



AI in Crime Detection

Abhishek Pagote, Shivanjali Pati, Prof. Reeta Singh, Prof. Nitin Ganeshar

ASM (IMCOST) Institute of Management And Computer Studies

ABSTRACT

Intelligent and machine learning systems have infiltrated cyber-physical systems and smart cities with technologies such as internet of things, image processing, robotics, speech recognition, self-driving, and predictive maintenance. To gain user trust, such systems must be transparent and explainable. Regulations are required to control crimes associated with these technologies. Such regulations and legislations depend on the severity of the artificial intelligence (AI) crimes subject to these regulations, and on whether humans and/or intelligent systems are responsible for committing such crimes, and therefore can benefit from a classification tree of AI crimes. The aim of this paper to review prior work in ethics for AI, and classify AI crimes by producing a classification tree to assist in AI crime investigation and regulation.

Keywords: Crime, Find Criminals, Crime Protection, Ai in Crime, Detect Crime.

Introduction

Artificial Intelligence is an approach to make a computer, a robot, or a product to think how smart human think. AI is a study of how human brain think, learn, decide and work, when it tries to solve problems. And finally this study outputs intelligent software systems. By detecting suspicious activities, AI can prevent crimes, and help investigators identify suspects more rapidly, ensuring stronger public safety and increased community confidence in law enforcement and criminal justice in general. AI also has a significant use in courts of law.

By using AI, companies can identify areas of potential crimes such as fraud, money laundering, and terrorist financing – in addition to more mundane crimes such as employee theft, cyber fraud, and fake invoices – to help public agencies with prosecuting these offenses much more effectively and efficiently.

AI as target crime is committed primarily based on security threats of AI system. Several articles dealt with taxonomy of the security threats; white-box and black-box attacks are the typical threat model. The attack with knowledge of dataset, architecture, and parameters of targeted AI system is called the white-box attack. Whereas the black-box attack contains little or no information about the structure of the targeted system.

Some studies proposed threat models on adversarial example(AEs). The AEs are input data with invisible noise, in order to misclassify the input and degrade the performance of AI. They focused on impacts when malicious data is injected in training phase or in inference phase. The experiments demonstrated the performance reduction of AI system attacked by AEs such as malware detection, facial recognition, intrusion detection, etc.

AI as Target Crime

AI facial recognition assesses clothing, skeletal structure, and body movements in order to detect abnormal or suspicious behaviour among masses, such shoplifters or dangerous drivers breaking traffic laws. It also helps with vehicle identification as AI programs are taught to decipher number plates even with poor resolution or low ambient light. Several governments have already allowed the use of AI in law enforcement, such as the Canadian police.

AI can be very helpful in detecting traffic accidents through closed circuit television (CCTV) surveillance, and online-related crimes including human trafficking, money laundering, fraud and sexual abuse.

By detecting suspicious activities, AI can prevent crimes, and help investigators identify suspects more rapidly, ensuring stronger public safety and increased community confidence in law enforcement and criminal justice in general.

AI also has a significant use in courts of law. Through crime-solving and from a scientific viewpoint, AI improves forensic laboratories and investigators in DNA testing and analysis by processing low-level or degraded DNA evidence which could not have been used a decade ago. Furthermore, decades-old cases have been reopened to submit sexual assault and homicide cold case evidence for perpetrator identifications. Such use of AI decreases unsolved crime which strengthens civilians' sense of trust in justice.

Another application of AI is predictive justice, which is the statistical analysis of a large amount of case law data – mainly previously rendered court decisions – in order to predict court outcomes. This can help judges focus their time on cases for which their expertise has a higher added value. In the long term it can strengthen justice stability worldwide by offering economic players more harmonised court decisions, therefore helping better anticipation.

The Main Concepts of Ai in Crime Detection

- **Predicting Future Crime Spots – Predpol**

One company using big data and machine learning to try to predict when and where crime will take place is Predpol. They claim that by analyzing existing data on past crimes they can predict when and where new crimes are most likely to occur. Currently their system is being in several American cities including Los Angeles, which was an early adopter.

- **Predicting Who Will Commit a Crime – Cloud Walk**

The Chinese facial recognition company Cloud Walk Technology is trying to actually predict if an individual will commit a crime before it happens. The company plans to use facial recognition and gait analysis technology help the government use advanced AI to find and track individuals.

The system will detect if there are any suspicious changes in their behavior or unusual movements. For example if an individual seems to be walking back and forth in a certain area over and over indicating they might be a pickpocket or casing the area for a future crime. It will also track individual over time.

