Review Article

Smart Policing: Application of Artificial Intelligence in Criminal Investigation

Tahir ul Gani Mir

Author Affiliation:

Research Scholar, Department of Forensic Science, School of Biosciences and Bioengineering, Lovely Professional University Phagwara Punjab 144411, India.

Corresponding Author:

Tahir ul Gani Mir, Research Scholar, Department of Forensic Science, Lovely Professional University, Phagwara, Punjab 144411, India.

Email: mirtahir4u@gmail.com

Abstract

In 1956 John McCarthy implemented Artificial Intelligence (AI) for the first time. AI is considered a tool for coping with extremely complex problems which cannot be solved through direct equations or statistical techniques. AI could be used for calculating differential and integral equations, electrical circuit theories, logical mathematics, and areas of gaming. Using the same strategy, AI has been included in law enforcement, where it can function as a statistical analysis that can efficiently anticipate and deter crimes. Law enforcement, has gradually turned to artificial intelligence to increase smart policing approaches. AI is said to be a critical element in law and it will help and promote efficiency in certain ways. The primary aim of law enforcement is to prosecute crimes by including a social aspect of protection and security, AI may be used in several forms to accomplish such targets. This article aims at reviewing the use of AI by law enforcement to tackle criminal activities.

Keywords: Smart policing; Artificial Intelligence; Machine Learning; Crime Investigation.

Introduction

Smart Policing can be defined as the use of a police force that is Stringent and Compassionate, Innovative and Smart, Alert and Responsible, Efficient and Responsive, Techno Savvy and Educated. This term was initiated at the 49th Annual Conference of Directors General and Inspectors-General in 2014 by the Prime Minister of India. Smart policing is the use of smart devices and smart methods that have the ability to concern scientific techniques to perform digital investigations automatically and autonomously. It also includes investigating crime or evidence using computing devices. Smart policing is becoming very important in today's developed world to handle organized crimes. Artificial intelligence and machine learning are some of the ideal approaches to deal with many complex and organized crimes. They not only provide accurate results but also provide results very fast. Artificial intelligence and machine learning in the modern world are considered the most important science field to serve mankind. Various smartphone-based devices have been developed that use artificial intelligence and machine learning to serve forensic experts at the crime scene (Duce et al., 2010; Farquhar et al., 1997; Turner, 2005). Nowadays, the rapid advancement of mobile phones and computers has made these gadgets to be used in various criminal activities. Because of the sophistication of technology, it is difficult to provide reasonable

and effective security measures, which makes prosecution of criminal activities involving such devices even more difficult. Digital forensics is the cyber world's computer crime detection technique. In this field, many researchers have helped forensic investigation to solve current challenges (Luger GF, 2010; E. Tyugu, 2011).

Legal insights can give deductively established methods for treating evidence for the act of legitimate framework, which is more complex because of the accessible broad data. Artificial intelligence can give simple and quick answers for lawful society and individuals who need it most. There was a correspondence hole between forensic statisticians, crime examiners, and legal counselors. The factual evidence is effectively misconstrued in court, coming about in wrong choices and deferred equity or wrong equity. Artificial intelligence can give new calculations, and the best techniques can be created to bolster the correspondence between the gatherings in question. Computer based intelligence will show occasions in graphical structures that can be utilized to express situations and bolster probabilistic thinking. Computer based intelligence can likewise give displayed situations and it will be useful for augmenting legal counselors furthermore, judgment from the judges. Artificial intelligence has created numerical and computational devices in the venture that will be evaluated by methods for practical contextual investigations. The normal final product of these modules will be the generation of systematic apparatuses for anticipating legal mistakes and reasonable devices for supporting law specialists (Duce et al., 2010). Artificial intelligence can do meta-examination of the meta-information accessible from various sources and it disentangles the intricate information into a justifiable language at a short access time (E. Tyugu, 2011). The significance of Artificial Intelligence in criminological science is that it's well built up capacity to clarify the thinking procedure and thereby, this thinking procedure differs starting with one calculation then onto the next, or it can be improved with change in the Artificial Intelligence calculations.

