
Investigative Frontiers Integration of Science Transforming Criminal Investigation

Year: 2026

Face of Justice: Biometrics, Facial Recognition, and the Ethics of Intelligent Surveillance

Dr. Santosh Kumar¹, Dr Manish Bharadwaj²

¹*Assistant Professor of law Amity law School Amity University, Gwalior, Madhya Pradesh*

²*Assistant Professor of law Amity law School Amity University, Gwalior, Madhya Pradesh*

Abstract

Artificial Intelligence (AI) has greatly improved biometric technologies, such as facial recognition, which are now an essential part of intelligent surveillance and contemporary criminal justice systems. It is a review of the principles, applications, opportunities, ethical considerations and regulatory issues on the use of AI powered Facial Recognition Technology in India. It outlines the basics of biometric modalities, how facial recognition works, and some of the ways it can be applied in law enforcement, border security, smart cities, and digital identity management. The review also emphasizes the efficiency and effectiveness of smart surveillance in crime prevention and suspect identification, as well as its limitations and the need for human monitoring. Ethical concerns such as privacy and data protection, algorithmic bias, civil liberties and new regulatory frameworks are critically analyzed, as are future policy trends and directions to support responsible and ethical use of biometric surveillance technology, to ensure that it is transparent, secure and accountable.

Keywords; Facial Recognition Technology; Biometrics; Intelligent Surveillance; Artificial Intelligence; Responsible AI.

¹ ISBN No. - 978-93-7640-081-2

1 Introduction

Biometric technologies are automated systems used to identify or verify an individual by means of their physical or behavioural traits, such as fingerprints, facial features, iris patterns, voice, gait or DNA. Facial Recognition Technology (FRT) is one of the most widely used biometric technologies, as it allows for faster, contactless and non-intrusive identification from digital images and streams of video. Conventional authentication methods include passwords or identity documents, while facial recognition relies on artificial intelligence (AI) and computer vision technologies to identify facial landmarks, extract distinct facial features, and match them to a database of faces for identification or authentication purposes.²

Facial recognition has been closely following in the footsteps of AI, especially machine learning and deep learning. In the early days of facial recognition, the systems were limited to hand-crafted approaches to feature extraction and controlled imaging conditions, making them unfeasible for real-world applications. The recent advancements in the field of CNN, large-scale biometric datasets and high performance computing have led to great progress in light, expression, and pose variation recognition accuracy. Thus, AI-powered facial recognition has become real-time and large-scale identity matching, enabling it to address a wide range of operational scenarios.³

Facial recognition is an example of a technology that has been widely adopted and integrated into our global security and surveillance landscape through the use of AI. The technology is becoming more and more popular within law enforcement to recognize suspects, find missing persons, aid with criminal investigations and improve Public Safety. In a similar way, border management cops and airports deploy biometric verification for passenger processing, and extend the use of facial recognition to a vast camera network at smart cities to facilitate traffic monitoring, access control, and public surveillance.⁴

Despite the operational advantages, there are significant ethical, legal, and social issues with the fast growth of facial recognition. The use of intelligent surveillance systems has sparked a

² H. Choung, P. David, and T.-W. Ling, "Acceptance of AI-powered facial recognition technology in surveillance scenarios: Role of trust, security, and privacy perceptions," *Technol. Soc.*, vol. 79, p. 102721, 2024, doi: <https://doi.org/10.1016/j.techsoc.2024.102721>.

³ C. Mingsung and L. Cai, "Research on the Application of Face Recognition System," in *International Conference on Humanities Science and Society Development*, 2020, pp. 23–29. doi: 10.1088/1742-6596/1684/1/012126.

