IDENTIFICATION PROCEDURES IN THE INDIAN CRIMINAL JUSTICE SYSTEM

Aabha Jain, PhD Research Scholar, Damodaram Sanjivayya National Law University, Visakhapatnam

ABSTRACT

Accurate identification of the accused is a cornerstone of criminal justice. Without reliably establishing identity, wrongful convictions or acquittals may result. Over time, a variety of identification methods ranging from traditional lineups to advanced biometrics have evolved. This paper examines the taxonomy of identification techniques, critiques their strengths and limitations, and analyzes how Indian courts treat their evidentiary weight. The study further explores infrastructure and legislative challenges in India and proposes reforms for a scientifically grounded, constitutionally compliant identification regime.

1. Introduction

In criminal law, the act of investigation is the vital first step toward justice: it is the phase in which suspicion is refined, evidence is collected, and the suspect is focused. Yet in many criminal cases, the complainant or eyewitness first encounters the alleged offender amid the commission of the offense or under traumatic, low-visibility conditions. In such circumstances, ensuring that the person presented to investigative and judicial authorities is the same individual who committed the crime becomes both critical and challenging.

Within this framework, the aims of this article are threefold: to explicate why identification is indispensable in criminal justice; to present and critically assess the full range of identification procedures, both perceptual and scientific; and to examine how Indian courts treat identification evidence, drawing lessons for a future, reformed regime. In doing so, the paper argues that India must pivot toward greater reliance on biometric and scientific identification, while embedding rigorous safeguards for procedural fairness and constitutional rights.

First, the article explores the normative significance of identification in criminal adjudication

and the inherent risks of perceptual error. Next, it maps a comprehensive taxonomy of identification methods and analyzing their operational challenges. Then the paper turns to Indian jurisprudence, assessing how courts have accepted or rejected identification evidence, and how they balance reliability with constitutional protections such as privacy and self-incrimination. The analysis culminates in practical recommendations for India's identification system.

2. Theoretical and Normative Foundations of Identification

To begin, identification in criminal jurisprudence denotes the process of linking an accused person to the act alleged, thereby satisfying both investigators and the court that the person before them is indeed the perpetrator. The function of identification is not merely procedural; it is central to fairness and legitimacy.[1] If identification is faulty, the very foundation of conviction collapses, risking both wrongful convictions and failure to penalize true offenders.[2]

Identification performs two critical roles: first, it steers the investigation by narrowing down suspects; second, it strengthens testimonial evidence by anchoring the accused before the court. In a system built on the presumption of innocence, error in identification is especially perilous. The widely accepted maxim that it is better that ten guilty people go free than one innocent suffer highlights the need for utmost caution in identity procedures.[3]

Yet the reliability of human perception is constrained. Witness memory is vulnerable to decay, environmental distortion, stress, and suggestion and procedural design, psychological factors, and suggestive cues may taint identification.[4] Thus the choice, administration, and judicial scrutiny of identification techniques become pivotal. This theoretical tension between the necessity of identification and its fallibility frames the rest of the analysis.

3. Taxonomy and Critique of Identification Methods

Identification methods fall broadly into two categories: perceptual / memory-based techniques

[1] Tom R. Tyler, *Psychological Perspectives on Legitimacy and Legitimation*, 57 ANNUAL REVIEW OF PSYCHOLOGY 375 (2006).
[2] Neema Haule, *Wrongful Convictions in Tanzania*, 6 IJFMR - INTERNATIONAL JOURNAL FOR MULTIDISCIPLINARY RESEARCH (2024), https://www.ijfmr.com/research-paper.php?id=32027.
[3] Rang Bahadur Singh v. State of Uttar Pradesh, A.I.R. 2000 S.C. 1209.
[4] K. Jayasankara Reddy, *Witness Testimony and Memory*, *in* FOUNDATIONS OF CRIMINAL FORENSIC NEUROPSYCHOLOGY : BRIDGING MIND, LAW, AND CRIMINAL JUSTICE 379 (K. Jayasankara Reddy ed., 2025), https://doi.org/10.1007/978-3-031-83771-5_14.

and biometric / scientific techniques. In practice, investigators often combine multiple methods to increase confidence. Below is a detailed exploration of each.

