What is the impact of AI used in digital forensics?*

Lukas Frauenknecht
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)
lukas.frauenknecht@fau.de

ABSTRACT

It is no longer a secret that cyber criminals nowadays rely on artificial intelligence (AI) and other automated methods to cause maximum damage in a short space of time with minimal effort. However, automation can also be used in digital forensics (DF) to analyze previous attacks and thus help prevent further attacks. Looking at the current figures, it quickly becomes clear that the number of reports of cyber crimes and the associated damage has multiplied in recent years. AI and its subsets machine learning (ML) and deep learning (DL) are coming into play to deal with the vast amounts of data, caused by this rapidly growing threat. This not only minimizes the loss in the event of damage, but also reduces the costs and time required for the collection, analysis and documentation of data. This is achieved through automation and the associated improved efficiency and reduced susceptibility to errors. The areas of application include automation of routine tasks like data collection, anomaly detection, pattern recognition, predictive analysis and many more. By explaining the process of digital forensics and looking at specific sub-areas, this paper aims to demonstrate the applicability and influence of AI, ML and DL with regard to cyber incidents.

KEYWORDS

Artificial intelligence, Automation, Digital Forensics, Machine Learning, Deep Learning

1 INTRODUCTION

Digital forensics is intended to find, collect, store, analyze and report data. A standardized procedure ensures that no relevant data is forgotten. A defined process model is ideal for this and with its certain degree of flexibility, it can be applied to any type of investigation. This is necessary because the data is often, but not always, digital evidence that is linked to a cyber crime and can only be used in court if a structured approach has been taken and every step has been documented. Cyber crime can be divided into cyber-dependent crime, cyber-enabled crime and crime with digital evidence [26]. As highlighted by the FBI [35], over the past five years, there have been worldwide an average of 758,000 complaints and a total of 3.79 million complaints related to cybercrime, causing a total loss of $37.4 billion. In addition, complaints almost doubled between 2019 and 2023 and the associated loss almost quadrupled [35]. An overview can be seen in Figure 1. According to a global survey conducted by Hiscox [20] in 2023, an average of 53% of the companies interviewed had been affected by a cyberattack in the last 12 months. In Germany, the figure was around 58% [20]. The rising numbers and ever-growing threat posed by cyber criminals should make it clear that the development of DF and its tools and techniques must also be driven forward. INTERPOL states on their website, that *"cybercriminals are increasingly agile and organized – exploiting new technologies, tailoring their attacks and cooperating in new ways"* [21]. AI is a suitable solution as it can process huge amounts of data, recognize patterns between data and solve complex problems with human-like intelligence. However, it can be helpful not only in analyzing evidence, but also in documentation and reporting. The insights gained can then in turn be used to develop preventative solutions that automatically detect new attacks and anomalies that indicate such. The subset ML has established itself as the optimal training method for AI and dominates all specialist areas [14]. A model is developed using selected algorithms, which is trained and improved with the help of large amounts of data. Various learning methods are used for this purpose. Since not only quantity but also quality is important for the learning process, data must be selected in a targeted manner. DL as a subset of ML is used to create order and to label and categorize the data. However, AI is not the universal solution for DF, as it also generates new challenges, as its use must be ethical and acceptable under data protection law. This paper compares whether AI is really suitable for use in DF, how it can be applied and what the difficulties are. First, section 2 explains the basics of DF, its challenges and how AI works. Section 3 highlights the fundamentals of AI with reference to ML and DL. The main part around the core question of the paper, the application of AI in DF, then is shown in section 4. Finally, an outlook and suggestions for future work and research are given in section 5. It is intended to make it easier for interested parties and students to get started with the topics of DF and AI, as it summarizes some of the basics. The aim of this paper is to show the influence and relevance of automation in DF and why it adds value to DF. It can therefore be used as a basis for further research on this topic. A qualitative approach was chosen as the research methodology, in which various scientific documents were researched, compared and summarized. The database of the Erlangen-Nuremberg University Library and Google Scholar, initially limited to a period from 2010 to 2023, were searched for relevant sources. The books and papers found then contained references to various other sources dating back to before 2010. The following keywords were used: Digital Forensics, Computer Forensics, Challenges of Digital Forensics, Automation, Artificial Intelligence, Machine Learning, Deep Learning, Ethics of Artificial Intelligence. In addition, various websites of companies and authorities were used to obtain current statistics and surveys. The methodology and results of this paper are verified by a peer-review process.

*This paper was written as part of the conference seminar "IT Security" which was organized by the chair of IT Security Infrastructures at the FAU during the summer term 2024. Special thanks to Dr. Keyin Mayer for the provided support during the course of this paper.

