



Artificial Intelligence in Criminal Investigation

Yusep Mulyana^{1*}, Subarsyah²

^{1,2} University of Pasundan, Indonesia

Email: yusep.mulyana@unpas.ac.id¹, tedie.sby@unpas.ac.id²

Corresponding author: yusep.mulyana@unpas.ac.id *

Abstract. Artificial Intelligence (AI) plays a vital role in criminal investigations, offering innovative solutions to challenges faced by law enforcement. With its fast and accurate data analysis capabilities, AI can identify behavioral patterns, detect anomalies, and predict potential crimes. Technologies such as facial recognition, social network analysis, and natural language processing help speed up the investigation process and improve prosecution effectiveness. However, the application of AI also raises ethical challenges, including privacy issues and potential bias in algorithms. Therefore, it is important to develop a framework that ensures the responsible use of AI in a legal context.

Keywords: Artificial Intelligence, Crime, Investigation.

1. INTRODUCTION

Artificial Intelligence technology has had a significant impact on various sectors of life, including criminal investigations. The use of this technology in the investigation process aims to increase efficiency and accuracy in uncovering crimes, identifying perpetrators, and analyzing crime patterns.

This technology can quickly analyze large amounts of data, detect anomalies, and generate predictions based on historical data and current information. Its use is not only helpful, but also a crucial element in modernizing and accelerating the law enforcement process.

Basically, Artificial Intelligence has the ability to perform in-depth and systematic data analysis, which is very necessary in criminal investigations. This technology is able to identify complex relationships between various variables in a case, which is often difficult or even impossible for humans to do in a short time.

One of the main applications in criminal investigations is digital forensic analysis, where the technology is used to identify digital traces left by perpetrators in cyberspace. The data can be in the form of emails, text messages, video recordings, or even financial transactions that can be processed to find certain patterns.

For example, algorithms can be used to identify suspicious transaction patterns in financial crime cases, which can lead investigators to a wider network of criminals.

Not only in data analysis, Artificial Intelligence is also used in facial recognition, where this system can match the faces of criminals with existing databases and identify people related to criminal incidents.

This facial recognition technology has proven to be very useful in identifying criminals in public places recorded by surveillance cameras (CCTV). The use of this technology not only saves time, but also reduces the potential for human error in visual identification, especially in situations where the perpetrators use disguises or tools to hide their identities.

In addition, Artificial Intelligence has the ability to manage and analyze DNA data. The investigation process involving DNA often takes a long time. However, with the help of this technology, DNA data can be analyzed faster and more accurately. This is very important in investigating cases involving many DNA samples, such as serial murders or sexual assaults.

Artificial Intelligence can also be used to predict a person's facial appearance based on the genetic information contained in their DNA. This is a breakthrough that drastically improves investigators' ability to build a profile of a perpetrator from biological evidence.

Another advantage of this technology is its ability to predict the possibility of crime through predictive analysis. Algorithms can process historical data on crime patterns in an area and predict the potential location and time of the next crime.

This method allows law enforcement to take preventive action before a crime occurs, which can ultimately reduce crime rates. Although this technology is still in its infancy, several police departments around the world have begun implementing it with promising results. For example, in Los Angeles, crime prediction technology has helped authorities reduce crime rates by 13% in recent years.

While this technology offers many benefits in criminal investigations, its application also presents several challenges, particularly related to privacy, ethics, and potential bias in the system itself. The use of this technology to monitor individuals or groups continuously can raise concerns about privacy violations.

In addition, algorithms, if not carefully designed, can carry biases inherent in the data they are trained on, which can lead to unfairness in the legal process. Therefore, proper regulation and oversight are essential to ensure that the use of technology in criminal investigations does not deviate from the principles of justice and human rights.

In an era where crime is increasingly sophisticated and complex, AI offers solutions that not only increase efficiency but also bring fundamental changes to the way law enforcement works. However, the application of this technology must be accompanied by appropriate policies so that it can be used responsibly and effectively in order to maintain public security and justice. Based on the description above, the problem formulation is:

1. How does Artificial Intelligence improve the efficiency and accuracy of criminal investigations?

2. What are the ethical and technical challenges of applying Artificial Intelligence in criminal investigations and their solutions?

