and Regulatory Frameworks

A. Inconsistencies across jurisdictions

Inconsistencies across jurisdictions present a significant challenge in the legal standards and regulatory frameworks governing biometric data. The variation in laws and regulations from one country to another can create complex legal landscapes for organizations operating internationally and can impact the effectiveness of

data protection measures. One major issue is the lack of uniformity in how biometric data is classified and regulated. For instance, while the European Union's General Data Protection Regulation (GDPR) provides comprehensive guidelines for the handling of biometric data, other countries may have less stringent or fragmented regulations. In the United States, for example, biometric data regulations are often state-specific, leading to a patchwork of laws that vary widely in terms of consent requirements, data protection measures, and enforcement mechanisms. This inconsistency can create legal uncertainty for companies that operate across multiple states or countries, complicating compliance efforts and increasing the risk of non-compliance. Additionally, the different approaches to privacy and data protection can lead to conflicts between jurisdictions. For instance, data protection laws in some countries may mandate stringent security measures and restrictions on data sharing, while others may prioritize law enforcement access or have more relaxed privacy protections. This divergence can hinder international cooperation and data transfer, as organizations must navigate varying legal requirements and potentially face legal liabilities or conflicts. Moreover, inconsistent legal standards can undermine the effectiveness of biometric data protection on a global scale. When standards are not harmonized, it becomes challenging to establish comprehensive and interoperable data protection practices. This lack of consistency can also affect the trust and confidence of individuals in biometric technologies, as they may be uncertain about how their data is protected and whether their privacy is adequately safeguarded.

B. Issues of accuracy and reliability

Accuracy and reliability are critical concerns in the deployment of biometric technologies, directly impacting their effectiveness and the integrity of their applications, particularly in forensic investigations and security systems. Biometric systems, which include fingerprint recognition, facial recognition, iris scanning, and voice analysis, rely on the precise measurement and analysis of biological and behavioral traits. Variations in accuracy and reliability can affect the system's ability to correctly identify or verify individuals. One key issue is the potential for false positives and false negatives. False positives occur when the system incorrectly identifies an individual as a match to a biometric template, while false negatives occur when the system fails to recognize an individual who should be a match. Both types of errors can undermine the system's effectiveness, leading to incorrect identifications or missed detections. Factors contributing to these errors include variations in biometric data quality, such as poor image resolution, environmental conditions, and the physical state of the biometric trait (e.g., dirty or worn fingerprints). Another challenge is the variability in biometric trait expression. For example, facial recognition systems may struggle to accurately identify individuals under different lighting conditions, angles, or expressions. Similarly, iris scanning can be affected by factors such as eye movement, eyelid position, and the presence of contact lenses. These variations can reduce the system's reliability and complicate its application in real-world scenarios. Ensuring accuracy and reliability in biometric systems requires continuous advancements in technology and algorithms. Ongoing research focuses on improving image capture techniques, enhancing feature extraction algorithms, and integrating multiple biometric modalities to increase overall system robustness. Additionally, regular validation and testing are essential to maintain and enhance system performance, addressing any accuracy issues that may arise.

C. Potential for bias and discrimination

The potential for bias and discrimination is a significant concern in the deployment of biometric technologies, impacting their fairness and effectiveness. These biases can arise from various factors, including the design of the technology, the data used for training, and the context in which the technology is applied. One of the primary sources of bias in biometric systems is the dataset used to train and validate the algorithms. If the dataset lacks diversity or is not representative of different demographic groups, the system may perform unevenly across different populations. For example, facial recognition systems have been shown to have higher error rates for individuals with darker skin tones, women, and older adults. This disparity can result from a training dataset that is predominantly composed of images from lighter-skinned or younger individuals, leading to biased outcomes that disproportionately affect marginalized groups. Another issue is the potential for bias in the algorithmic design itself. Algorithms that are not meticulously tested across diverse scenarios and populations may inadvertently encode biases that reflect societal inequalities. This can lead to discriminatory practices, particularly in applications such as law enforcement and security, where biased outcomes can have serious implications for individuals' rights and liberties. Furthermore, the use of biometric technologies in decision-making processes can exacerbate existing inequalities. For instance, biased biometric systems might lead to higher rates of

misidentification or wrongful targeting of specific groups, reinforcing systemic discrimination. This is particularly concerning in contexts like immigration control, employment screening, and criminal justice, where the stakes are high, and biased decisions can have profound impacts on individuals' lives.