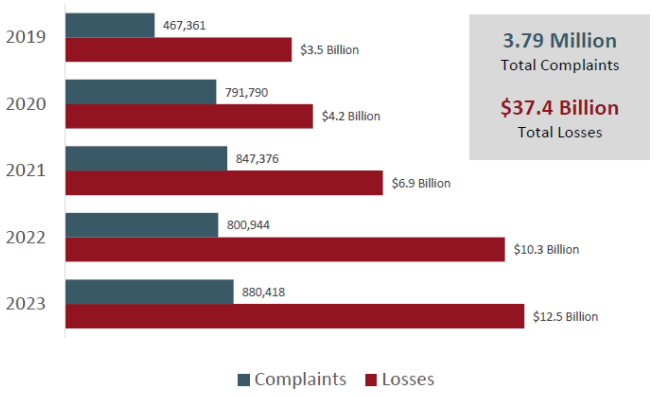

Figure 1: Overview of the complaints and losses over the last five years [35]

2 DIGITAL FORENSICS EXPLAINED

Digital Forensics (DF) is not only a synonym for computer forensics, it is more likely an expansion to it, that includes all kinds of digital technology. DF in general is the process of preserving, collecting, analysing and presenting data, that has a correllation to an occured incident, in order to find evidence that can be used in a court of law due to a cyber crime. Furthermore DF is not only used for inicent response but DF examinations can also help to predict and prevent future cyber attacks. A more formal definition was made by Palmer [36] where he defined the science of DF as *"the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purposes of faciliating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations"*.

A DF investigation should not be thought of as a single process, but more as a collection of individual tasks, steps and routines, to maintain its flexibility to be adapted to each situation [37]. The tools and methods used by DF experts may vary but all must follow a strict order. So no matter how many and how different DF experts take part in an investigation, all of them should come to the same result.

2.1 Digital forensic process model

In order to be successful in a digital forensic investigation, forensic scientist must be well prepared and already have an universal plan of methods before starting the actual examination. Every investigator should use a framework and try to answer the following six questions during an investigation: *who, what, where, when, why and how* [5].

- *Who* are the individuals involved?
- *What* is determined by the data? (data may contain hints to the actions/events)
- *Where* did the incident take place?
- *When* did the incident happen?
- *Why* did the incident occur? (refers to the motivation behind the incident)
- *How* was the incident carried out? (refers to the procedure to perform the incident)

These questions can all be answered by following step-by-step digital forensic process model which consists of several sub-processes. Over the past few years, a number of process models have been developed and improved, which differ in detail and scope but are essentially the same. Kohn et al. [28] compared and combined a number of selected models to create their own *"integrated digital forensic process model"*. This consists of the processes *perparation, incident, incident response, physical investigation, digital forensic investigation, presentation and documentation.* A representation of the processes and their sequence can be seen in Figure 2. These processes are again split in sub-processes, like the digital forensic investigation for example contains collect, examine, compare, analyze, review and many more.

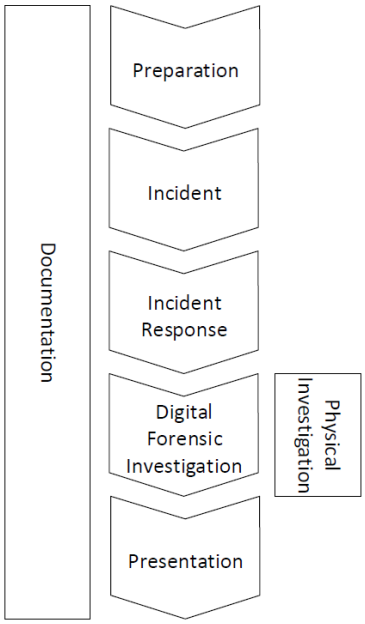

Figure 2: The sequence of the integrated digital forensic process model [28]

2.1.1 Documentation. The documentation process covers the entire examination, contains all relevant investigation documents and serves as a protocol. This log is not only helpful for the ongoing investigation, but also serves to ensure traceability afterwards and is also necessary in court.

2.1.2 Preparation. The preparation for an examination is just as important as the examination itself. All possible factors, both internal and external, are taken into consideration in advance in order to be prepared for any situation. A distinction is made between different types of investigation and the appropriate process description must be available for each type.

2.1.3 Incident. An incident is the actual event to be investigated, to be more precise any action that serves to threaten the confidentiality, integrity, and availability[1] of a system. An incident is detected and reported by an automated detection system or by humans, that inform the appropriate investigative authority.