Brief Review of Artificial Intelligence used in Griminal Investigation

Accessible literature shows that Artificial intelligence methods as of now have various applications in battling against digital and cyber violations. Neural networks are being applied to interruption recognition and counteractive action. However, there are additional recommendations for utilizing neural networks in Denial of Service

(DoS) identification, PC worm discovery, spam location, zombie recognition, malware grouping, and forensic examinations (Hoelz et al., 2009; Duce et al., 2010). Computer-based intelligence procedures, for example, Heuristics, Data Mining, Neural Networks, and AISs, have additionally been applied to new age anti-virus innovation (Salama, 2017). Wang et al. (2008) expressed that the eventual fate of anti-virus identification innovation is in use of Heuristic Technology which signifies "the information and aptitudes that utilization a few techniques to decide and shrewdly break down codes to identify the obscure virus by certain guidelines while checking

Face recognition is one of the advanced technology and various applications in the field of forensic science. Artificial intelligence and machine learning have made it possible to make face recognition system accurate and efficient. Face recognition is an important application in the field of image analysis. It plays an important role in information access, security machine interaction, etc. Face recognition is a biometric system used to verify a person's identity using facial characteristics. Fuzzy logic, Neural networks, and Genetic algorithm (GA) are some of the commonly used soft computing techniques to face recognition. The neural systems are among the best basic leadership frameworks which can be prepared to perform complex capacities in different fields of utilization, including design acknowledgment, enhancement, identification, and classification. Intrator et al. proposed a crossover or semi regulated strategy. They consolidated un-managed techniques for extricating highlights and directed strategies for finding features to lessen classification mistakes. They utilized feed-forward neural systems (FFNN) for classification (Roomi et al.,2013).

Case-Based Reasoning (CBR) is one of the new examples of artificial intelligence that is used in the field of forensic science. CBR technique can be an elective strategy that can be utilized in crime scene investigation. Although the present techniques utilized in criminology can perform astoundingly well, a few existing handy confinements can be overwhelmed by utilizing CBR approach. By applying the CBR strategy, the connections and links between cases dependent on evidence can be drawn without hardly lifting a finger. The CBR strategy that utilizes scientific information to foresee another case is unmistakably progressively productive as contrasted and the customary legal techniques, which are fundamentally built upon human expert info or analyses (Yeow et al., 2014).

The estimation of the age of the bloodstain is important in the forensic investigation for tracking the actual perpetrator. There are various conventional methods to detect the age of the bloodstain but all have some shortcomings like low accuracy, time-consuming, etc. By virtue of machine learning, a device has been developed to overcome the drawbacks of conventional methods. The device is called a smart forensic phone and can precisely estimate the age of the bloodstain. The principle of the device is based on the change in color of the blood sample with respect to the time. The color change in the sample is recorded by RGB (Red, Green, Blue) values and these values change after a different interval of time and the results are obtained by using a smartphone application. The device can estimate the age of the bloodstain if the blood stain is up to 42 hours old (Shin J et al., 2017).

Facial reconstruction from the skull is a useful asset to support forensic examiners in recognize skeletal remains when other data is not accessible. It has been effectively applied in numerous genuine criminological cases. Although in the previous two decades, many PC designs based facial reconstruction techniques have been developed to assist law enforcement. Researchers from Louisiana State University build up an algorithm to perform facial reconstruction from an unknown skull. This method has scientific application in aiding the forensic experts in the identification of skeletal remains when other data is inaccessible. Existing systems straightforwardly reproduce the face from the skull, but in this technique, they used a database of portrait photographs to make faces, play out a superimposition to get a very much coordinated face, and afterward amend it as indicated by the superimposition. To help this they assemble a successful autoencoder for picture-based facial reconstruction and a generative representation for compelled face in the painting. Another study on facial reconstruction displayed a methodology for craniofacial reconstruction dependent on facial soft tissue thickness insights, using computed tomography (CT) data. Their strategy relies upon 78 selected marks on the skull, which directs the format of the skull to every skull, followed by utilizing the Iterative Closest Point algorithm (ICP) (LiuCelong et al., 2018; ShuiWuyang et al. 2016).