2. THEORETICAL BASIS

Understanding Artificial Intelligence

Artificial Intelligence (AI) or Artificial Intelligence is a branch of computer science that focuses on the development of systems or machines that are able to imitate human intelligence, such as thinking, learning, and solving problems.

AI enables machines to perform tasks that would normally require human intelligence, such as speech recognition, vision, data analysis, decision-making, and problem-solving. AI can be categorized into different levels, ranging from weak AI, which is designed to complete specific tasks, to strong AI, which has fully human-like intellectual capabilities.

In the context of law and crime, AI is specifically used to assist law enforcement officers in the investigation process, evidence analysis, and information management related to criminal cases. The use of AI here includes technologies such as digital forensic analysis, facial recognition, video surveillance systems, and predictive algorithms to analyze crime patterns and predict future criminal incidents.

AI in law and crime plays a role in increasing efficiency in evidence collection, reducing human error in data analysis, and helping to identify and apprehend criminals more quickly. For example, AI is used in big data analysis to filter relevant information from large amounts of digital data, such as video footage, messages, and financial transactions. This helps speed up the investigation process and strengthen the evidence presented in court.

In addition, AI is used in crime prediction by analyzing historical data to predict the likelihood of crime in an area. The algorithms used can detect patterns that are invisible to humans and provide recommendations to law enforcement regarding preventive actions.

In this case, AI not only functions as an analytical tool, but also as a strategic tool in preventing crime.

Types of Artificial Intelligence

There are several types of Artificial Intelligence used in criminal investigations:

a. Machine Learning (Machine Learning)

Machine Learning is a subfield of AI that allows systems to learn from data without having to be explicitly programmed. In criminal investigations, machine learning is used to identify patterns in data, such as recognizing patterns of criminal behavior from video footage or financial transaction data. Machine learning algorithms can help predict crime-prone areas or detect suspicious activity based on historical data analysis.

An example of its application is in the crime prediction system used by police in several countries to anticipate crimes before they occur.

b. Deep Learning (Deep Learning)

Deep learning is a branch of machine learning that uses multi-layered artificial neural networks to analyze data. This technology is very useful in facial and object recognition from CCTV or video footage, which allows for fast and accurate identification of criminals. Deep learning is also used in digital forensic analysis, such as voice and text pattern recognition to help verify the identity of perpetrators or analyze communication content.

c. Neural Networks (Artificial Neural Network)

Artificial neural networks are computing systems that mimic the way the human brain processes information. In criminal investigations, neural networks are often used for image recognition, text analysis, and DNA data management.

An example of its use is in automatic facial recognition, where the system can recognize perpetrators from images taken from surveillance cameras, despite changes in facial expression or lighting.

d. Natural Language Processing

Natural Language Processing (NLP) is a technology that allows computers to understand, analyze, and manipulate human language. In the context of criminal investigations, NLP is used to analyze communications in various forms such as emails, text messages, and telephone conversations. This technology can detect threats or illegal activities by analyzing certain language patterns or contexts used by criminals.

e. Computer Vision (Computer Vision)

Computer vision is an AI technology that allows computers to understand and analyze images or videos. In criminal investigations, computer vision is used to analyze CCTV footage or images taken from crime scenes (TKP).

This technology allows law enforcement officers to recognize certain objects, faces, or activities from videos, which greatly assists in the process of identifying and tracking criminals.

f. Predictive Policing (Predictive Policing)

Predictive Policing is an AI method used to predict future crimes based on historical data and crime trends. Using machine learning and big data analysis, the system can provide recommendations on areas with high potential for crime. These

predictions allow law enforcement to conduct more effective patrols and focus resources on specific areas.

Criminal Investigation

A criminal investigation is a systematic process carried out by law enforcement officers to collect, analyze, and present evidence related to a crime. This process begins immediately after a crime report is received and aims to identify the perpetrators, understand their modus operandi, and gather information necessary for further legal proceedings. In an investigation, every step must be carried out carefully so as not to damage existing evidence and to ensure that all legal procedures are followed.

One of the main aspects of a criminal investigation is the collection of evidence. Evidence can be physical, such as weapons or other evidence, or non-physical, such as witness testimony or CCTV footage. Investigators use a variety of techniques to collect this evidence, including witness interviews, forensic analysis, and field investigations. Careful collection of evidence is essential, as even a small mistake can have a major impact on the outcome of the investigation and subsequent trial.

