

The Role of Artificial Intelligence in Digital Forensics: Case Studies and Future Directions

Simon Parkinson, Saad Khan

Abstract

The increase in digital evidence, especially in cases involving Indecent Images of Children (IIOC), presents a pressing challenge for law enforcement agencies. In this article, we discuss two of the most prominent types of Artificial Intelligence (AI) and how they can be used in digital forensic processes, providing examples, and highlighting potential challenges that are likely to be experienced in developing and adopting AI. The two main types are of Data-Driven Model (DDM) age classification and Model-Based Reasoning (MBR), and in this article, examples for both are provided and discussed in the contents of IIOC investigations.

Introduction

Both in the UK and globally, Police forces and law enforcement agencies (LEAs) are facing huge demand to view, process, and analyse digital evidence. The continuous increase in computer, mobile, and internet device use has created rapid growth in digital policing requirements. Future, the increase in case size and diversity in technology utilised by perpetrators will provide problems for law enforcement to handle (Montasari et al., 2020).

One such example demonstrating the growth of digital forensics is that of cases involving Indecent Images of Children (IIOC). In the United Kingdom, just as globally, the number of law enforcement cases suspected of containing Indecent Images of Children (IIOC) is increasing. Details on the specific number of IIOC cases processed in the UK are not available in isolation; however, the Office for National Statistics provides crime trend information in England and Wales over a 20-year duration. In the data set, the number of offences categorised as “Obscene publications, etc and protected sexual material”¹ is provided. As evident in the data, the number of cases has rapidly increased by over a factor of six. This evidences an increased burden on law enforcement resources. Any delay in discovering IIOC content prevents timely conviction and the opportunity to identify victims, which could permit ensuring their safety and well-being. Previous work including partners and children of offenders reveals that families can be without electronic devices for up to three years, adding to the psychological, social, and physical impact of the offence.

The technology, process, and available resources used during forensic investigations have seldom changed in the last 20 years, and due to this restriction, typically only a few concurrent investigations can be handled at any one time, resulting in a continuously increasing backlog. A reduction in processing time would have a transformative impact, by enabling timely identification of victims, swift intervention with perpetrators to prevent re-offending, and reducing the traumatic psychological effects of any ongoing investigation for the accused and their families. Recent literature presenting a survey of practitioner opinion indicates the future value of more advanced technologies, mainly Artificial Intelligence (AI) (Sanchez et al., 2019). The digital investigation process is currently planned and managed manually using finite resourcing. Furthermore, the outcome of the investigation is not known until the end of the process. The investigator is responsible for considering all ongoing cases and determining a viable plan to utilise available resources. The investigator is likely to have competing demands in terms of more cases to process than available resources. For this

¹ Crimes categorised under the offence code 86 “Obscene publications, etc and protected sexual material” is not exclusively those of an IIOC nature and it is unfortunately not possible to acquire further breakdown. Data acquired from <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables>

reason, researchers and practitioners are pursuing the use of AI technologies to enhance and improve investigative processes to scale to current and future demands.

Aim

In this article, we discuss the types of AI and how they can be used in digital forensic processes, providing examples, and highlighting potential challenges that are likely to be experienced in developing and adopting. The paper continues with the use and discussion of IIOC cases as they occupy most of the LEA time yet still have parallels with all other digital investigations that follow the same process model.

What is Artificial Intelligence?

Artificial Intelligence is “the science and engineering of making intelligent machines, especially intelligent computer programs” (McCarthy, John, 2004) and can largely be categorised into two approaches: (i) model-based reasoning (MBR) approaches where sensory input is evaluated against a predefined understanding of how it can be utilised to achieve desired outcomes (often referred to as *action-based AI*), and (ii) data-driven model (DDM) approaches whereby the data itself is processed identify meaning. DDM approaches are typically used for applications where data requires sorting or processing to identify aspects of interest or identify new insights. For example, processing large volumes of images to group them based on their contents. These approaches are used where performing the task manually by a human would be far too time-consuming. MBR approaches are typically used for automating and representing well-known processes. For example, planning the optimal allocation of resources while considering many forensic cases. This would be challenging for a human and error-prone, whereas the machine can objectively consider all possibilities to arrive at the optimal.