Artificial intelligence and machine learning are also used by forensic experts to detect adulteration in food. Food adulteration is increasing day by day and dealing with these kinds of adulterations, various devices have been developed that can check adulteration and, the quality of food and medicine. Recently researchers from IIT Hyderabad have developed a device by virtue of which one can check the quality of milk using a smartphone application. The smartphone application is provided with kNN and SVM algorithmic database that uses Ph and color values of RGB to detect adulteration in milk (Tripathy et al., 2019). Various spectroscopic devices have been designed that can check the authenticity of medicine. A company called Costumer Physics has built a handy portable spectrophotometer device that can be used to check the quality of food and the authenticity of medicine (Benjamin K et al., 2017).

Artificial Intelligence systems, for example, Artificial Neural Networks (ANN), Genetic Algorithms (GA), and Support Vector Machine (SVM) play a significant job in displaying non-customary answers for fingerprint issues. The concept behind these procedures is to construct a vector of components and teach the computer how to process the vector according to certain specific rules. Along these lines, all procedures and processes proficiently entangled unique finger impression information, and consequently, contribute to taking care of certain issues of the fingerprint recognizable system. The Automated Fingerprint Identification System (AFIS) has replaced human specialists with unique fingerprint identification and classification systems for fingerprints. This consists of two stages: (i) Enlistment stage/Registration stage (ii) identification stage. The first stage is to enlist the individual fingerprint in a database for future use, while the stage of identification is responsible for obtaining the information from the database (Awad A, 2012; Egawa et al., 2012; Jain et al., 2009)

Machine Learning and Artificial Inteligence Currently used by Law Enforcement in India

Punjab police have begun using Artificial Intelligence-Based Facial Recognition System (PAIS) with the motive of face search for arresting criminals. They have developed a database with more than 100,000 records of lawbreakers who were arrested crosswise over Punjab. The thought process behind this application is to click a picture with their cell phones when defied with a suspect. Staqu Technologies constructed the police application, which uses facial recognition to make a face's one of a kind guide. The Punjab police office stowed the FICCI Smart Policing Awards 2018 for utilizing PAIS the state police of Bhubaneswar is about to utilize AI and versatile figuring to improve the investigation of criminal activities. The state police of Bhubaneswar are about to utilize Artificial Intelligence. The innovation will manage police officials on strategies of handling crime

investigation. On the off chance that any official makes any mistake in the investigation, artificial intelligence will quickly give an alarm. It will assist officials with making a fast and precise pursuit of a specific crime and its modus Operandi

Trinetra, an Artificial intelligence empowered application enabled with a database of around 5 lakh lawbreakers was developed by UP police. The database incorporates criminal records of the state police and records from the jail division.

Andhra Pradesh released e-Pragati in July 2018, a database that contains information about Andhra Pradesh's millions of people. The server includes the Aadhaar number for e-KYC authentication. Any kind of information required can be obtained by searching from the database in the control room. The main motive to set up this artificial intelligence was to control the crime rate

The Delhi police have made a step in social media analysis and cyber policing by collaborating with the Indraprastha Institute of Information Technology (IIIT). This collaboration aims to develop an artificial intelligence equipped center that can assist the Delhi police in criminal identification, law and order management, cyber policing, etc. The advanced traffic management system is also to be implemented by the Delhi police. Sensor-enabled High-resolution cameras will also be fitted with real-time traffic volume counting would be installed on roads and signals.

Conclusion

The ability of AI to change policing to smart policing and improve the efficiency of police services, such as to recognize the person of concern in busy, environments, detecting and predicting crime, label and categorizes large police investigation information (such as evidence and chain of custody) has made a dramatic evolution in crime control and criminal investigation. AI technology is also capable of raising situational awareness and understanding among law enforcement, thus leading to the wellbeing of the police due to better-informed solutions to possible dangers. Technologies like robots and drones can also be used to monitor privacy safety and the implementation of these technologies into public safety networks offer a secure way to benefit the public and the police. In addition, robotic and drone technologies could provide valuable intelligence, and increase professionalism in criminal law. In some cases, AI technology is now better equipped

than any individual police officers to identify suspicious activity. By adopting AI, the law enforcement system is better placed to respond to incidents, prevent threats, investigate, and analyze criminal activities.