- **Pretrial Release and Parole – Hart and COMPAS**

After being charged with a crime, most individuals are released until they actually stand trial. In the past deciding who should be released pretrial or what an individual's bail should be set at is mainly now done by judges using their best judgement. In just a few minutes, judges had to attempt to determine if someone is a flight risk, a serious danger to society, or at risk to harm a witness if released. It is an imperfect system open to bias.

The Major Issues of Ai in Crime Detection and Possible Solutions

Increased use of AI tools for crime prevention could also cause external risks to cascade in unexpected ways. A company could lose its credibility with the public, regulators, and other stakeholders in myriad ways — for example, if there are false alerts that mistakenly identify people as “suspicious” or “criminal” due to a racial bias unintentionally built into the system. Or, at the other end of the spectrum, if they miss criminal activities, like drug trafficking conducted by their clients or funds channeled from sanctioned countries such as Iran. Criminals could resort to more extreme, and potentially violent, measures to outmaneuver AI. Customers could flee to less closely monitored entities outside of regulated industries. A moral hazard could even develop if employees become too reliant on AI crime-fighting tools to catch criminals for them.

To prevent this from happening, companies need to create and test a variety of scenarios of cascading events resulting from AI-driven tools used to track criminal activities. To outsmart money launderers, for example, banks should conduct “war games” with ex-prosecutors and investigators to discover how they would beat their system.

With results produced through scenario analysis, managers can then help top executives and board members decide how comfortable they are with using AI crime-fighting. They can also develop crisis management playbooks containing internal and external communication strategies so they can react swiftly when things (inevitably) go wrong.

By using AI, companies can identify areas of potential crimes such as fraud, money laundering, and terrorist financing — in addition to more mundane crimes such as employee theft, cyber fraud, and fake invoices — to help public agencies with prosecuting these offenses much more effectively and efficiently. But with these benefits come risks that should be openly, honestly, and transparently assessed to determine whether using AI in this way is a strategic fit. It will not be easy. But clear communication with regulators and customers will allow companies to rise to the challenge when things go wrong. AI will eventually have a hugely positive impact on reducing crime in the world — as long as it is managed well.

Benefits of AI in Crime

WHERE AI WILL BE USED TO DETECT CRIMES IN THE FUTURE

Today, AI is most commonly used to detect crimes such as fraud and money laundering. But in the future, it will likely become commonly used in other industries as well. Below are three areas where we see AI being used to prevent:

1. **Transportation of illegal goods.** With AI, express delivery companies can assess the likelihood that parcels contain illegal goods, like narcotics, and report them to the relevant authorities.

2. **Terrorist activities.** Retailers and pharmacies could use sophisticated AI tools to identify customers who purchase unusual amounts of chemicals that could be used as precursors to terrorist activities.
3. **Human trafficking.** Shipping companies can use their data and AI capabilities to identify the containers that are most likely to be used for human trafficking and thus save lives.

Conclusion and Evaluation

The main purpose of this research is to gather the information about smart ways to find crimes. Moreover, this paper discussed the various types of concepts and issues related to crime.

In conclusion, humanity is called on to evolve by integrating new methods resulting from technical progress and creative destruction. Today's ultra-connected world implies a technological overexposure but also an evolution of criminal practices.

In this context, an equivalent response seems to be crucial to face these new technological challenges. AI could be the answer to curb certain crimes which date back to the dawn of time, such as domestic violence.

In the current context of minorities (religion, race, sexual orientation), the use of AI seems to increase the discrimination they already face.

However, like any immature technology, it needs time and mistakes to progress. Until then, an international consensus is needed to guarantee fundamental rights and principles, especially those of fair trial, and to ensure the privacy of citizens around the world, through code ethics, based on transparency and accountability.

References

- Y. LeCun, Y. Bengio and G. Hinton, "Deep learning", *Nature*, vol. 521, no. 7553, pp. 436-444, 2015.
- N. Akhtar and A. Mian, "Threat of adversarial attacks on deep learning in computer vision: A survey", *IEEE Access*, vol. 6, pp. 14410-14430, 2018.
- G. Hinton, L. Deng, D. Yu, G. Dahl, A.-R. Mohamed, N. Jaitly, et al., "Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups", *IEEE Signal Process. Mag.*, vol. 29, no. 6, pp. 82-97, Nov. 2012.
- I. Sutskever, O. Vinyals and Q. V. Le, "Sequence to sequence learning with neural networks", *Proc. Adv. Neural Inf. Process. Syst.*, pp. 3104-3112, 2014.
- G. Litjens, T. Kooi, B. E. Bejnordi, A. A. A. Setio, F. Ciompi, M. Ghafoorian, et al., "A survey on deep learning in medical image analysis", *Med. Image Anal.*, vol. 42, pp. 60-88, Dec. 2017.