3.1. Perceptual Techniques

3.1.1. Test Identification Parade

One of the oldest and most widely used methods, a Test Identification Parade (commonly referred to as lineup) involves placing the suspect among multiple "fillers" of similar appearance and requesting the witness to pick out the accused.[5] Because it mimics a live confrontation, it is considered a check on memory reliability. However, its success depends heavily on neutrality of procedure e.g. blind lineup administration including use of panch witnesses, careful selection of fillers, unbiased instructions. Many courts caution that TIPs are unsafe when an eyewitness had only a fleeting glance or poor viewing conditions.[6]

Identification by parade cannot be relied upon unquestioningly and must be assessed in light of surrounding circumstances. The delay in conducting a lineup weakens reliability. Another danger is that a witness may see the accused between the crime and the lineup, or be coached. The suggestion inherent in parade proceedings is nontrivial, so rigorous procedural safeguards, such as independent observers and documentation, are essential.[7]

3.1.2. Photographic Identification

Instead of live lineups, witnesses may be shown photographs (physical or digital) of suspects or similar individuals. This is operationally easier, especially in jurisdictions with limited resources or dispersed populations. But photo arrays suffer from two principal weaknesses: photographic distinctiveness such as lighting, background, image quality, which may influence selection, and memory bias or false recognition may occur. To reduce bias, photos should be randomized, of uniform quality, and shown without suggestive cues.

3.1.3. Modus Operandi and Criminal Profiling

The modus operandi method assumes that habitual offenders often repeat particular methods

[5] Ravi Anand, Proof of the Identification Parade (Apr. 2, 2009), https://papers.ssrn.com/abstract=1372353.
[6] State of Maharashtra v. Sukhdev Singh, A.I.R. 1992 S.C. 2100.
[7] Gary L. Wells et al., *Eyewitness Identification Procedures: Recommendations for Lineups and Photospreads*, 22 LAW AND HUMAN BEHAVIOR 603 (1998).

or signature behaviors, e.g., choice of entry, sequence of acts, tools used. Investigators compare crime patterns to link crimes or suspect behavior.[8] Criminal profiling goes further, using psychological, behavioural, and victimology analysis to infer traits or demographic features of the offender.[9] While these techniques rarely yield definitive identity, they can narrow suspects in absence of direct evidence and guide investigative strategies.

3.1.4. Voice Recognition

In cases involving recorded calls or video with audio, voice recognition may assist identification. A witness familiar with the speaker may attempt recognition. Forensic voice spectrography may compare voice prints. However, voice is variable due to health, mood, recording quality, and acoustical distortions may mislead. Courts tend to treat voice identification cautiously, requiring corroboration.

3.1.5. Field Viewing

Sometimes police present a suspect to a witness in situ, e.g. at or near the crime scene. This method is highly vulnerable to suggestion and is discouraged except under stringent safeguards (e.g. blind protocol, multiple options). It is considered less reliable than controlled lineups since suggestion and authority bias are strong.

3.1.6. Gait and Footprint Identification

More recently, gait analysis (the pattern of walking) and footprint ridges have emerged as identification options.[10] Research shows human footprints and gait patterns can be distinctive. In forensic and cybersecurity research, gait and footprint biometrics are being explored as behavioral identifiers, especially when optical or biometric facial modes are unavailable.[11] However, these techniques are nascent, less mature in forensic validation, and subject to environmental variation and data quality constraints.

---

[8] Irkutsk State University & I.A. Fomina, *Modus Operandi in the Investigation of Crimes*, 2 SIB.LAWHERALD 111 (2021).
[9] *[PDF] Investigative (Psychological) Profiling | Semantic Scholar*, https://www.semanticscholar.org/paper/Investigative-(Psychological)-Profiling/0550065e74c4088f9e2e92ade024eab4616ccc69 (last visited Oct. 1, 2025).
[10] Mhaske Sakshi Vitthal & Sakshi Mhaske, *Gait Pattern Analysis Through Various Techniques and Methods - A Review*, 11 INT J SCI RES SCI & TECHNOL 536 (2024).
[11] Prerna Arora, *Survey on Human Gait Recognition* (2015), https://www.semanticscholar.org/paper/Survey-on-Human-Gait-Recognition-Arora/f251d2b6433123b1f05ebe7bba420019720eb9c1.

