KI - Künstliche Intelligenz (2022) 36:121–124
https://doi.org/10.1007/s13218-022-00777-3

EDITORIAL

Special Issue on Application of AI in Digital Forensics

Johannes Fähndrich[1] · Wilfried Honekamp[2] · Roman Povalej[3] · Heiko Rittelmeier[4] · Silvio Berner[5]

Published online: 21 November 2022

Keywords Digital forensics · Artificial intelligence · Legal investigation · Cybercrime

1 Introduction

When crimes are committed, countless traces are created. An constantly growing proportion of these are digital traces. For example approximately 400 thousand new variants of malware enter circulation every day [1]. The increasing proliferation of information systems offers an ever-growing gateway for these malicious programs. With the increasing use of digital communication channels such as instant messaging, the number of traces to be analyzed has grown far beyond human capabilities [2]. With the simplified use of anonymization techniques, new challenges arise, such as the use of author determination methods [3]. This has been researched for years for traditional media such as e-mail, [4] but has found little application in the forensic context. Approaches to the use of machine learning in forensics have also been part of the scientific discourse for some time [5]. The field of digital forensics has specific requirements for the methods used. Chain of custody and legal certainty as well as data protection are major hurdles for the use of Artificial Intelligence (AI).

With this growing amount of potential sources of evidence, the application of AI in forensics is essential. Machine learning and data science methods must be extended to be explainable and valid for legal purposes. One example is the article by Bermann et al. in this special issue, which uses deep learning for the classification of blood spatter patterns in criminal investigations. This article argues that the use of such methods should not be based on trust, but controls of the used data and the learned features which influenced the output of the used methods.

In machine learning, the use of statistical models is validated through experiments, where the data is separated in three sets [6]. This is done to build models which perform well outside the training data set and reduce problems like overfitting [7].

Training set: Most of the data, which is used for training the model. The data points are normally randomly chosen (following a probability distribution) to reduce bias.

Validation set: This is a smaller part of the data to validate hyper parameters of the learned model. After training a model with some parameters, one validates its performance on this data. The date should have the same probability distribution as the training set to reduce bias.

Roman Povalej, Heiko Rittelmeier and Silvio Berner have contributed equally to this work.

✉ Johannes Fähndrich
johannesfaehndrich@hfpol-bw.de

Wilfried Honekamp
wilfried.honekamp@hochschule-stralsund.de

Roman Povalej
roman.povalej@polizei.niedersachsen.de

Heiko Rittelmeier
heiko@rittelmeier.de

Silvio Berner
Silvio.Berner@polizei.sachsen.de

[1] Police College Baden-Württemberg, Villingen-Schwenningen, Germany

[2] University of Applied Science Stralsund, Stralsund, Germany

[3] Police Academy of Lower Saxony, Nienburg (Weser), Germany

[4] Central Office for Information Technology in the Security Sector (ZITiS), Munich, Germany

[5] University of Applied Police Sciences Saxony, Rothenburg O.L., Germany

Test set: Some of the data, which is used to test the model. This data set also should have the same probability distribution as the training set and the validation set. The final performance of the model is tested on this data. Sometimes, this data is not available to the creators of the model.

Depending on the size and quality of the data sets, the learned model has different properties like generalizability, robustness to error and bias, or accuracy. Using this approach, depending on the outcome of the model performance on the test set, we can decide on the utilization of the learned model. For the use of machine learning in forensics, the learned models have to hold to high standards, because errors could have fatal influences on human lives. This means that the test data set must be large and well analyzed to reduce bias or other errors.

Developments in recent years have shown that the heterogeneity of the traces to be processed and their data errors, such as incorrect or outdated information, inconsistencies or missing values, and the amount of irrelevant data, are particularly problematic [8]. The lack of automatic detection of data types, such as entropy analysis, and the lack of ontological integration, such as data property classification [9], and thus understanding the meaning of unstructured data, make this work a high manual effort [2]. One example of such data is the analysis of videos with the goal of identifying humans based on their gait, cloth, or body type features. The article of Becker et al. presents the result of a research project, which uses AI for a forensic analysis of persons.

