Available online at https://sanad.iau.ir/journal/ait
Publisher : Ya.C., Islamic Azad University
Artificial Intelligence Tools in Software and Data Engineering

Using Artificial Intelligence: Focusing on Identity Verification in Police Missions

M. Yavari[1]*, M. Hamidi[2]

[1]Department of law, May.C., Islamic Azad University, Maybod, Iran.

yavari.m3766@gmail.com

[2]Head of the Office of Applied Research, Yazd Provincial Police Command

mahdi.hamidi@iau.ac

Article type: Research Article

Article history: Received 12 May 2024, Revised 12 July, 2024, Accepted 25 Oct. 2024 Published 30 Oct. 2024

***Abstract*- The role of Artificial Intelligence (AI) in the field of security and law enforcement is rapidly increasing. While focusing on its technical, legal, and ethical challenges, despite the significant benefits of AI in crime prediction, data analysis, and increasing police efficiency, the use of these technologies, particularly in the areas of face recognition and identity verification, has raised major concerns. Technical challenges, such as the low accuracy of algorithms in real-world conditions and the potential for false positive and false negative errors, can lead to wrongful identifications and arrests. Furthermore, legal issues like violation of privacy and racial and gender bias stemming from bias in training data have been raised as serious obstacles to the widespread adoption of these technologies. Concerns related to the leakage of sensitive data and the lack of transparency regarding the collection and use of citizens' biometric information are other challenging issues in this domain.**

Keywords: **Artificial Intelligence, Face Recognition, Privacy, Bias, Surveillance**

I. INTRODUCTION

The role of Artificial Intelligence (AI) is increasingly expanding in the field of security and law enforcement across the globe. Law enforcement agencies and authorities are progressively utilizing AI-powered technologies for various purposes, including crime prediction, preliminary data analysis to identify behavioral and criminal patterns, smart administrative tasks like report generation, and improving resource allocation. Among the many applications of AI in law enforcement, identity verification have emerged as powerful tools for identifying suspects, monitoring large populations, and ensuring public safety. Over the last decade, the identity verification process has seen a drastic shift from static to dynamic authentication systems. While the traditional password and PIN techniques have taken center stage until now, their vulnerabilities have increasingly come to the forefront in the form of data breaches, phishing, and fraud. This has, in

Cite this article: M. Yavari1, M. Hamidi. (2024). Using Artificial Intelligence for Identity Verification in Police Missions. ***Journal of Artificial Intelligence Tools in Software and Data Engineering (AITSDE)****, 2* (1), pages.

turn, given rise to the quest for more secure and convenient options, and Behavioural biometrics have been a part of the modern authentication process. AI-based identity verification technologies can help increase trust and transparency in police interactions with the public. With the growing volume and complexity of data and the improving technical sophistication, law enforcement agencies need corresponding investments to use advanced technology for proactive enforcement and reduction. Techniques like face recognition and biometric screening, which now use AI to enhance their performance, can quickly identify individuals and suspects and assist in investigations. The use of these techniques has significantly reduced response times, improved public safety, and provided tools for police officers to combat criminals. These tools are currently used to aid in identifying and preventing drug trafficking, human trafficking, money laundering, border monitoring, behavioral analysis of defendants during interrogation, and other instances. Despite the significant potential of AI to improve police efficiency and effectiveness, the use of these technologies also brings major challenges. These challenges include technical limitations and legal issues related to privacy and racial discrimination, problems related to data management and security, and the need for effective oversight and accountability. Undoubtedly, without carefully considering and addressing these challenges, the widespread use of AI in policing could lead to unintended consequences, including the violation of civil rights, increased public distrust, and the exacerbation of existing inequalities.

