Journal of Advanced Zoology

ISSN: 0253-7214
Volume 43 Issue S-1 Year 2022 Page 66:69

Use of Facial Recognition Technique in Criminal Investigations in India

Dr. Renu Pal Sood[1] and Ms. Malvika Gupta[2]

Associate Professor[1] and PhD Scholar[2], Shoolini University, Solan, Himachal Pradesh

**Corresponding author's E-mail: Renu Pal Sood*

Article History

Received: 06 June 2023
Revised: 05 Sept 2023
Accepted: 16 Dec 2023

Abstract

The social interactions of the modern period are characterised by the extensive use of technical tools for information processing. Considering the quick advancement of computer technology, they are already competent to perform challenging tasks needing the careful solution of technical and imaginative issues. The term "Artificial Intelligence" is successfully used in a wide range of activities, from smartphone screens to the creation of music and art. Legal academics are increasingly considering the need for using technical tools in criminal area in light of these circumstances, notably for deciding punishment and other kinds of criminal law influence against people who have committed destructive activities. Use of facial recognition technologies is rising in the post-COVID environment. Law enforcement organisations have seen significant gains in criminal investigation and crime prevention thanks to face recognition technologies, but there are also well-known privacy risks and data misuse issues. This essay explores the applications of Facial Recognition Technology in India and dissects the institutional and technological issues on its usage in law enforcement. Additionally, it offers both immediate and long-term answers that must be established before these technologies are widely used.

Keywords: *Artificial Intelligence, Facial recognition, Criminal Investigation*

1. Introduction

Given the rapid advancement of computer technology, it is already shown that they are capable of doing complicated assignments that require comprehensive answers to both technical and imaginative challenges. Artificial intelligence related technologies are currently being successfully applied in many areas of human life, from facial recognition on a smartphone to the creation of original works of art and music. Given these circumstances, the employment of technology in criminal administration of justice, including to decide punishment and other types of factors against people who have committed a criminal act, is being judged by legal scientists more and more. At the legislative level, the term "artificial intelligence" is not yet officially defined. Various rulings on this issue have been laid down in the legal literature. According to one of them, the existence or absence of thinking is what distinguishes artificial intelligence from a regular robot. Thinking is specifically the psychophysiological processes of the operator's brain. As a result, it should be regarded as the area of information technology that focuses on researching and creating machines that have the same cognitive capacities as humans.

What Is Facial Recognition Technique

A digital map of the face is built by the algorithm-based Facial Recognition Technique (FRT) by locating a person's facial features, which is then compared against the data it has access to.

It may be applied in two ways:

Identity Verification

Here, the face map is acquired in order to confirm a person's identification by comparing it to their database-stored photograph. For instance, unlocking phones uses 1:1 verification. It is increasingly utilized to grant access to government programmes or benefits.

One-To-Many Identification

The map of the face is extracted from a picture or video and compared to the whole data to identify the person in the image or video. This method is known as one-to-many identity identification.FRT is typically purchased for 1:n identification by law enforcement agencies like the Delhi Police. It calculates a likelihood of a match score between the suspect who has to be recognised and the database of known criminals. Based on the likelihood that they are the right match, a list of potential matches is created with corresponding match scores. However, a human analyst eventually chooses the final probable match from the list of matches produced by FRT. At least 124 FRT projects are approved by the government in India, according to Internet Freedom Foundation's Project Panoptic, which monitors the growth of FRT in the country. Facial recognition technology (FRT) has been rapidly implemented in India recently without any laws being put in place to oversee their use.

Use of Frt In Criminal Investigations

FRTs have potential in the investigations in terms of their evidentiary value. The Automatic Facial Recognition System in India is designed to make it easier to investigate crimes, identify criminals, and find criminals, missing children and adults, unidentified dead bodies, and untraced children and adults (NCRB, 2020). Due to weak or untraceable evidence, 75% of First Information Reports (FIRs) in 2017 were closed without inquiry. The use of technology can significantly improve the quality of the investigation, especially considering the high number of vacancies in the police and the backlog of cases. Currently, investigations are primarily reliant on oral testimony, therefore if witnesses become hostile, the matters are frequently not followed owing to a lack of evidence. The issue of evidence quality and pendency can both be addressed with the use of improved forensic evidence and results from CCTVs/FRT. According to statistics 3,000 missing children were found utilising FRTs by the Delhi police. According to news reports from April 2018, the Delhi High Court's facial recognition system trial was successful in identifying almost 3000 missing children.