Artificial intelligence methods have not yet been commonly used in forensic investigations, not only for technical reasons, but also for legal reasons [10]. Typical applications include automatic profiling of suspects, vehicle identification, analysis of cryptocurrencies, or automatic recognition of child pornography imagery [11]. Explainable AI (XAI) is an important methodological approach to meet the legal requirements mentions above, as it can be used to trace how the systems come to their conclusions. The article of Szepannek and Lübke shows an investigation into partial dependence plots for the increase of interpretability for methods of machine learning. They show that partial dependence plots can be used in automated classification of chemical analysis for glass identification tasks.

At many points in an investigation, artificial intelligence methods can facilitate the work, even when the flow of an investigation changes between several people. Here, errors could be avoided, and automatable process steps could be mapped by machine learning and automatically adopted in the future. The article of Solanke et al. analyzes common methods of machine learning and discusses techniques for evaluating their effectiveness, e.g. for classification and regression algorithms. In this regard, the interaction between forensic scientists and investigators must be redefined depending on the context. An attempt to formalize and analyze this process has already been made. The article of Spranger et al. describes a system which is designed for the analysis of mobile communication, enabling investigators to deal with the massive amount of communication found in evidence like smartphones. Various support systems have been presented and their problems and limitations have been discussed. Unfortunately, language models such as BERT and image models such as Image GPT-3 have not yet been integrated into forensic applications [12].

The ever-increasing flood of data to be analyzed, and thus the information content can only be handled by automation. Artificial intelligence methods can and will increasingly support investigative authorities in the future. One challenge in itself is the multimodal processing of data. This includes, for example, object recognition and thus the linking of pictorial and textual representations. In this context, research is still being done today on the semantic analysis of images or videos. Image GPT is a recent example of how a system can be taught identifiers, also called labels, using images. Through one-shot learning, this system can recognize objects in images without having seen them before [13].

Many areas of AI research can find application in forensics. Unfortunately, this connection has not yet been established to the point where the scientific community wants to evaluate it on a large scale. Data sets, problem sets, and application scenarios could and should be created so that more of the new methods can be applied. Specific to the application area under investigation is, however, that the prototypes developed in research must each be tested for legal explainability and forensic replicability. A sufficient understanding of the methods used is necessary to ensure that no errors have occurred in the classification. However, with most blackbox methods, such as large neural networks, comprehensibility is only possible to a limited extent [14]. Several hurdles therefore stand in the way of its use in an investigative procedure. One must provide the right insights and then stand up in court by explaining why this method and its result can be used. We interviewed one of the leading experts in the science of AI and explainability Prof. Dr. Müller at the Technical University Berlin who explains the basic ideas of XAI. An interesting interdisciplinary field of research between computer science and law is emerging here.

This special issue collects papers on AI with application to forensics, focusing on the fusion of computer science, data analytics, and machine learning with discussion of law and ethics for their application to cyberforensics.

2 Content

This special Issue includes the following content.

2.1 Technical Contributions

- Digital Forensics and Strong AI
- Explaining Artificial Intelligence with Care Analyzing the Explainability of Black Box Multiclass Machine Learning Models in Forensics
  (Gero Szepannek, Karsten Lübke)
- Automatic Classification of Bloodstains with Deep Learning Methods
  (Tommy Bergmann, Martin Klöden, Jan Dreßler, Dirk Labudde).

2.2 Discussion Paper

- Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques
  (Abiodun Abdullahi Solanke, Maria Angela Biasiotti).

2.3 System Description

- MoNA: A Forensic Analysis Platform for Mobile Communication
  (Michael Spranger, Jian Xi, Lukas Jaeckel, Jenny Felser, Dirk Labudde).