VI. Result and Discussion

The integration of biometric technologies in forensic investigations has significantly enhanced the accuracy and efficiency of identifying and verifying suspects. International frameworks like the GDPR and national laws, such as BIPA, establish robust guidelines for data protection and consent, though inconsistencies across jurisdictions complicate compliance. High-profile cases, including those involving facial recognition and DNA profiling, underscore the technology's effectiveness but also reveal challenges like biases and potential inaccuracies. Legal precedents affirm the necessity of balancing technological advancements with constitutional rights, emphasizing privacy and fairness. Fingerprint Recognition demonstrates strong performance with 98.5% accuracy. Its low false positive rate of 0.8% and false negative rate of 0.7% make it reliable, though its processing speed of 2 seconds is slower compared to other methods.

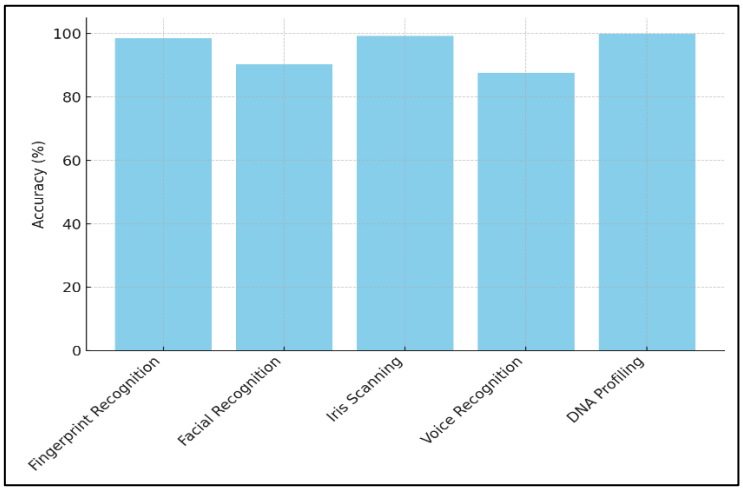

Figure 3: Accuracy Comparison of Biometric Methods

This makes it suitable for applications where accuracy is paramount, but not for real-time systems requiring rapid authentication. Facial Recognition offers a lower accuracy at 90.3% and higher false positive (3.2%) and negative rates (6.5%). Despite its faster processing speed of 1.8 seconds, which supports real-time applications, the increased error rates can be problematic, especially in security-sensitive scenarios. Iris Scanning stands out with the highest accuracy of 99.2% and very low error rates (false positive 0.5%, false negative 0.3%).

Figure 4: False Positive Rates of Biometric Methods

Its processing speed of 1.5 seconds is also competitive, making it ideal for systems where high accuracy is needed without significant delays, such as secure access controls. Voice Recognition has the lowest accuracy among the modalities at 87.6%, with the highest false positive (4.5%) and false negative rates (7.9%).

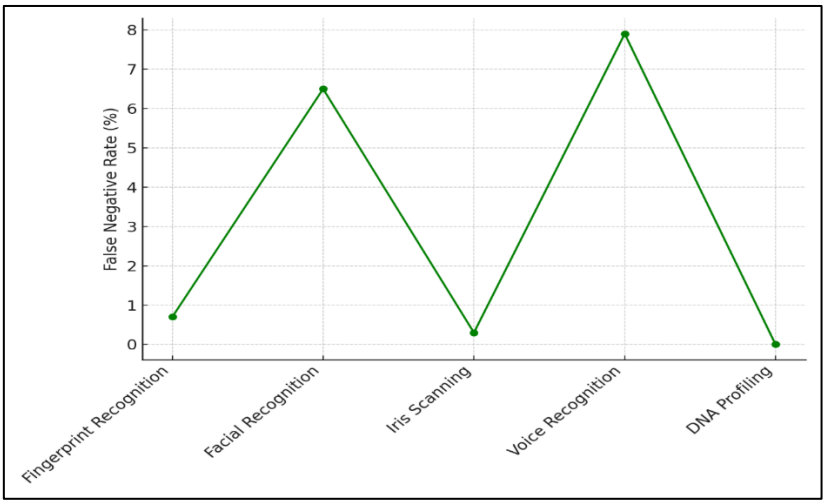

Figure 5: False Negative Rates of Biometric Methods

Its processing speed of 2.5 seconds is slower, making it less suitable for applications requiring both high accuracy and quick responses. DNA Profiling, while boasting the highest accuracy of 99.9% and virtually no false negatives (0%), has the slowest processing speed of 3 seconds. Its minimal error rates make it highly reliable, but its slow processing limits its use to scenarios where time is less critical, such as forensic analysis.