⁴ N. Lynch, "Facial Recognition Technology in Policing and Security—Case Studies in Regulation," *Laws*, vol. 13, no. 35, pp. 1–14, 2024, doi: <https://www.mdpi.com/journal/laws>.

renewed debate on how to avoid and prevent discriminatory outcomes, algorithmic bias, data security, informed consent and questions of privacy. The potential for misidentification and insufficient regulatory oversight further underscores the importance of a balance between technological innovation and safeguarding fundamental rights and civil liberties. Hence, the present review explores the technological underpinnings, use, ethics and governance issues of biometrics and AI-powered facial recognition in modern "intelligent" surveillance.⁵

2 Biometrics and Facial Recognition Technologies: Principles and Applications

The use of biometric technologies has emerged as crucial parts of contemporary identity management and intelligent surveillance solutions, allowing for automatic identification and verification of individuals based on their distinctively human traits. Unlike traditional authentication methods that are based on either a combination of a password or a document of identification, biometric systems are based on measurable physiological or behavioural characteristics. Over the years, the accuracy, speed and scalability of biometric recognition systems have been enhanced by the continuous development of artificial intelligence (AI), computer vision and deep learning, and making them applicable to large, public and private setups. Facial recognition is one of the modalities that is most highlighted from the available biometric technologies as it provides non-contact identification, can be used with an existing camera system, and can be used for real-time recognition in dynamic environments. The principles of biometric technologies and the working process of facial recognition should be understood to be able to assess their capabilities and limitations in terms of applications in the field of intelligent surveillance and criminal justice.⁶

A. Overview of Biometric Modalities

Biometric systems use physiological or behavioural features to recognise identities. Physiological biometrics encompass facial characteristics, fingerprints, iris patterns, palm prints and DNA; behavioural biometrics include voice, signature dynamics, gait and keystroke patterns. Each modality has its own specific advantages with regards to accuracy, permanency, ease of use, and resistance to spoofing.

⁵ R. B. Sedilla, R. T. M. C. B. T. Pacheco, and M. J. P. Baric, "AI in Criminal Justice: Enhancing Crime Prediction, Surveillance, and Forensic Investigations in the Philippines," *Int. J. Law Soc.*, vol. 9, no. 2, pp. 254–261, 2026, doi: <https://doi.org/10.11648/j.ijls.20260902.21>.

⁶ B. Arora, A. Raj, and S. Kumar, "Biometric Data and Facial Recognition," *Indian J. Leg. Rev.*, vol. 6, p. 192, Mar. 2026, doi: 10.65393/OOCB1973.

In particular among these modalities, facial biometry has emerged as the most popular option since a facial image can be obtained from a distance without requiring any user action or direct interaction. Unlike fingerprint or iris recognition, facial recognition can be used to identify people in video footage, on mobile devices or from surveillance footage, making it particularly useful for public security, transportation hubs, and smart city applications. The incorporation of deep learning algorithms has significantly improved the capability of facial biometric systems to recognize facial images in challenging scenarios where lighting, facial expression, pose and aging, as well as partial occlusions, vary.⁷

B. Basic Working Principle of Facial Recognition

A typical AI-enabled facial recognition system follows a sequence of interconnected processes:⁸

1. **Image acquisition:** Facial images or video frames are captured using cameras, surveillance systems, or mobile devices.
2. **Face detection and preprocessing:** The system locates the face, aligns facial orientation, and normalizes image quality to improve recognition accuracy.
3. **Feature extraction:** AI and deep learning models, particularly convolutional neural networks (CNNs), extract distinctive facial features and convert them into numerical feature vectors.
4. **Feature matching:** The extracted facial template is compared with stored biometric templates in a database using similarity algorithms.
5. **Decision making:** Based on predefined confidence thresholds, the system either verifies a claimed identity or identifies the closest matching individual from the database.

Recent deep learning approaches have significantly increased recognition accuracy by automatically learning complex facial representations from large datasets, reducing dependence on manually designed features.

C. Types of Facial Recognition Systems

1. **Verification (One-to-One Matching):** Confirms whether a person's claimed identity matches the stored biometric template.

⁷ N. E. L. Fadel, "Facial Recognition Algorithms: A Systematic Literature Review," *J. Imaging*, 2025, doi: <https://doi.org/10.3390/jimaging11020058>.

⁸ S. K. Thampan and J. Joseph, "Intelligent Surveillance System for Crime Prevention Using Deep Learning," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 12, pp. 288–292, 2023, doi: 10.48175/568.

2. **Identification (One-to-Many Matching):** Searches an entire biometric database to determine the identity of an unknown individual.
3. **Static Facial Recognition:** Performs recognition using still photographs or stored digital images.
4. **Live (Real-Time) Facial Recognition:** Analyses continuous video streams to identify individuals instantly in operational environments such as airports, railway stations, and public surveillance networks.