2.4 Project Report

- COMBI: Artificial intelligence for computer-based forensic analysis of persons Project Reports
  (Sven Becker, Marie Heuschkel, Sabine Richter, Dirk Labudde).

2.5 Interviews

- Iterview: AI Expert Prof. Müller on XAI Interview
  (Johannes Fähndrich, Roman Povalej, Heiko Rittelmeier, Silvio Berner).

3 Service

3.1 Conferences

- International Workshop on Digital Forensics - An interexchange of law enforement and science. https://informatik2022.polizeiinformatik.de/
- Police Informatics. https://polizeiinformatik.de/
- The International Conference on Forensic Computer Science. http://icofcs.org/
- European Academy of Forensic Science Conference. https://www.eafs2022.eu/.

3.2 Journals

- IEEE Transactions on Information Forensics and Security. http://www.signalprocessingsociety.org/publications/periodicals/forensics/
- Forensic Science International: Digital Investigation. https://www.journals.elsevier.com/forensic-science-international-digital-investigation
- Forensic Science Communications. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications
- International Journal of Cyber-Security and Digital Forensics. http://sdiwc.net/ijcsdf/
- International Journal of Digital Crime and Forensics. https://www.igi-global.com/journal/international-journal-digital-crime-forensics/1112
- International Journal of Electronic Security and Digital Forensics. https://dl.acm.org/journal/ijesdf
- International Journal of Forensic Computer Science. http://ijofcs.org/policies-focus.html
- The Journal of Digital Forensics, Security and Law. https://www.jdfsl.org/
- International Journal of Cyber Forensics and Advanced Threat Investigations. https://conceptechint.net/index.php/CFATI

References

1. BSI (2021) Die Lage der IT-Sicherheit in Deutschland. http://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf;jsessionid=90C4A17D4F4086D74E308B211D0A66C1.2_cid287?__blob=publicationFile&v=3. Accessed 11 Apr 2022

2. Spranger M, Heinke F, Appelt L, Puder M, Labudde D (2016) MoNA: automated identification of evidence in forensic short messages. Int J Adv Secur 9:1
3. Iqbal F, Debbabi M, Fung BC (2020) Machine learning for authorship attribution and cyber forensics. Springer, Berlin
4. De Vel O (2000) Mining e-mail authorship. In: Proceedings of the workshop on text mining, ACM international conference on knowledge discovery and data mining (KDD'2000). Citeseer
5. McClendon L, Meghanathan N (2015) Using machine learning algorithms to analyze crime data. Mach Learn Appl Int J (MLAIJ) 2(1):1–12
6. Kohavi R et al (1995) A study of cross-validation and bootstrap for accuracy estimation and model selection. In: Ijcai, vol 14. Montreal, Canada, pp 1137–1145
7. Hawkins DM (2004) The problem of overfitting. J Chem Inf Comput Sci 44(1):1–12
8. Garfinkel S (2012) Lessons learned writing digital forensics tools and managing a 30 TB digital evidence corpus. Digit Investig 9:80–89
9. Glimm B, Horrocks I, Motik B, Stoilos G (2010) Optimising ontology classification. In: International semantic web conference. Springer, Berlin, pp 225–240
10. Rademacher T (2020) Artificial intelligence and law enforcement. In: Regulating artificial intelligence. Springer, Berlin, pp 225–254
11. Raaijmakers S (2019) Artificial intelligence for law enforcement: challenges and opportunities. IEEE Secur Priv 17(5):74–77
12. Povalej R, Rittelmeier H, Fähndrich J, Berner S, Honekamp W, Labudde D (2021) Die Enkel von Locard. Inf Spekt 44(5):355–363
13. Chen M, Radford A (2020) Sutskever: image GPT. https://openai.com/blog/image-gpt/. Accessed 11 Apr 2022
14. Samek W, Montavon G, Vedaldi A, Hansen LK, Müller K-R (2019) Explainable AI: interpreting, explaining and visualizing deep learning, vol 11700. Springer, Berlin