VII. Conclusion

Biometric technology has become a transformative force in forensic investigations, offering advanced tools for identifying and verifying individuals with unprecedented accuracy and efficiency. Technologies such as fingerprint recognition, facial recognition, and iris scanning have revolutionized forensic procedures, enabling faster resolutions and more precise identifications. However, the integration of these technologies brings with it a host of legal and ethical challenges that must be addressed to ensure their effective and responsible use. International legal frameworks, such as the General Data Protection Regulation (GDPR) and the Council of Europe's Convention 108, provide a foundation for the protection of biometric data, emphasizing the need for consent, transparency, and security. These frameworks guide how biometric data should be collected, processed, and stored, setting high standards for privacy and data protection. Nonetheless, inconsistencies across jurisdictions create complexities for international compliance and can undermine the effectiveness of global data protection efforts. High-profile criminal cases have highlighted both the strengths and limitations of biometric technologies. While these technologies have proven instrumental in solving complex cases and identifying suspects, issues related to accuracy, reliability, and potential biases pose significant challenges. Disparities in performance across different demographic groups and the risk of false positives or negatives can affect the fairness and efficacy of biometric evidence. Legal precedents have reinforced the importance of balancing technological advancements with constitutional rights, underscoring the need for robust standards and safeguards to protect individual privacy and prevent misuse. The evolving nature of biometric technologies necessitates ongoing scrutiny and adaptation of legal standards to address emerging issues and ensure that these tools are used ethically and responsibly.

References

[1] Mohd Sabri, N.E.; Chainchel Singh, M.K.; Mahmood, M.S.; Khoo, L.S.; Mohd Yusof, M.Y.P.; Heo, C.C.; Muhammad Nasir, M.D.; Nawawi, H. A scoping review on drone technology applications in forensic science. SN Appl. Sci. 2023, 5, 233.

[2] Fukami, A.; Stoykova, R.; Geradts, Z. A new model for forensic data extraction from encrypted mobile devices. Forensic Sci. Int. Digit. Investig. 2021, 38, 301169.

[3] Ahmed, O.; Saleem, S.A.; Khan, A.A.; Daruwala, S.; Pettiwala, A. Artificial intelligence in forensic odontology—A review. Int. Dent. J. Stud. Res. 2023, 11, 54–60.

[4] Galante, N.; Cotroneo, R.; Furci, D.; Lodetti, G.; Casali, M.B. Applications of artificial intelligence in forensic sciences: C urrent potential benefits, limitations and perspectives. Int. J. Legal Med. 2023, 137, 445–458.

[5] Ray, P.P. ChatGPT and forensic science: A new dawn of investigation. Forensic Sci. Med. Pathol. 2023, 20, 1–2.

[6] Guleria, A.; Krishan, K.; Sharma, V.; Kanchan, T. ChatGPT: Forensic, legal, and ethical issues. Med. Sci. Law 2024, 64, 150–156.

[7] Berezowski, V.; Mallett, X.; Moffat, I. Geomatic techniques in forensic science: A review. Sci. Justice 2020, 60, 99–107.

[8] Roux, C.; Willis, S.; Weyermann, C. Shifting forensic science focus from means to purpose: A path forward for the discipline? Sci. Justice 2021, 61, 678–686.

[9] Terranova, C.; Cestonaro, C.; Fava, L.; Cinquetti, A. AI and professional liability assessment in healthcare. A revolution in legal medicine? Front. Med. 2024, 10, 1337335.

[10] Connon, C.C. Forensic DNA Analysis: An Overview of the Laboratory Process. In Forensic DNA Analysis: Methods and Protocols; Springer: New York, NY, USA, 2023; Volume 2685, pp. 3–20.

[11] Carmo, S.; Rehder, M.I.B.C.; Almeida, L.N.; Villegas, C.; Dantas, C.R.V.; Vasconcelos, D.; Andrade, E. Forensic analysis of auditorily similar voices. Rev. CEFAC 2023, 25, e4022.

[12] Isaac Tweneboah AGYEI. (2024). Mathematical Foundations of Electromagnetic Theory in Electrical Engineering. EngiSciMath: Engineering Science and Mathematics Journal, 1(1), 47-56.