Once the evidence is collected, the next stage is analysis. At this stage, investigators will assess all the information obtained to look for patterns or possible links between the perpetrator and the crime that occurred. This analysis can involve sophisticated techniques, including the use of information technology and data management systems. With the help of data analysis software, investigators can dig deeper into the information, identify trends, and uncover criminal networks that may be involved.

Criminal investigations often involve collaboration between agencies. Law enforcement may work with other agencies, such as forensic agencies, laboratories, and even international organizations in certain cases. This collaboration is essential to obtaining more comprehensive and effective results in an investigation. By exchanging information and resources, investigators can increase their chances of catching perpetrators and solving cases quickly.

3. RESEARCH METHOD(S)

The research method is descriptive analytical, namely describing the problems and facts that occur based on positive legal norms, namely laws related to this research. The normative legal approach method is to use positive legal norms related to Artificial Intelligence in Criminal Investigation. Data analysis was carried out qualitatively, meaning without using numbers and statistical formulas.

4. FINDINGS AND DISCUSSION

Artificial Intelligence (AI) has changed the way criminal investigations are conducted, especially in terms of efficiency and accuracy. AI technology is able to process large amounts of data quickly and accurately, providing a huge advantage for law enforcement who have to handle various complex evidence and information in a short time.

In traditional investigations, investigators need days or even weeks to analyze CCTV footage, digital data, or other physical evidence. Using AI technologies, such as facial recognition and biometric analysis, these evidences can be analyzed in minutes, speeding up the investigation process.

AI can improve the accuracy of identifying perpetrators. For example, AI-powered facial recognition algorithms can match a suspect's face against a large database more accurately than manual methods, even in less than ideal lighting conditions or imperfect camera positions. This is very helpful in crime investigations that require speed and accuracy in identifying suspects.

In the context of crime data analysis, AI provides extraordinary capabilities in detecting complex crime patterns. Machine learning and deep learning enable AI to identify hidden relationships between different elements of a crime that may not be visible to human investigators.

AI has proven effective in analyzing digital forensic data, such as emails and text messages, to extract critical information quickly and accurately. This capability makes AI invaluable in cases of cybercrime and transnational crimes involving large amounts of digital data.

However, the application of AI in criminal investigations not only provides efficiency and accuracy, but also reduces the risk of human error. In many cases, investigators can be affected by fatigue, bias, or emotional stress, which can lead to errors in evidence analysis or decision-making. AI, which works based on consistent algorithms and without these factors, is able to minimize such errors.

However, AI is not without its challenges. AI algorithms can be affected by biases in their training data, potentially leading to discrimination or unfair outcomes. Therefore, the use of AI in criminal investigations must be accompanied by appropriate regulation and careful oversight to ensure this technology is used fairly and responsibly.

Artificial Intelligence (AI) has been shown to significantly improve efficiency and accuracy in criminal investigations. With its ability to rapidly analyze big data, AI allows law enforcement to process information in a shorter time than traditional methods, such as digital evidence processing, facial recognition, and DNA analysis.

In addition, AI is able to detect complex crime patterns and provide more accurate predictions regarding criminal behavior, helping in the identification of perpetrators and crime prevention. Despite ethical and technical challenges, the right application of AI, supported by adequate regulation and comprehensive training, can strengthen the effectiveness of investigations without compromising the values of justice and human rights. AI is an essential tool to overcome the challenges of modern investigations in the digital era.

The application of Artificial Intelligence (AI) in criminal investigations brings various benefits, but on the other hand, it also raises a number of challenges that must be overcome so that this technology can be applied in an ethical and effective manner. These challenges arise from two main aspects: ethical challenges related to privacy and fairness, and technical challenges related to the accuracy of the technology and the infrastructure required. Both challenges need to be addressed carefully to ensure that AI can function as a tool that supports law enforcement without posing risks to the public or violating basic human rights principles.

One of the main ethical challenges in the application of AI in criminal investigations is the threat to individual privacy and the potential for excessive surveillance. AI systems used for facial recognition, biometric analysis, and crime prediction can provide law enforcement with vast access to track and monitor individuals' activities, which risks violating privacy.

There are concerns that this use of mass surveillance could be abused by authorities to excessively monitor individuals, even when they are not involved in criminal activity. Privacy is a particularly important concern because AI allows law enforcement to more easily monitor populations on a large scale, potentially violating civil rights.