D. Major Applications of Facial Recognition

The major applications of facial recognition include:⁹

1. **Criminal investigation:** Identification of suspects, missing persons, unidentified victims, and forensic comparison of surveillance images.
2. **Law enforcement:** Real-time monitoring, suspect tracking, crime prevention, and investigative support during public events.
3. **Border and airport security:** Automated passenger verification, immigration control, e-passports, and watch-list screening.
4. **Smart cities:** Intelligent traffic management, public safety monitoring, crowd analysis, and urban surveillance.
5. **Access control and digital identity:** Secure authentication for government services, banking, workplaces, educational institutions, and mobile devices.

3 Intelligent Surveillance in Criminal Justice: Opportunities and Operational Challenges

Artificial Intelligence (AI) combined with biometric surveillance has revolutionised criminal justice, allowing for the automated analysis of images, videos, and other digital evidence. Today's smart surveillance systems integrate facial recognition technology, computer vision, machine learning and a robust camera infrastructure to enable evidence-based policing, identify suspicious activity, and individuals. The technologies have improved the situational awareness and investigative efficiency, but system performance relies on the quality of the data, reliability of the systems, and human oversight. However, the use of intelligent surveillance presents technical and operational challenges that could impact its accuracy, fairness, and admissibility in a court of law, thereby limiting its potential to enhance public safety.

⁹ S. Wang, "The Application of Face Recognition System," in International Conference on Social Development and Media Communication, 2021, pp. 242–247. doi: 10.2991/assehr.k.220105.046.

A. Opportunities

Through AI-powered surveillance, law enforcement can now more efficiently and quickly monitor public areas and analyse vast amounts of visual data. Capable of automated recognition and continual monitoring has extended scope of criminal investigations and public security operations.¹⁰

1. **AI-assisted surveillance systems:** By using AI to process live and recorded video feeds, the system identifies unusual activity, can identify individuals and produce automated alerts, which can minimize manual monitoring and enhance investigative effectiveness.
2. **Real-time facial recognition in public spaces:** When used at transportation hubs, shopping centres and public events, facial recognition systems can match live video feeds with databases of persons of interest for fast identification.
3. **Crime prevention and suspect identification:** Intelligent surveillance enables identifying repeat offenders and wanted suspects in real-time, which helps in pro-active policing, to speed up criminal investigations and to gather digital evidence.
4. **Missing person identification:** Face recognition technology allows for the quick identification of missing children, elderly people, and unidentified persons by comparing to government or law enforcement databases.
5. **Counter-terrorism and border monitoring:** Biometric surveillance is used by border agencies and national security agencies for identity verification, to identify people on watch lists, to combat identity fraud, and for enhanced counter-terrorism capabilities.

B. Operational Challenges

Despite the many advances in technology, intelligent surveillance systems are still subject to technical and operational restrictions that can impact recognition accuracy and influence decision making. To meet these challenges, this was always a necessity for the reliable, fair and accountable deployment.¹¹

1. **False positives and false negatives:** Misidentification of innocent people “false positives” or failure to identify genuine matches “false negatives” can taint investigations and result in incorrect interventions.

¹⁰ S. K. Thampan and J. Joseph, “Intelligent Surveillance System for Crime Prevention Using Deep Learning,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 12, pp. 288–292, 2023, doi: 10.48175/568.

¹¹ S. Kakade and U. Raut, “Biometric authentication systems: Trends, challenges, and future prospects – A comprehensive review,” *MethodsX*, vol. 16, 2026, doi: <https://doi.org/10.1016/j.mex.2026.103908>.

2. **Image quality:** The resolution of the camera, motion blur, low light and environment can affect facial recognition accuracy significantly.
3. **Occlusion (masks, lighting, camera angles):** Facial expressions, extreme facial views, lighting, shadow effects and facial coverings can disguise important facial characteristics that are essential for successful recognition.
4. **Database limitations:** The usefulness of biometric databases for recognition performance is closely related to their completeness, quality and representativeness. Reliability of datasets may be compromised by outdated data, limited information, or biased information.
5. **Human oversight requirements:** AI-generated matches need to be used in a way that complements human judgement. To ensure that system outputs are accurate, that contextual evidence is evaluated and that the risk of automated error is minimized, trained investigators must verify these before taking any operational or legal action.