Section 1 - Technical Challenges in Identity Verification

Face recognition technology can be used to identify and track suspects or missing persons. Data can also be used to generate thousands of versions of an image with different eye colors, hairstyles, and skin tones, and these synthetic training datasets can dramatically improve the performance of face recognition algorithms. Furthermore, today, biometric indicators such as voice recognition, iris scanning (unique pattern registration), retina scanning (blood vessel patterns), hand geometry (hand shape and size), keystroke dynamics (typing patterns), and gait analysis are used for identity verification. One of the most significant challenges in using face recognition technology in policing is the technical limitations of the algorithms used under different conditions. Factors such as low lighting, varying facial angles, facial coverings (like masks), changes in appearance due to age or injuries, and low image quality can significantly impact the accuracy of these algorithms. Even algorithms that show high accuracy rates in controlled environments may face much higher error rates in real-life situations. This is because real police conditions often involve low-quality images from surveillance cameras, which may lack the necessary resolution for accurate face recognition. [1] Between 2015 and 2018, initial research focused primarily on testing the feasibility and initial implementation of Behavioural biometrics in identity verification systems. These studies were predominantly unimodal in nature, employing keystroke dynamics—defined by the timing of key presses and mouse movement behaviour. For example, a study by Zhao et al (2017) revealed keystroke dynamics could achieve an accuracy rate of 95% for legitimate user identification, but also revealed issues with regard to environmental factors such as variation in typing speed. Similarly, Jain et al (2016) examined the feasibility of employing mouse movement patterns, the results of which indicated that while this approach was effective, it was still vulnerable to spoofing with the use of recorded patterns or even mild imitation. [2]

The potential for errors and misidentification is another serious concern. Numerous cases of wrongful arrests due to face recognition errors have been reported, highlighting the human consequences of these mistakes. In the context of face recognition, there are two types of errors: false positives (incorrectly identifying an innocent person as a suspect) and false negatives (failing to identify a suspect). Both types of errors can have serious consequences. A false positive can lead to the arrest and detention of innocent individuals, while a false negative can result in criminals evading police officers. The

performance of face recognition algorithms is heavily influenced by the quality of the training data used for their development. Therefore, if the training data contains specific societal biases (such as in the United States, where there are particular sensitivities toward the Black community), the resulting algorithm may struggle to accurately identify individuals. Studies have shown that in the US, the error rate of face recognition algorithms is significantly higher for individuals with darker skin tones and women. These biases can lead to discrimination in police operations and disproportionately affect minority communities. [2]

Section 2 - Legal Challenges

2-1- The Challenge of Privacy Violation

The legal definition and meaning of privacy is a right that determines the freedom from intrusive surveillance and the protection of an individual's information. Privacy encompasses various dimensions, including informational privacy, bodily privacy, communication privacy, and territorial privacy. The right to privacy is a fundamental human right enshrined in several international conventions and treaties. Article 12 of the Universal Declaration of Human Rights (UDHR) states that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) of 1966 provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor to unlawful attacks on their honor and reputation, and everyone has the right to the protection of the law against such interference or attacks. Looking at the aforementioned provisions of the UDHR and ICCPR, one can conclude that the legal provisions were suited for the era of telegrams and paper, a time when the digital revolution and technology were unimaginable. However, times have changed, and technology has emerged in society. Drawing the lines and limitations of the right to privacy under these provisions is difficult. Due to this technological revolution, the regulations defined by previous human rights treaties and conventions are no longer considered applicable. The concept of privacy has now expanded to include not only individuals but also governments. Surveillance, data collection, data analysis, profiling, face recognition technology, voice and biometric data, and other activities all contribute to the expansion of privacy rights. In the digital age, the need for a more comprehensive interpretation of privacy is felt, as technology evolves daily. Although AI surveillance systems and face recognition systems have numerous advantages, it is vital to consider their potential risks to privacy and data. These technologies rely on the widespread collection and analysis of visual data, as well as machine learning algorithms, to evaluate personal information through cameras installed in various locations. There are concerns about the continuous and real-time surveillance of individuals using face recognition technology, which constantly tracks and monitors them at all times. Authorities and private entities have the ability to store and analyze extensive records of individuals over time, enabling them to monitor people's actions and interactions. This practice of AI surveillance undermines the anonymity of individuals in public places and areas where they expect complete privacy, while also violating their right to privacy. [3]

The collection and use of individuals' facial data by the police raises serious issues concerning the violation of citizens' privacy. The widespread use of face recognition for surveillance can have a chilling effect on the freedom of assembly and the right to freedom of expression. Even if facial data are collected for legal purposes, there is a risk of their misuse. The unique nature of biometric data, such as facial images, creates specific privacy concerns, as, unlike passwords that can be changed, biometric features are permanent. The lack of clear legal frameworks regarding the collection, retention,

and use of this data can lead to unauthorized uses and the violation of individuals' fundamental rights. [4]

To ensure that face recognition and identity verification technologies are not misused by the police, establishing robust oversight mechanisms is essential. This includes creating detailed records and reports of how and when these systems are used, as well as the role of supervisory bodies in reviewing their deployment. Transparency regarding the operation and deployment of these systems is crucial for building public trust and enabling effective oversight. Should errors or violations occur in the use of these technologies, clear accountability mechanisms must be in place so that affected individuals from misidentification or privacy violations can pursue legal remedies for compensation. Furthermore, the responsibility of the AI-deploying organization and the technology vendor in cases of error or misuse must be precisely defined.