3.2. Biometric / Scientific Techniques

3.2.1. Fingerprint Analysis

Fingerprint identification is a hallmark of forensic science. Each human fingerprint has a unique pattern of ridges, loops, and whorls, stable over time in absence of injury. Latent fingerprints from crime scenes can be compared with known exemplars via systems such as Automated Fingerprint Identification Systems. In India, the National Automated Fingerprint Identification System (NAFIS) under the National Crime Records Bureau (NCRB) integrates fingerprint records across states, enabling cross-jurisdictional matching.[12] Fingerprinting is relatively inexpensive, fast, and objective compared to perceptual methods. Its reliability depends on quality of prints, clarity, examiner skill, and proper chain of custody.

3.2.2. DNA Profiling / Genetic Fingerprinting

DNA profiling is widely regarded as one of the strongest forensic identification tools. Biological samples such as blood, saliva, hair roots are collected, DNA extracted and amplified, and then compared to suspect DNA or DNA databanks. Indian jurisprudence has increasingly accepted DNA evidence, though courts remain vigilant about procedural rigor, chain-of-custody, contamination risk, and laboratory standards.[13] Critics highlight that India lacks uniform statutory guidelines regulating DNA use, making admissibility dependent on judicial discretion. DNA remains costlier and more resource-intensive than fingerprinting but provides stronger discriminatory power when applicable.

3.2.3. Iris Biometrics

The patterns in the iris or retina are highly distinctive and stable across an individual's life. While iris and retina recognition are more common in civil identification systems (e.g. Aadhaar), their forensic application is in infancy in India. High-resolution imaging, edge cases (glasses, reflections), and pose variation pose technical challenges. If these hurdles are overcome, iris biometrics can offer strong identification potential.

---

[12] Robert Allen, Pat Sankar & Salil Prabhakar, *Fingerprint Identification Technology*, *in* BIOMETRIC SYSTEMS: TECHNOLOGY, DESIGN AND PERFORMANCE EVALUATION 22 (James Wayman et al. eds., 2005), https://doi.org/10.1007/1-84628-064-8_2.

[13] Lairenjam Dhanamanjuri Devi, *Science On Trial: A Critical Study of The Role of DNA And Forensic Evidence in Indian Courts*, KUEY (2021), https://kuey.net/index.php/kuey/article/view/10303.

3.2.4. Facial Biometrics

Facial recognition systems map facial landmarks such as distance between eyes, nose shape, jawline and compare against large databases e.g. CCTV or mugshots. Indian research has investigated 3D facial recognition tailored to Indian environmental and demographic conditions.[14] Facial recognition aids in identifying suspects captured on surveillance footage.[15] But it suffers from variations in lighting, pose, ageing, occlusions (masks), and algorithm biases.[16] Courts typically demand human validation, explanation of algorithmic error rates, and transparency before accepting such evidence.[17]

3.2.5. Ballistics / Toolmark Identification

While not directly identifying a person, ballistic forensics helps connect bullets or cartridges to specific firearms. By analyzing microscopic striations on projectiles and casings, forensic experts can assert that a particular weapon fired the involved ammunition, thereby strengthening attribution to a suspect who possessed or controlled that firearm. Such linkage can indirectly support identification.

3.2.6. Cyber Forensics

In modern crime involving digital devices, identification may arise via metadata, IP logs, device IDs, geolocation logs, email or social media accounts, device fingerprinting, and digital signatures.[18] Because nearly all modern crimes leave digital traces, cyber forensic identification is becoming indispensable, especially in financial crime, hacking, and organized crime.