4 Ethical, Privacy, and Human Rights Issues

The growing use of facial recognition technology (FRT) in India has enhanced criminal investigations and public security while raising important ethical, privacy, and human rights concerns. Responsible data governance and regulatory oversight are critical when using AI-powered surveillance technologies that handle sensitive biometric data. With the growing use of facial recognition in policing and public surveillance, it is important to balance the need for security with protection of individual rights, creating a new policy challenge.¹²

- **Privacy and Informed Consent:** Facial recognition systems are used to gather biometric data which can be used to recognize people in public places and generally without their knowledge. These issues involve concerns about personal privacy, informed consent, and how far they can go in controlling the collection and utilization of their own biometric information.¹³
- **Mass Surveillance Concerns:** Facial recognition can be combined with CCTV systems to allow for real-time surveillance of public areas. Such surveillance has a positive impact on crime prevention and public safety, but over monitoring can lead to unnecessary tracking of people and raise issues of proportionality and privacy.

¹² M. Smith and S. Miller, "The ethical application of biometric facial recognition technology," *AI Soc.*, vol. 37, no. 1, pp. 167–175, 2022, doi: 10.1007/s00146-021-01199-9.

¹³ M. Pisarić, "Intelligent Video Surveillance, Police And Human Rights," *Facta Univ. Ser. Law Polit.*, vol. 24, p. 37, May 2026, doi: 10.22190/FULP260114004P.

- **Data Protection and Biometric Database Security:** Biometric data is highly sensitive and needs to be stored securely, encrypted, and accessed on a need-to-know basis. Poor security controls or unauthorized access can lead to misuse of identity, data breaches, and potential privacy threats in the future, thus the importance of good data governance.
- **Algorithmic Bias and Demographic Discrimination:** If the data used for training the AI models is not balanced, recognition accuracy can differ amongst various demographic groups. This bias has the potential to lead to incorrect identifications or omissions in the matching process, highlighting the need for diverse training data, periodic performance testing, and independent algorithmic audits.
- **Transparency, Explainability, and Accountability:** Facial recognition must be done in a way that is open, with clear goals, working methods and data management processes. AI-generated results should complement, not supplant, human decisions, and accountability measures and regular audits are crucial for responsible deployment.
- **Civil Liberties and Freedom of Expression:** Continuous biometric surveillance could make people more reluctant to attend public events or speak openly about their views, as they would not want to be monitored at all times. Surveillance systems should be put in place for a legitimate purpose, with adequate protection of fundamental freedoms.
- **Public Trust and Social Acceptance:** For public acceptance of facial recognition to occur, it must be done transparently, accurately, with data protection, and under strict oversight by the regulatory framework. Ethical use of AI, independent oversight, and responsible governance are essential for building trust, ensuring balance between safety and privacy/rights.¹⁴

5 Regulatory Frameworks, Responsible AI, and Future Directions

To make the most effective use of technology through facial recognition in India, the appropriate regulation is necessary that will not undermine innovation but also uphold privacy, human rights, and public interest. While the use of AI-powered biometric surveillance in policing, transportation, and public administration continues to grow, responsible governance is crucial to ensure these technologies are used legally, transparently, and fairly. While India has taken steps

¹⁴ G. Mesch and I. Lam, “Public perceptions about the police’s use of facial recognition technologies,” *AI Soc.*, vol. 40, no. 5, pp. 3869–3879, 2025, doi: 10.1007/s00146-024-02158-w.

to establish policies for data protection and responsible AI, ongoing efforts are required to refine governance structures to tackle new challenges arising from intelligent surveillance.¹⁵

A. Ethical AI Principles for Biometric Surveillance

Ethical principles for the deployment of biometric surveillance should adhere to the principles of AI, such as fairness, privacy, transparency, reliability and non-discrimination. Facial recognition systems should be built with a minimum of algorithmic bias, to guarantee the security of delicate biometric data, and to make sure that automated choices help, not supplant, people's decisions. Regularly assessing a system to ensure it is accurate and trusted is also a critical component of ethical AI.¹⁶

B. National Regulatory Approaches

The passing of the Digital Personal Data Protection Act, 2023, represents a key milestone in India's efforts to regulate the processing of personal data, while national AI initiatives underscore the importance of developing AI responsibly and trustworthily. India currently lacks any legislation targeting facial recognition, but the current data protection laws and sectoral guidelines offer a preliminary guideline for responsible use of biometric data by public institutions and private companies.¹⁷

C. Governance Principles

Effective governance of facial recognition systems should be based on the following principles:

- i. **Transparency:** Clearly communicate the purpose, scope, and use of facial recognition systems.
- ii. **Accountability:** Define responsibilities for the collection, storage, and processing of biometric data.
- iii. **Human oversight:** Ensure that AI-generated matches are verified by trained personnel before operational or legal decisions are made.