2-2- Discrimination in AI Performance

AI bias occurs when the output of a machine learning model can lead to discrimination against specific groups or individuals. These groups are typically those that have been historically discriminated against and marginalized based on gender, social class, sexual orientation, or race, although this is not always the case. This can happen due to prejudiced assumptions in the model development process or non-representative, inaccurate, or simply incorrect training data. It is important to emphasize that bias means a deviation from a standard and does not necessarily lead to discrimination. Bias in data can manifest in various ways that lead to discrimination, such as algorithmic bias. The quality of the collected data will affect the quality of algorithmic decisions; if the data is biased with a prejudiced example of bias, the result will likely follow, unless appropriate controls are in place. [5]

The data used for making decisions in predictive policing in the US is derived from the collection and analysis of historical crime data and police activity. Reliance on historical crime data for predictive policing decisions is inherently biased because the data shows that the Black community is disproportionately negatively affected in the criminal justice system due to targeted policing and discriminatory criminal laws. Numerous cities across the United States have deployed predictive policing tools. Algorithms may divert supervisory concerns from police officers and their superiors to the technical details of a predictive algorithm. Furthermore, the data on which algorithms are trained can be severely flawed, as reported crimes are not the same as committed crimes, and reported crimes may have been inaccurately described. There are also concerns that disadvantaged neighborhoods will be heavily subject to police surveillance, which can be seen as a form of racial bias. [6]

In cases where Iranian police use AI technology for face recognition of individuals, due to sensitivity toward illegal immigrants, there is a possibility that if the police proceed with an action to arrest unauthorized immigrants using AI face recognition technology, this AI may become biased in identifying faces, leading to the unwarranted detention of some citizens. To prevent this, it is necessary to adjust the input data and AI algorithms to be free of sensitivity and bias regarding facial features, to avoid similar discrimination to what occurs in American policing.

2-3- Data Leakage Resulting from AI Inferred Data

One major problem in machine learning is data leakage, which can be directly linked to adversarial attacks and raises serious concerns about the validity and reliability of AI. Data leakage occurs when the independent variables used to train the machine learning algorithm include the dependent variable itself or a variable that contains explicit information about what the model is trying to predict. This data leakage leads to unreliable and poor prediction results after the model is developed and used. Data leakage prevents the generalizability of the model, which is essential in a machine learning problem, and consequently leads to false assumptions about its performance. To have a strong and generalizable predictive

model that can produce significant prediction results, special attention must be paid to detecting and preventing data leakage. [7] AI systems with facial analysis capabilities can perform behavioral analysis of states such as anxiety, fear, anger, etc. The data resulting from these behavioral analyses must be kept confidential by the police and used strictly within the defined scope of their mission. Therefore, the insecurity of police data centers and the risk of leakage of information resulting from behavioral analyses can emerge as one of the challenges for police in using AI. Furthermore, there is also the possibility of internal misuse and the use of data by police employees themselves. Unauthorized access to this data can be used for personal, political, or commercial purposes, which highlights the necessity for decision-making authorities to establish strict security protocols and regulations for data preservation.