3.2.7. Trace / Chemical / Micro-Comparative Evidence

Sometimes, linking a suspect's property or person to a crime scene involves analyzing unique

---

[14] Saurjya Ranjan Das, Sreepreeti Champatyray & Dhiren Kumar Panda, *Anthropometric Analysis of Facial Dimensions Using 3D Imaging for Forensic Identification and Ethnicity-Specific Reference Models*, 12 FORENSIC SCIENCE INTERNATIONAL: REPORTS 100428 (2025).
[15] *Bias in the Algorithm: Issues Raised Due to Use of Facial Recognition in India - Intifada P. Basheer, 2025*, https://journals.sagepub.com/doi/10.1177/24551333241283992 (last visited Oct. 1, 2025).
[16] *Id.*
[17] *Who Monitors the Monitors? Analysing the Legal Intricacies of Digital Forensic-Based Facial Recognition Technology in Law Enforcement - Akash Bag, Abhinav Pradhan, 2025*, https://journals.sagepub.com/doi/abs/10.1177/23220058251376612 (last visited Oct. 1, 2025).
[18] Patil Rachana Yogesh & Satish R. Devane, *Primordial Fingerprinting Techniques from the Perspective of Digital Forensic Requirements*, *in* 2018 9TH INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND NETWORKING TECHNOLOGIES (ICCCNT) 1 (2018), https://ieeexplore.ieee.org/document/8494064.

chemical signatures, soil particles, glass fragments, paint chips, fibers, or residue profiles.[19] While not direct human identification, such associative evidence can reinforce identification when combined with biometric or testimonial methods.

4. Judicial Approach to Identification Evidence in India

Understanding how Indian courts accept, weigh, or reject identification procedures is vital. The jurisprudence reveals recurring themes: cautious acceptance of perceptual methods, high regard for biometric evidence, subject to safeguards, and key constitutional tensions concerning privacy and self-incrimination.

4.1. Perceptual Methods: Corroborative, Not Conclusive

There is a certain value attached to the identification procedures even when they are subjective. There have been various instances wherein the court has held that a witness just cannot come to the court and identify the accused for the first time. An identification parade must be conducted prior to it.[20] The witness cannot be believed if a proper identification is not conducted.[21]

But, this seems to be an unsettled issue as the Supreme Court in another instance has held that failure to hold identification parade does not make evidence inadmissible.[22] The Court in this case was of the opinion that weight to be attached to such identification procedure was a matter of fact. The Supreme Court in case of Dastagir Sab v. State of Karnataka, held that where the witness has seen the accused on multiple occasions, the failure to hold identification procedure was not fatal.[23] Even Andhra Pradesh High Court had a similar view in this regard. It was of the opinion that, "the prosecutrix cannot be disbelieved on the ground of lapse of time and absence of identification parade."[24]

However, identification does not constitute substantive evidence.[25] Also, an identification

[19] *The Chemistry of Forensic Evidence*, https://onlinelibrary.wiley.com/doi/10.1002/9781118496879.ch1 (last visited Oct. 1, 2025).
[20] State of Maharashtra v. Sukhdev Singh, A.I.R. 1992 S.C. 2100.
[21] Kanan v. State of Kerala, 1980 M.L.J. (Cri) 1.
[22] Kanta Prasad v. Delhi Administration, A.I.R. 1958 S.C. 350.
[23] Dastagir Sab v. State of Karnataka, (2004) 3 S.C.C. 106.
[24] Toorpati Majsaiah and Another v. State of A.P., 2005 Cri. L.J. 568.
[25] Mahabir v. State of Delhi, 2008 (3) Supreme 111.

procedure cannot be a decisive factor of convicting a person.[26] Thus, just because a witness identified a person to be the perpetrator, it cannot become the sole ground on the basis of which the accused is convicted. There must be substantial grounds for conviction. The identification of the accused in the identification procedure is not a sine qua non for establishing guilt.[27]

The identification of an accused must be made beyond reasonable doubt. The question doesn't arise in methods like fingerprinting, but, in methods where subjectivity is involved it becomes imperative that it is beyond reasonable doubt. In cases where the witness has seen accused for the first time, the Supreme Court at various instances has held that identification procedure wouldn't amount to the proof beyond reasonable doubt.[28]