¹⁵ S. Al Ali, I. Al Shawabkeh, and E. M. AlQodsi, "Facial Recognition Technology: Protecting Biometric Privacy in the Digital Age," *ASCE*, vol. 18, no. 2, pp. 1–9, 2026, doi: 10.1061/JLADAH.LADR-1435.

¹⁶ M. H. Al-bayed, I. Haddad, B. S. Abu-nasser, and S. S. Abu-naser, "Surveillance in the Age of AI: Navigating Ethical Boundaries and Human Rights," *Int. J. Acad. Inf. Syst. Res.*, vol. 9, no. 4, pp. 7–14, 2025.

¹⁷ Y. K. Simanjuntak, D. T. Putra, G. L. Panjaitan, C. G. Siregar, and N. S. P. Pangaribuan, "Privacy Protection And The Use Of Facial Recognition Technology In Public Surveillance: Legal Perspectives And Policy Implementation In The Digital Era," *Probl. Huk. J.*, vol. 9, no. 1, pp. 14–23, 2023, doi: 10.33021/ph.v9i1.5200.

- iv. **Proportionality:** Deploy facial recognition only where necessary and appropriate for legitimate public security objectives.

D. Privacy-Preserving Biometrics and Explainable AI

New privacy-preserving methods like biometric template protection, encryption, federated learning, and secure data processing can further minimize the risk of unauthorized access to biometric data. In the same way, explainable AI can help investigators and regulators to gain insights into the process of making recognition decisions, fostering transparency, accountability, and public confidence in AI-driven surveillance.¹⁸

E. Future Research Directions and Policy Recommendations

Moving forward, there is a need to build a more equitable and non-discriminatory facial recognition model with various Indian datasets, enhance the performance of facial recognition under real-world conditions, and fortify privacy-preserving AI methods. Policy measures should focus on the need for broad regulations in the field of biometric surveillance, on the necessity for independent oversight mechanisms, on standardized proving of accuracy, and on regular audits of the algorithms. To ensure that facial recognition technologies are used responsibly while also serving national security interests, public awareness and cross-disciplinary collaboration will be crucial, along with ongoing monitoring and assessment.

6 Conclusion

In the realm of intelligent surveillance, facial recognition technology has emerged as a game-changer by enabling identity verification, aiding criminal investigations, and bolstering public safety with the aid of AI-powered biometric analysis. It can be seen how it is part of law enforcement, border management, smart cities and digital identity systems, which are areas of great potential for improving operational efficiency and assisting evidence-based policing. The use of facial recognition, however, comes with key privacy, data protection, algorithmic bias, transparency and human rights issues. The increasing use of biometric surveillance in the Indian context underscores the importance of establishing strong governance mechanisms to regulate the responsible and ethical utilization of AI, while simultaneously protecting individual rights and freedoms. Public trust is essential, and depends on regulatory policies that are transparent, data protection measures that are effective, human oversight and on-going algorithmic audits.

¹⁸ S. M. H. Abidi, S. A. Hassan, S. M. Raza, and M. J. Beliatas, "Advances in Face Recognition: A Comprehensive Review of Feature Extraction and Dataset Evaluation," *Electronics*, vol. 15, no. 338, pp. 1–27, 2026, doi: <https://doi.org/10.3390/electronics15020338>.

Going forward, efforts need to be made to enhance fairness, explainability, and privacy-preserving technologies, ensuring that facial recognition technologies can serve national security goals while upholding democratic norms and fundamental rights.