In Sadhan Haldar v. The State NCT of Delhi , the Delhi High Court authorised the use of Automated Facial Recognition System (AFRS) for the tracking and reunion of children. 3202 of the 10,617 children whose identities the system had matched with missing cases across the nation have had their identities confirmed. Due to greater evidence, FRTs also have an edge in terms of their huge impact on policing procedures, particularly those involving custody. It's commonly known that the police have used force against people who are in their custody.The limited time in custody is the fundamental justification for the employment of "third-degree" procedures in India. Due to the police's obligation to present the suspect to the court within 24 hours, there is less time for an interrogation. Additionally, confessions made to them are not admissible as evidence, which fosters widespread mistrust of the police. However, Section 27 of the Indian Evidence Act permits evidence that is discovered as a result of a confession to be used in court. If the evidence is accepted, FRT might contribute to addressing the requirement for high-quality evidence. These innovations have the potential to bring down crime as well. Violence cost India 9% of its GDP in 2017, according to the Institute for Economics and Peace. The media has reported that FRTs have worked as deterrents of crime and decreased it’s incidence, despite the fact that we lack estimates of the direct impact of these technologies on the economic cost of violence. As an illustration, the Surat city police attribute a 27% decrease in crime to their FRT system.

Limitations

The quality of the image uploaded or captured (in the case of live automatic facial recognition technology), the use of makeup, the quality of the lighting, and the distance/angle from which the picture was taken are some of the variables that affect how accurate the results are. The accuracy of computerised facial analysis is negatively impacted by variations in position, illumination, and expression, among other things.

FRT has the potential to be helpful in assisting with individual identification, but it has the ability to be misused depending on who uses it, why and how it has been applied. Specially if there isn't a legal or regulatory framework in place to regulate it. Inaccurate, biassed, and discriminating judgements may be made by FRT systems that have been poorly developed and trained.

Two issues can be outlined as to the use of FRT: Problems with misidentification brought on by inaccurate technology Problems with mass surveillance brought on by improper use of technology

Extensive investigation into the technology has shown that racial and gender factors significantly affect accuracy rates.This may lead to either a false positive results, where someone is mistakenly identified as someone else, or a false negative rate, where a person's identity is not confirmed. Cases of a false positive outcome can result in prejudice against the person who was incorrectly identified.

On the other side, instances of misleading negative results may result in the person being barred from using crucial programmes. For instance, where a 90-year-old person's biometric authentication with Aadhaar failed.

At the moment, neither a general FRT legislation nor a data protection statute exist in India to guard against misuse. In such a legal void, there are no controls to guarantee that authorities, as in the case of the Delhi Police, only utilise FRT for allowed reasons.FRT can make it possible to violate someone's fundamental right to privacy by continuously monitoring them.

The narrative of national security enters the picture once again and cannot be disregarded.It is feared that the Act will encourage the gathering of personal information in excess and in contravention of generally accepted best practises for data collection and processing.This information presents several issues because the usage of face recognition technology can result in unlawful detentions and widespread surveillance that violates people's privacy if utilised for propaganda politics.

4. Conclusion

The use of FRT by the state and law enforcement agencies in India is still in its infancy, but it is expanding. The following observations can be made based on information that is readily accessible about the application of FRT in India. There is a requirement for a legal and governing structure. There are currently dearth of legal or regulatory frameworks in India that control the use of FRT, and the country's current legal structure for surveillance does not explicitly include the use of FRT technology.

The Supreme Court ruled in the Puttaswamy case (2017), that the right to privacy is a basic right, and like other fundamental rights, it is not an absolute one. The right is subject to reasonable limitations ie. It must pass three tests: (i) legality; (ii) a justifiable governmental goal; and (iii) proportionality.The laws and rules in place were created to control targeted surveillance, not mass surveillance. The technology for mass surveillance was still in its infancy when these rules and regulations were created, and the conversation around privacy and surveillance was less developed than it is now.The goal limitation, collection limitation, data quality, monitoring and accountability, as well as the rights of the people who are being watched over are essential privacy elements that are not included in India's current surveillance laws. It is crucial that surveillance legislation incorporate these basic principles in the absence of a data protection law.

The use of FRT is a method of mass surveillance, and it is unclear if this method complies with the proportionality principle, which, in the wake of the Puttaswamy ruling, has been adopted as one of the criteria for evaluating constraints on the right to privacy. Additionally, as previously mentioned, the Home Ministry claimed in response to a legal notice submitted by the Internet Freedom Foundation that a 2009 cabinet note serves as the foundation for the FRT system, including the AFRS. However, a cabinet note is not a statutory enactment and cannot be used as a legal basis for the implementation of facial recognition technology.

In the Aadhar decision, the Supreme Court declared that using Aadhar to verify SIM cards was illegal since there was no legal justification for it and that doing so constituted an excessive and arbitrary state requirement. Also unknown are the policies and processes being implemented when the technology is used at the state and local government levels.This raises major questions about governance, responsibility, recourse for the use of FRT, and the regular application of safeguards to defend against abuse. As a result, a precise regulatory framework that outlines FRT's legal applications, the procedures involved in using it, and precautions to prevent its use for widespread surveillance is required.