There have been quite interesting cases with regard to this as well. In the case of State of Madhya Pradesh v. Sunder Lal, it was contended that the 13 year old girl just caught the fleeting glimpse of the accused and has forgotten his face and therefore reliance cannot be placed on identification procedure.[29] Their lordships were of the opinion that she couldn't forget the face of a man who has committed such a ghastly crime upon her and said that identification procedure was believable.[30]

4.2. Scientific Evidence: High Probative Value Subject to Safeguards

Fingerprint and DNA evidence, when properly gathered, processed, and authenticated, command robust probative force in Indian courts.[31] Provided procedural rigor, chain of custody, expert credentials, lab accreditation, documented protocols, the courts accept such evidence as strong corroboration or near-conclusive proof unless convincingly rebutted.[32]

Nonetheless, courts remain vigilant. DNA evidence has been discarded in judgments where contamination, incomplete documentation, or improper storage cast doubt. Because India lacks a uniform admissibility standard, courts often evaluate forensic evidence case-by-case, relying on expert consensus, procedural transparency, and cross-examination.

---

[26] Indian Evidence Act of 1872, § 9.
[27] Visveswaran v. State Rep. by S.D.M., A.I.R. 2003 S.C. 2471.
[28] Chander Pal v. State of Haryana, A.I.R. 2002 S.C. 989.
[29] State of Madhya Pradesh v. Sunder Lal, 1992 Cri. L.J. 2519.
[30] *Id.*
[31] Sunil K. Verma & Gajendra K. Goswami, *DNA Evidence: Current Perspective and Future Challenges in India*, 241 FORENSIC SCIENCE INTERNATIONAL 183 (2014).
[32] *Id.*

Facial recognition, iris biometrics, and algorithm-based identifications are newer to Indian jurisprudence. Given concerns about algorithmic bias, error margins, and opacity, courts often require human review, explanation of methodology, disclosure of training data, and expert cross-examination before accepting machine-only identification results.

4.3. Constitutional and Statutory Constraints

The constitutional right to privacy was recognized in Puttaswamy v. Union of India.[33] It restricts intrusive collection or retention of biometric or genetic data by the State unless justified by law, necessity, and proportionality. The Criminal Procedure (Identification) Act, 2022 authorises the collection of "identifying information" such as fingerprints, DNA, etc., from convicted or arrested persons. However, this statutory power must be exercised compatibly with privacy rights, avoiding arbitrary or disproportional intrusions.

Article 20(3)'s protection against self-incrimination is another significant constraint.[34] Courts have grappled with whether compelling biological samples infringe this right. Some judgments hold that such samples are physical, non-testimonial, and thus do not attract Article 20(3). Others caution about overreach if compulsion is indiscriminate.[35]

The statutory and constitutional landscape in India is evolving. The DNA Technology (Use and Application) Regulation Bill, 2019, which aimed to regulate DNA collection, retention, and databanks, with safeguards for privacy and limited uses, was withdrawn from the Lok Sabha in July 2023. Several parliamentary reports had expressed concerns about the bill potentially being misused to target individuals based on religion, caste, or political views. While DNA technology is recognized as a valuable tool for forensic investigations and identifying individuals, including victims and missing persons, its use in India currently lacks a specific, comprehensive legal framework. However, the Criminal Procedure (Identification) Act, 2022 incorporates some provisions related to the collection, storage, access, and sharing of DNA information, addressing the immediate needs for its use in criminal investigations. In the absence of specific legislation, the admissibility of DNA evidence is largely determined by judicial discretion, leading to inconsistencies in court decisions. Until legislative uniformity

[33] Puttaswamy v. Union of India, (2017) 10 SCC 1.
[34] Constitution of India of 1949, A. 20 (3).
[35] Selvi & Ors v. State of Karnataka, AIR 2010 SC 1974.

arrives, judicial discretion and procedural enforcement remain primary safeguards.