7 Reference

- [1] H. Choung, P. David, and T.-W. Ling, "Acceptance of AI-powered facial recognition technology in surveillance scenarios: Role of trust, security, and privacy perceptions," *Technol. Soc.*, vol. 79, p. 102721, 2024, doi: <https://doi.org/10.1016/j.techsoc.2024.102721>.
- [2] Mingsung and L. Cai, "Research on the Application of Face Recognition System," in *International Conference on Humanities Science and Society Development*, 2020, pp. 23–29. doi: 10.1088/1742-6596/1684/1/012126.
- [3] N. Lynch, "Facial Recognition Technology in Policing and Security—Case Studies in Regulation," *Laws*, vol. 13, no. 35, pp. 1–14, 2024, doi: <https://www.mdpi.com/journal/laws>.
- [4] R. B. Sedilla, R. T. M. C. B. T. Pacheco, and M. J. P. Baric, "AI in Criminal Justice: Enhancing Crime Prediction, Surveillance, and Forensic Investigations in the Philippines," *Int. J. Law Soc.*, vol. 9, no. 2, pp. 254–261, 2026, doi: <https://doi.org/10.11648/j.ijls.20260902.21>.
- [5] Arora, A. Raj, and S. Kumar, "Biometric Data and Facial Recognition," *Indian J. Leg. Rev.*, vol. 6, p. 192, Mar. 2026, doi: 10.65393/OOCB1973.
- [6] N. E. L. Fadel, "Facial Recognition Algorithms: A Systematic Literature Review," *J. Imaging*, 2025, doi: <https://doi.org/10.3390/jimaging11020058>.
- [7] S. K. Thampan and J. Joseph, "Intelligent Surveillance System for Crime Prevention Using Deep Learning," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 12, pp. 288–292, 2023, doi: 10.48175/568.
- [8] S. Wang, "The Application of Face Recognition System," in *International Conference on Social Development and Media Communication*, 2021, pp. 242–247. doi: 10.2991/assehr.k.220105.046.
- [9] S. K. Thampan and J. Joseph, "Intelligent Surveillance System for Crime Prevention Using Deep Learning," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 12, pp. 288–292, 2023, doi: 10.48175/568.
- [10] S. Kakade and U. Raut, "Biometric authentication systems: Trends, challenges, and future prospects – A comprehensive review," *MethodsX*, vol. 16, 2026, doi: <https://doi.org/10.1016/j.mex.2026.103908>.
- [11] M. Smith and S. Miller, "The ethical application of biometric facial recognition technology," *AI Soc.*, vol. 37, no. 1, pp. 167–175, 2022, doi: 10.1007/s00146-021-01199-9.
- [12] M. Pisarić, "Intelligent Video Surveillance, Police And Human Rights," *Facta Univ. Ser. Law Polit.*, vol. 24, p. 37, May 2026, doi: 10.22190/FULP260114004P.
- [13] Mesch and I. Lam, "Public perceptions about the police's use of facial recognition technologies," *AI Soc.*, vol. 40, no. 5, pp. 3869–3879, 2025, doi: 10.1007/s00146-024-02158-w.
- [14] S. Al Ali, I. Al Shawabkeh, and E. M. AlQodsi, "Facial Recognition Technology: Protecting Biometric Privacy in the Digital Age," *ASCE*, vol. 18, no. 2, pp. 1–9, 2026, doi: 10.1061/JLADAH.LADR-1435.
- [15] M. H. Al-bayed, I. Haddad, B. S. Abu-nasser, and S. S. Abu-naser, "Surveillance in the Age of AI: Navigating Ethical Boundaries and Human Rights," *Int. J. Acad. Inf. Syst. Res.*, vol. 9, no. 4, pp. 7–14, 2025.

- [16] Y. K. Simanjuntak, D. T. Putra, G. L. Panjaitan, C. G. Siregar, and N. S. P. Pangaribuan, "Privacy Protection And The Use Of Facial Recognition Technology In Public Surveillance: Legal Perspectives And Policy Implementation In The Digital Era," *Probl. Huk. J.*, vol. 9, no. 1, pp. 14–23, 2023, doi: 10.33021/ph.v9i1.5200.
- [17] S. M. H. Abidi, S. A. Hassan, S. M. Raza, and M. J. Beliatas, "Advances in Face Recognition: A Comprehensive Review of Feature Extraction and Dataset Evaluation," *Electronics*, vol. 15, no. 338, pp. 1–27, 2026, doi: <https://doi.org/10.3390/electronics15020338>.