2.1.4 Incident response. In the event of an incident response, the first investigators decide on a strategy and search directly for potential evidence, which is immediately preserved and stored. Additionally, is is tried to restore the affected system to its original state.

2.1.5 Physical and digital forensic invenstigation. The investigation process is the core of the integrated digital forensic process model and if it is not only carried out on a digital level, then physical and digital forensics run in parallel. The data preserved in the previous process is first copied in order to be able to work with the copies without altering the original data. These are then sorted, categorized and compared so that they can be better analyzed. Finally, the results of the analysis are interpreted and processed so that they can be transmitted to the interested parties and presented in the next step.

2.1.6 Presentation. During the presentation, the results of the investigation are shown to third parties, e.g. the management, in order to draw conclusions and make decisions regarding the incident and all people involved. The outcome is used to review the companies policies and operations, in order to improve. Finally, the original evidence is returned to the owner.

2.2 Challenges in digital forensics

In DF, there have always been a wide variety of challenges that experts have to overcome. Depending on the type and phase of the DF investigation, challenges can arise in different ways. Nickson and Hein [25] group these into four main challenges: *Technical, legal systems and/or law enforcement, personell-related and operational challenges*. These are further divided into sub-categories.

2.2.1 Technical Challenges. Technical challenges can be dealt with specialist knowledge and skills. DF experts need to be familiar with a wide range of hardware and software, technologies and techniques. In addition, they must always be up to date, as newly emerging technologies and devices also bring new challenges. With the advance of digitization and the ever-increasing affordability of persitent and disk storage, the amount of data has multiplied, both in the private and business environment [31]. Not only does it take plenty of time collecting these vast volumes of data, investigators often have just a limited window of opportunity for collection of potential digital evidence. These must then be analyzed as quickly and accurately as possible so as not to endanger the integrity of the data due to the volatility of the digital evidence.

2.2.2 Legal systems and/or law enforcement challenges. In order for the evidence gathered to have any legal value at all and, if necessary, to be used in court, the legal systems and/or law enforcement challenges must be faced. Therefore, the admissibility of DF tools and techniques must always be guaranteed and established scientific standards must be demonstrably respected. But it is not only the jurisdiction that must be considered, because DF investigators often have to deal with ethical issues [4]. Confidential and personal data of individuals and companies must be kept secret and must not fall into the hands of unauthorized third parties or become public under any circumstances, otherwise it is a violation of the data protection law and the code of ethics.

2.2.3 Personnel-related challenges. To prevent this and to ensure the quality of the data analysis, professional personnel are required. However, this is not always available, as there is a lack of qualified digital forensic personnel (Training, Education and Certification) due to the personnel-related challenges. While cybercrime is on the rise and DF is becoming an important area for fighting these crimes, the number of DF experts is only increasing marginally, as it takes some time and dedication to acquire the needed IT skills and experience [10]. The easiest way for new investigators to acquire these is to draw on the findings of previous investigations.

2.2.4 Operational challenges. Operational challenges can be overcome through organizational practices such as planning, monitoring, logging and well-defined procedures. Incident detection, response and prevention systems should be established in any conventional IT environment nowadays. But simply having these systems in place is useless if there are no trained administrators and a lack of standardized processes and procedures exists. These systems and the DF team must be ready for service at all times. The challenge of DF readiness in organizations can significantly affect the outcome of a successful DF investigation, as not all relevant evidence may have been captured [31].

3 FUNDAMENTALS OF ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is nowadays a well known term, which combines algorithms and data analysis with human-like behaviour, to solve complexe problems that "non intelligent" software can't solve. We have all had contact with well-known language assistants or chatbots, which in principle are based on Natural Language Processing (NLP) and Large Language Models (LLM). But for this software to understand us humans, it first has to be taught to do so.

This means that the intelligence which makes AI so special needs to be achieved and trained first. This is where machine learning (ML) comes to play. ML itself also contains another subset called deep learning (DL). The realtionship between automation, AI and ML/DL can be seen in Figure 3. The recognition of human writing and speech can be just as useful in DF as the identification based on biometric features, the search for clues using relationships between individual data fragments or the data analysis itself. [23]

3.1 Machine learning

Machine learning is a subset of AI and has become one of the most used training techniques. It uses large amounts of data and different algorithms with the aim to build up a model which then can be used for big data processing, pattern recognition between different datasets, anomaly detection, prediction purposes and many more. Therefore ML is a perfectly suitable trainig tequnique to be used

[1] **C**onfidentiality, **I**ntegrity and **A**vailability are represented by the CIA-Triad, a common model as basis for the scurity of a system.