The solution that can be taken is to introduce clear and strict regulations regarding the limitations of the use of AI in criminal investigations. The regulations must ensure that the use of AI is limited to legitimate investigative purposes and in accordance with legal principles.

This transparency is important, where individuals must be given the right to know what personal data is collected and how it is used, so that the potential for misuse can be minimized.

From a technical perspective, one of the biggest challenges in applying AI to criminal investigations is the limitations of technology and accuracy. Although AI has the ability to analyze data very quickly, this technology is not yet fully accurate, especially in the context of facial recognition and identifying criminal patterns.

Misidentifications, such as false positives in facial recognition, can lead to wrongful arrests, which can have a significant impact on a person's life. This is especially problematic when AI is used as the sole decision-making tool in an investigation.

To overcome these challenges, AI technology development must continue to be carried out to improve accuracy, including by involving more high-quality and relevant data. In addition, AI should not be used alone in investigations; there must be a combination with traditional investigation methods and human verification to minimize fatal errors. AI systems should be treated as an aid that increases efficiency, not as the sole decision maker.

5. CONCLUSION AND RECOMMENDATION

Artificial Intelligence (AI) has been shown to significantly improve the efficiency and accuracy of criminal investigations. With its ability to rapidly analyze big data, AI allows law enforcement to process information in a shorter time compared to traditional methods, such as digital evidence processing, facial recognition, and DNA analysis. In addition, AI is able to detect complex crime patterns and provide more accurate predictions regarding criminal behavior, helping in the identification of perpetrators and crime prevention. Although there are ethical and technical challenges, the right application of AI, supported by adequate regulation and comprehensive training, can strengthen the effectiveness of investigations without sacrificing the values of justice and human rights. AI is an essential tool to overcome the challenges of modern investigations in the digital era.

There are ethical and technical challenges to the application of AI in criminal investigations, but with proper regulation, continued technological development, and adequate training, these challenges can be overcome. With the right solutions, AI can be used responsibly to improve the accuracy and efficiency of criminal investigations without compromising ethical principles and human rights.

REFERENCES

- _____, *Artificial Intelligence in Law and Crime Investigation*, Oxford University Press, London, 2019
- _____, *Predictive Policing and AI*, Los Angeles: CrimeTech Press, 2022
- _____, *Artificial Intelligence and Crime Investigation*, New York: TechLaw Press, 2021
- _____, *Digital Forensics in the Age of AI*, Cambridge: ForensicTech Publications, 2020

- _____, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations, RAND Corporation, Santa Monica, 2013
- _____, The Role of AI in Forensic Science, London: Science Press, 2019
- Goodfellow, Bengio, & Courville, Deep Learning, MIT Press, Cambridge, 2016
- Husni. Forensic Analysis in Criminal Investigation. Laksana, Yogyakarta, 2017
- Johnson, Digital Ethics and AI, Routledge, London, 2021
- Jurafsky & Martin, Speech and Language Processing, Pearson, London, 2018
- LeCun, Bengio, & Hinton, Deep Learning, MIT Press, Cambridge, 2016
- Perry, Improving AI Systems in Criminal Investigations, RAND Corporation, Santa Monica, 2022
- Rodriguez, Predictive Policing and AI, CrimeTech Press, 2022
- Roesli, S. Criminal Investigation Methodology. Citra Aditya Bakti, Bandung, 2015
- Russell & Norvig, Artificial Intelligence: A Modern Approach, Prentice Hall, New Jersey, 2010
- Sidharta, Criminology and Law Enforcement. Rajawali Press, Jakarta, 2010
- Smith, AI Bias and Law Enforcement, TechLaw Publishing, New York, 2021
- Stuart Russell and Peter Norvig in Artificial Intelligence: A Modern Approach Prentice Hall
- Suharso, E. Inter-Institutional Cooperation in Law Enforcement. Prenada Media, Jakarta, 2018
- Szeliski, Computer Vision: Algorithms and Applications, Springer, New York, 2011
- Taylor, Ethical Dilemmas in AI and Law Enforcement, Chicago: JusticeTech Publishing, 2023
- Williams, AI and Forensic Science: A Modern Approach, Science Press, London, 2019