References:

Agrawal, A., “Issues Around Surveillance In The Personal Data Protection Bill, 2019” MediaNama (2020)
AK, A., “Proportionality Test For Aadhaar: The Supreme Court's Two Approaches”, Bar and Bench (2018)
Aristeidis, T., Cristina, C., et. al., “Bio-Inspired Presentation Attack Detection For Face Biometrics” (2019)
Barik, S., “NCRB Released Revised RFP For AFRS, Scraps CCTV Use”, MediaNama, (2020).
Bedi, A., “Geo-Mapping CCTV Cameras, AI- How Telangana Police Is Using Tech To Enforce Covid Safety”, (2020)
Bhandari V., Parsheera S., et. al.., “India's communication surveillance through the Puttaswamy lens” (2018)
Carlaw, S.,. “Impact On Biometrics Of Covid-19”,(2020) https://www.sciencedirect.com/
Champion, G., “CCTV And The GDPR – An Overview For Small Businesses,” IT Governance UK Blog. (2020).
DCAF Parliamentary Brief, “Safeguards in Electronic Surveillance”, The Geneva Centre for the Democratic Control of Armed Forces (DCAF).
Ghosh, I., “Mapped: The State Of Facial Recognition Around The World”, Visual Capitalist (2020).

Hamann K., and Smith R.,. “Facial Recognition Technology: Where Will It Take Us?”. American Bar Association (2019)
Jain, A.,. “Problems With Facial Recognition Systems Operating In A Legal Vacuum”, Internet Freedom Foundation, (2020)
Kharbanda, V., “Policy Paper On Surveillance In India”, (2015). Cis-india.org.
Law Enforcement Imaging Technology Task Force, “Law Enforcement Facial Recognition Use Case Catalog”, (2019).
Lokaneeta, J., “Why Police in India Use 'Third-Degree' Torture Methods for Interrogation”. The Wire (2020)
Mazoomdaar, J., “Delhi Police Film Protests, Run Its Images Through Face Recognition Software To Screen Crowd,” The Indian Express (2019)
Mohamed, M.A. and Abou-Elsoud, M.E.,et.al, “Automated face recognition system: Multi-input databases”, ICCES (2011)
Nagpal, S., Singh, M., et. al, “Deep learning for face recognition: Pride or prejudice?” arXiv preprint arXiv:1904.01219, June 2019
Peeters, B., “Facial Recognition At Brussels Airport: Face Down In The Mud”, CITIP Blog, (2020)
Reuters, “Delhi, UP Police Use Facial Recognition Tech At Anti-CAA Protests, Others May Soon Catch Up”, India Today (2020)
Satish, M.,. "Bad Characters, History Sheeters, Budding Goondas And Rowdies:Police Surveillance Files And Intelligence Databases In India”, Manupatra (2011)
Singh, NK, “The Plain Truth: Memoirs of a CBI Officer New Delhi”, Konark Publishers, (1996)
Editorial, “How the Police Use Facial Recognition, and Where It Falls Short”, The New York Times.(2020) Available at: https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html
Venkatesan, V. and Mathew, S.,. “Police Reforms Still Largely Only On Paper”, Frontline (2019)
Von Grafenstein, M., “The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation” (2018) BOOKS
Asit Kumar Datta, Madhura Datta,(ed.) et.al, Face Detection and Recognition, Theory and Practice, (CRC Press 2015)
Francoise Fogelman Soulie, Harry Wechsler, et. al. (ed.), Face Recognition From Theory to Applications, (Springer Berlin Heidelberg, 2012)
Nitin Bhatia, V. K. Mago (ed.), Cross-disciplinary Applications of Artificial Intelligence and Pattern Recognition Advancing Technologies, (Information Science Reference, 2012)
Stan Z. Li, Anil K. Jain (ed.), Handbook of Face Recognition, (Springer London, 2011) REPORTS, COMMISSIONS AND COMMITTEES Council of Europe, Guidelines on Facial Recognition, 2021
Council of Europe, CAHAI -Ad hoc Committee on Artificial Intelligence, 131st Session of the Committee of Ministers, 21 May 2021.
European Commission, press release, EU-US: A new transatlantic agenda for global change, 2020.
European Commission, Impact Assessment, 2021, p. 18. France, Finland, Czechia and Denmark.
European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs study, Biometric Recognition and Behavioural Detection, 2021.
UN Human Rights Council, Resolution on the promotion and protection of human rights in the context of peaceful protests, A/HRC/44/L.11, 2020.
World Economic Forum, What to know about the EU's facial recognition regulation – and how to comply, 2021.

Websites

BBC https://www.bbc.com/news/world
CNN https://edition.cnn.com
Reuters https://www.reuters.com
The Hindu https://www.thehindu.com
The Indian Express https://indianexpress.com
Tribune India https://www.tribuneindia.com

List of Abbreviations

AFRS	Automated Facial Recognition System
CCTV	Closed-circuit television
COVID	Coronavirus disease
FIR	First Information Report
FRT	Facial Recognition Technique
GDP	Gross Domestic Product
NCRB	National Crime Records Bureau
NCT	National Capital Territory