How can AI benefit?

There are many potential benefits of adopting AI can Digital Investigations, and here we focus on two specific examples relating to IIOC investigations. The first is a DDM approach involving the use of machine learning to classify images based on the age of individuals (Roopak et al., 2023), and the second is an MBR prioritisation approach where a multi-stage investigation is optimised to handle multiple concurrent cases (Khan et al., 2023).

Age classification: the analysis of computer files is essential to digital forensic processes, regardless of the type of case being investigated. Different file types will be investigated in different ways to establish their relationship to the case. For example, files containing text will be investigated to determine whether their contents and authorship are of significance, whereas image files will be investigated based on their visual contents. One prominent investigative task related to IIOC investigations is establishing the age of individuals within images. This is a challenging task for a human investigator, as cases suspected of involving IIOC content are likely to involve high quantities of images and manually inspecting each will be time-consuming and detrimental to investigator welfare. For this reason, there is strong motivation to pursue the use of DDM AI approaches, in the form of Machine Learning, to predict the age of an individual in an image. Experimental work using supervised machine learning involved algorithms to learn the relationship between 316K images and their known ages before predicting the age of new images (Roopak et al., 2023). The algorithm demonstrated that in 90% of cases, it could correctly separate images into child (<18 years of age) and adult (≥18 years of age) classes. Further, the time to analyse each image is less than 0.5 seconds and considerably quicker than the human analysis. There are however complexities to overcome when utilising a machine learning approach, which often centres around the availability and use of data. There needs to be sufficient labelled (assigned a

known class) data available for training the algorithm and the algorithm should be trained according to the classification aim. For example, if separating the data into child and adult classes, it might be more appropriate and advantageous for the algorithm to be trained to predict whether the individual is a child or adult (binary classification) rather than trying to predict the actual age (regression). This is because the algorithm, just like a human analyst, will find it easier to determine distinguishing visual features to separate children and adults. Predicting actual age is challenging because individuals age at different rates and identifying unique visual characteristics for a specific age (e.g., 25) may not be possible.

Process automation and optimisation: replacing manual multi-stage processes with automated solutions that are capable of dynamically allocating and optimising resources can have a positive impact on the time required to process cases and resource scalability. MBR approaches involve the creation of a model to describe the application and the actions that can be applied. An algorithm can then be used to automatically determine which actions can be applied to manipulate the model's description to reach a goal. One example of an MBR approach is in the modelling and optimisation of the multiple tasks involved in IIOC investigations. Traditionally, these tasks are ordered sequentially and involve data acquisition, data carving, and image processing. Dependencies between stages and different software tools result in a slow case processing duration of 13-25 days per case (Khan et al., 2023). This is time-consuming and hinders the ability to keep pace with case processing demands. Therefore, a change of process is necessary, whereby optimisation of the process can enable concurrent case handling. Using MBR techniques, the investigative actions can be modelled in terms of actions which correspond to each task (e.g., carving, image analysis, etc.), and sensory input (e.g., number of files to analyse) can be used to select the most appropriate task to perform. Furthermore, information regarding any findings of interest (e.g., IIOC images discovered) can be used to prioritise case investigations where computer resources are limited. For example, if only five PCs are available for case investigation at any one time, it would be better to process cases where discoveries are being made to reach prosecution limits more quickly. Empirical analysis of 5 case studies resulted in a reduction of 36% in processing time and a 26% reduction in time required to discover IIOC content. In future work, further experimentation is to be performed to examine the approach's capability when handling a larger number of cases, as well as investigate techniques to increase efficiency. In addition to the analysis using simulated benchmarks, trials within LEAs will enable access to real historic cases. There are however challenges with this approach when it comes to creating the model of the process being automated and optimised. This requires a good understanding of the problem domain and AI technology to model the problem in an abstract way where only key and necessary aspects are modelled to avoid them becoming overly complex.