5. Recommendations

Following the analysis of India's identification regime, this section outlines a calibrated reform approach that integrates scientific rigor, constitutional protection, and procedural fairness. The recommendations focus on updating identification architecture, establishing clear statutory standards, institutionalizing quality control, ensuring algorithmic transparency, implementing robust privacy safeguards, and enhancing judicial and investigative capacity.

A hybrid identification architecture should be adopted, prioritizing scientifically robust methods while carefully integrating others. Fingerprinting and DNA profiling should serve as the primary identification techniques where physical evidence is available. Subjective methods, such as Test Identification Parades (TIP) and photo arrays, should be relegated to a supplementary role, used only when biometric options are unavailable. The gradual introduction of advanced biometrics, including facial recognition and iris scanning, must be contingent on thorough validation to ensure reliability.

To ensure forensic safeguards are operational, new legislation is required to set minimum standards and provide clear guidelines. Even the Supreme Court has suggested that law relating to identification procedures need to be amended to cater the needs of criminal justice system.[36] This legislation should prescribe protocols for sample collection, storage, and chain of custody, as well as standards for blind lineup procedures, accreditation, and algorithm validation. Additionally, provisions must be made for rights of review. To effectively implement these new standards, the existing framework under the Bharatiya Nagarik Suraksha Sanhita (BNSS) and the Bharatiya Sakshya Adhiniyam (BSA) must be aligned with and supplemented by specific rules.

Forensic accreditation and quality control must also be institutionalized across the country. All forensic laboratories should be required to obtain and maintain accreditation. This would involve mandatory adherence to standard operating procedures, regular audits, transparent reporting, proficiency testing, and ongoing studies of error rates. These measures will build trust in forensic evidence and ensure consistent, high-quality results.

[36] State of U.P. v. Ram Babu Misra, (1980) 2 S.C.C. 343.

For algorithmic technologies, such as facial recognition and gait analysis, there must be a commitment to transparency and human oversight. Developers must disclose training data, error margins, and the results of bias audits to allow for independent scrutiny. Furthermore, courts should require human expert validation of algorithmic determinations and allow cross-examination of the underlying technology and its findings to prevent overreliance on potentially flawed systems.

Protecting individual privacy is paramount, consistent with the principles established in the Puttaswamy judgment. This requires implementing strict safeguards for genetic and biometric data. Key measures include informed consent (where applicable), robust deletion policies, restricted access to profiles, data minimization practices, and the establishment of independent oversight boards to protect against misuse.

Procedural safeguards for lineups must also be mandated to reduce eyewitness error and bias. These safeguards should include double-blind lineups where neither the administrator nor the witness knows the suspect's identity. Furthermore, neutral instructions for witnesses, random placement of fillers, the inclusion of Panch Witnesses, video recording of proceedings, and contemporaneous documentation should all be standard practice.

Finally, judicial and investigative capacity building is essential to ensure these reforms are effectively implemented. Comprehensive training programs are needed for police, prosecutors, and judges to increase their literacy in forensic science, algorithmic processes, error analysis, and cognitive biases. In parallel, establishing an independent oversight mechanism, such as a National Forensic Regulator or Commission, would ensure accountability by empowering a body to audit labs, set guidelines, monitor court compliance, investigate forensic misconduct, and publish objective error statistics.

6. Conclusion

Identification is the linchpin that links suspicion to conviction. India stands at a critical juncture: its traditional reliance on perceptual methods like lineups is increasingly untenable in an era of biometric and algorithmic technologies. Yet blind adoption of technology without legal safeguards risks grave violations of rights.

Indian jurisprudence rightly treats perceptual identifications as corroborative, not conclusive,

and places heavy reliance on biometric evidence when procedural rigor is met. Going forward, India must pivot toward a balanced, hybrid system in which fingerprinting and DNA profiling form the foundation, supported by validated biometric tools and controlled perceptual methods. This transformation must be undergirded by legislation, forensic accreditation, algorithmic openness, privacy protection, and capacity building.

If implemented diligently, such reforms can reduce misidentification, strengthen public confidence, uphold constitutional values, and deliver justice more reliably. The task now lies in translating these principles into operational law, institutional frameworks, and judicial culture.