2-4- Citizen Consent and Awareness

Informed consent is a crucial legal and ethical principle applied in various fields, especially medicine, scientific research, and personal data protection. This principle means that an individual must have complete, accurate, and understandable information before making any decision that affects their life, body, or personal information, so they can freely and without any pressure or coercion consent to or decline that action. In many legal jurisdictions, the principle of informed consent is considered a fundamental condition for the collection and use of individuals' personal information. However, applying this principle to the use of face recognition systems in public spaces faces challenges. Can the police be expected to obtain consent from every individual before scanning their face? Even if obtaining consent is not practical in all cases, mechanisms must exist to increase public awareness about the use of these systems. The main issue is finding a balance between the potential security benefits of face recognition and the right to privacy. While proponents argue that this technology can make communities safer by helping to arrest criminals and prevent terrorist attacks, opponents raise serious concerns about its potential for misuse. [8] For example, the General Data Protection Regulation (GDPR) is a legal framework in the European Union whose primary goal is to strengthen and unify data protection for all individuals within the EU and the European Economic Area. This regulation gives individuals more control over their personal data and requires organizations to adhere to strict principles for collecting and processing this data. It defines all covered data privacy laws, sets a baseline standard, and identifies personal data as any information relating to an identified or identifiable natural person (data subject), either directly or indirectly. Therefore, the concept of personal data in the GDPR is much broader than Personally Identifiable Information (PII) like a name or address. In short, any data that identifies an individual or can identify an individual in the future is personal data. Public and non-sensitive information can also fall within the scope of personal data, with pseudonyms, IP addresses, tracking cookies, similar data, as well as location data and online identifiers being added as examples of identifiers in the GDPR definition of personal data. [9] Therefore, the police must have transparent and accessible policies regarding how face recognition and identity verification systems are used and inform citizens about what data is collected, how it is used, and what rights individuals have in this regard, to strike a balance between the benefits of accessing personal identity information and the violation of privacy, thereby gaining the relative consent of citizens.

Conclusion

The use of Artificial Intelligence in security and law enforcement holds immense potential for improving efficiency, reducing response times, and enhancing public safety. Technologies such as face recognition and biometric analysis have emerged as powerful tools for combating organized crime, human trafficking, and other security threats. However, as this research demonstrates, the implementation of these technologies is accompanied by significant technical, legal, and ethical

challenges that must be addressed to ensure public acceptance and effective operation. The findings indicate that technical errors in AI algorithms, especially under poor lighting conditions or the presence of facial coverings, can lead to misidentifications. Furthermore, the presence of racial and gender biases in training data can lead to systematic discrimination against minorities and reduce public trust in police institutions. From a legal perspective, the widespread use of these technologies without clear regulations and strict oversight seriously violates citizens' right to privacy. Issues related to data leakage and internal misuse further underscore the necessity for strict security protocols. For the successful utilization of AI in policing, the following measures must be taken:

1. Developing Legal and Regulatory Frameworks: Creating comprehensive laws for the collection, storage, and use of biometric data, and ensuring accountability in case of errors.
2. Increasing Transparency and Public Information: Informing the public about how these technologies are used and their rights in this domain.
3. Addressing Biases and Striving to use diverse and unbiased training datasets to reduce algorithmic errors.
4. Training Police Forces: Educating officers to understand the technical and ethical limitations of AI systems and how to use them responsibly.

Ultimately, the success of AI in law enforcement depends on a delicate balance between technological innovation and commitment to human rights and ethical values. Only by considering these observations can the full potential of this technology be leveraged in a fair, ethical, and safe manner.

REFERENCES

[1] D. Board, "Law enforcement on the AI frontier," SAIC Publishing, 2024.

[2] S. Tiwari, R, Mishra, "AI and Behavioural Biometrics in Real-Time Identity Verification: A New Era for Secure Access Control," International Journal of All Research Education and Scientific Methods, vol. 11, 2023.

[3] T. W. Ford, "It's time to address facial recognition, the most troubling law enforcement AI tool," Bulletin of the Atomic Scientists, 2021.

[4] R. Ullah, "The impact of Artificial Intelligence (AI) on privacy rights: An analytical exploration," Annual Methodological Archive Research Review, vol. 3, p. 327, 2025.

[5] N. Ezeh, A. Widgery, C. Canada, "Artificial Intelligence and Law Enforcement," National Conference of State Legislatures, 2025.

[6] L. Belenguer, "AI bias: Exploring discriminatory algorithmic," PMC PubMed Central Publishing, 2022.

[7] R. A. Berk, "Artificial Intelligence, Predictive Policing and Risk Assessment for Law Enforcement," Annual Review of Criminology, vol. 4, p. 209, 2021.

[8] Q. Dong, "Leakage Prediction on Machine Learning Models," PMC PubMed Central Publishing, 2022.

[9] A. S. Molashaik, "The risk of AI in cybersecurity: Finding the right balance between security and privacy," IAPP Publishing, 2025.

[10] C. J. Hoofnagle, B. V. Sloot, F. Z. Borgesius, "The European Union general data protection regulation," Information & Communications Technology Law, vol. 28, p. 65, 2019.