Key advantages and disadvantages

As the use of AI systems in digital forensic processes progresses, new advantages and challenges will inevitably be identified and addressed by the research community. The below lists summarise key advantages and challenges of using AI in digital forensics:

Advantage

- Automating data analysis and pattern recognition: large volumes of data can be processed efficiently, saving the investigator time, and more quickly identifying any information pertinent to the case.
- Decision-making and optimisation: verifiable and traceable decisions can be made in complex situations maintaining the objective of processing cases more quickly and systematically.

- Natural language processing: the ability to process natural language enables the possibility to interpret the text and identify parts of significance.
- Behavioural/predictive analysis: through the use of DDM approaches, information can be profiled to identify routine and anomalous data sets.

Challenges

- Skills: the development, deployment and maintenance of AI systems require specialist skills and expertise that are currently in short supply. This is not because there is a lack of interest and individuals moving into the sector, rather the growth of AI systems is vastly outpacing the new employees.
- Interpretable and explainable: the output of AI systems often requires further explanation and understanding of how the AI system works to evaluate outcomes. However, the majority of AI systems are to assist less skilled employees in accessing expert systems in a specific domain (Solanke, A. A., 2022).
- Legal and ethical: the use of AI systems in digital forensic processes comes with challenges and enters into unknown territory. The system needs to be deterministic - i.e., its behaviour must be fully predictable and known. Any unexpected behaviour could be problematic and cast doubt over reliability, which could prove problematic to defend.
- Resource constraints: AI systems require significant computing resources – something not available within LEAs due to budgetary constraints. Furthermore, the use of cloud computing resources might not be possible, as it would require case data to be uploaded to the cloud for processing.

Conclusion

In conclusion, the increase in digital evidence, especially in cases involving Indecent Images of Children (IIOC), presents a pressing challenge for law enforcement agencies. The traditional manual methods struggle to keep pace, resulting in significant backlogs and delayed interventions. The integration of Artificial Intelligence (AI) offers a promising solution, with two promising examples discussed in Data-Driven Model (DDM) age classification and Model-Based Reasoning (MBR) process optimisation. AI provides efficient data analysis, pattern recognition, and decision-making, substantially reducing processing times. However, challenges such as skill shortages, interpretability, and legal considerations must be addressed. Despite obstacles, AI has a transformative potential to reshape digital forensics, improving efficiency, and ensuring justice underscores the need for strategic implementation and collaborative efforts in navigating this evolving landscape.

References

Montasari, R., Hill, R., Parkinson, S., Peltola, P., Hosseinian-Far, A., & Daneshkhah, A. (2020). Digital forensics: challenges and opportunities for future studies. *International Journal of Organizational and Collective Intelligence (IJOICI)*, 10(2), 37-53.

Sanchez, L., Grajeda, C., Baggili, I., & Hall, C. (2019). A practitioner survey exploring the value of forensic tools, AI, filtering, & safer presentation for investigating child sexual abuse material (csam). *Digital Investigation*, 29, S124-S142.

McCarthy, John. "What is artificial intelligence?." (2004).

Roopak, M., Khan, S., Parkinson, S., & Armitage, R. (2023). Comparison of deep learning classification models for facial image age estimation in digital forensic investigations. *Forensic Science International: Digital Investigation*, 47, 301637.

Solanke, A. A. (2022). Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. *Forensic science international: digital investigation*, 42, 301403.

Khan, S., Parkinson, S., Roopak, M., Armitage, R., & Barlow, A. (2023, July). Automated planning to prioritise digital forensics investigation cases containing indecent images of children. In *Proceedings of the International Conference on Automated Planning and Scheduling* (Vol. 33, No. 1, pp. 500-508).