References

1. Awad, A. I. (2012). Machine Learning Techniques for Fingerprint Identification: A Short Review. Advanced Machine Learning Technologies and Applications, 524–531. doi:10.1007/978-3-642-35326-0_52

2. Benjamin K. Wilson, Harparkash Kaur, Elizabeth Louise Allan, Anthony Lozama, David Bell. (2017) New Handheld Device for the Detection of Falsified Medicines: Demonstration on Falsified Artemisinin-Based Therapies from the Field, The American Society of Tropical Medicine and Hygiene p. 1117 – 1123 DOI:https://doi.org/10.4269/ajtmh.16-0904

1. Celong Liu, & Xin Li. (2018). Superimposition-guided Facial Reconstruction from Skull. ArXiv, 1(1). https://arxiv.org/pdf/1810.00107.pdf

2. Duce DA, Mitchell FR, Turner P (2007) Digital forensics: challenges and opportunities. In: Haggerty J, Merabti M (Eds.), ACSF 2007: Proceedings of the 2nd Conference on Advances in Computer Security and Forensics, School of Computing & Mathematical Sciences, Liverpool John Moores University, UK.

3. Egawa, S., Awad, A.I., Baba, K.: Evaluation of Acceleration Algorithm for Biometric Identification. In: Benlamri, R. (ed.) NDT 2012, Part II. CCIS, vol. 294, pp. 231–242. Springer, Heidelberg (2012)

4. E. Tyugu, (2011) "Artificial intelligence in cyber defense", 3rd International Conference on Cyber Conflict (ICCC 2011), pp. 1–11.

5. Farquhar A, Fikes R, Rice J (1997) The ontolingua server: a tool for collaborative ontology construction. International Journal of HumanComputer Studies 46: 707-727.

6. Hoelz, B. W. P., Ralha, C. G., & Geeverghese, R. (2009). Artificial intelligence applied to computer forensics. Proceedings of the 2009 ACM Symposium on Applied Computing - SAC '09. doi:10.1145/1529282.1529471

7. Jain, A.K., Bolle, R., Pankanti, S.: Biometrics Personal Identification in Networked Society. Springer (2009)

8. Luger GF (2010) Artificial intelligence: structures and strategies for complex problem solving. In: Russell S, Norvig P (Eds.), Artificial Intelligence: A Modern Approach. (6th edn), Prentice Hall, USA.

9. Roomi, Mansoor & Beham, Dr.M.Parisa. (2013). A Review Of Face Recognition Methods. International Journal of Pattern Recognition and Artificial Intelligence. 27. 10.1142/ S0218001413560053.

10. Salama, Usama. (2017, March 22). Smart Forensics for the Internet of Things (IoT). Security Intelligence.

11. Shin, J., Choi, S., Yang, J.-S., Song, J., Choi, J.-S., & Jung, H.-I. (2017). Smart Forensic Phone: Colorimetric analysis of a bloodstain for age estimation using a smartphone. Sensors and Actuators B: Chemical, 243, 221–225. doi:10.1016/j. snb.2016.11.142

12. Shui, Wuyang & Zhou, Mingquan & Deng, Qingqiong & wu, zk & Ji, Yuan & Li, Kang & He, Taiping & Jiang, Haiyan. (2016). Densely Calculated Facial Soft Tissue Thickness for Craniofacial Reconstruction in Chinese Adults. Forensic Science International. 266. 10.1016/j. forsciint.2016.07.017.

13. Tripathy, S., Reddy, M.S., Vanjari, S.R.K. et al. A Step Towards Miniaturized Milk Adulteration Detection System: Smartphone-Based Accurate pH Sensing Using Electrospun Halochromic Nanofibers. Food Anal. Methods 12, 612–624 (2019) doi:10.1007/s12161-018-1391-y

14. Turner P (2005) Unification of digital evidence from disparate sources (Digital Evidence Bags). Digital Investigation 2(3): 223-228.

15. Yeow, W. L., Mahmud, R., & Raj, R. G. (2014). An application of case-based reasoning with machine learning for forensic autopsy. Expert Systems with Applications, 41(7), 3497–3505. doi:10.1016/j. eswa.2013.10.054

16. X. B. Wang, G. Y. Yang, Y. C. Li, D. Liu, (2008) "Review on the application of Artificial Intelligence in Antivirus Detection System", IEEE Conference on Cybernetics and Intelligent Systems, pp. 506 509.

Web Source

1. https://securityintelligence.com/smart-forensics-for-the-internet-of-things-iot/