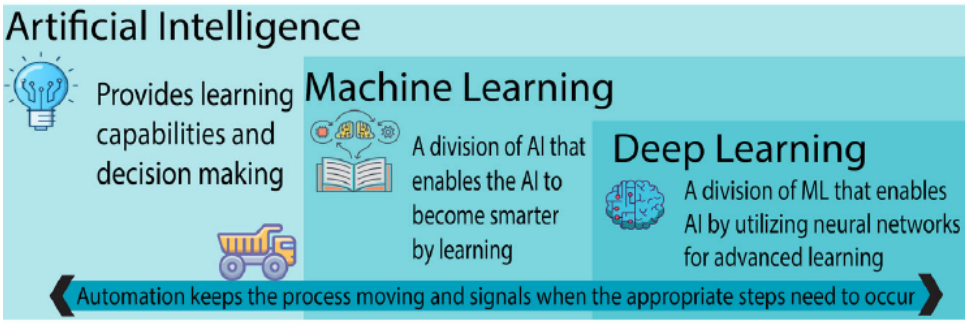

Figure 3: The realtionship between automation, AI and ML/DL [23]

in DF. This goal is achieved through a defined sequence of five steps that are crucial to the success of the ML process: *Data order, Selection of the model, Training of the model, Evaluation of the model and Fine-tuning of the model.* [42]

The obvious advantage of ML is, that this model does not have to be programmed, but are obtained by learning from various data and by using different algorithms. Taulli [42] divides these algorithms into four main classes: supervised, unsupervided, reinforced and semi-supervised learning. Where supervised and unsupervised learning are the commonly used categories for ML.

The main difference between supervised and unsupervised learing is that supervised learning uses data that is labeled by a teacher, which also monitors the learning process and corrects it if needed, while unsupervised learning does not, because the learner is self responsible for its learning concepts as shown by Chowdhary in [8]. Further the author stats, that the teacher can be a human being, software or an environment. For the data labeling, the data firstly needs to be analysed, then categorised and at the same time the quality needs to be measured. Since DF-experts are confronted with huge amounts of data, that are mostly unlabeled, the logical conclusion is to preferly use unsupervised learning algorithms, if possible. But the unstructured data has also to be processed in some kind. The most common approach is clustering, where DL algorithms are used to detect similarities between datasets and create datapattern. Reinforced learning is a method in which a trial and error process is used, which means decisiong are made on either a positive or negative feedback. This approach is also used by well-known algorithms such as depth-first search (DFS), breadth-first search (BFS) and backtracking, which are used to calculate possible moves in chess games, for example. Semi-supervised learning is a mixture of supervised and unsupervised learning, which is used when a small amount of unlabeled data is available in order to convert it into labeled data using DL. The fully labeled data can then be processed directly.

3.2 Deep Learning

Although DL is a relatively new tequnique, which is still being developed and explored, the main focus lies on it if it comes to AI in gerneral and training of AI [41]. DL uses artificial neural networks (ANNs), similar to the human brain, to recognize relationships and pattern between data. These networks are called neural networks because they are orignally inspired by the neuroscience and they basically consist of lots of knodes or neurons, that are connected to eachother and thus form several layers [16]. The first layer is used for the input and the last one is used for the output. Inbetween these two layers can be theoretically numerous other layers, that are called hidden layers. Hidden layers because their output is not visible through the processed data and only shown as final output. Each layer is working independently and is not influenced by the used data, so the algorithm itself has to decide which knodes and layers it uses to calculate the correct output. The input data passes through each, layer where linked functions, which are indicator for the depth of the model, are used for the calculation. Because of that forwarding processing they are also called neuronal feedforward networks. There are several special variations of ANNs, including recurrent neural networks (RNN). These not only process data through a strict forward movement but, as the name suggests, have recursive processes, as nodes are linked to their predecessors. This makes it possible to handle most tasks where a one-to-one mapping is possible, but if this is not the case, as with more complex tasks, the problem cannot yet be solved by deep learning [16].

4 APPLICATION OF AI IN DIGITAL FORENSICS

The automation of computer systems and processes is essential in today's fast-paced world. However, automating a process does not necessarily require the use of AI and vice versa, as they are two independent concepts [23]. Nevertheless, the automation of DF can benefit from the integration of AI and in the following a few of the many possible applications are highlighted. Simple processes such as collecting a lot of similar data are already handled by automated DF tools. The heterogeneity of big data examination slows down forensic experts because it means, e.g., that different tools have to be used, which may not be fully compatible [30]. As a result, dependencies between pieces of evidence are overlooked or can only be recognized with additional effort. As with the process model and techniques of DF, there is no universal solution that applies to all cases when using AI in DF.

4.1 Use cases

AI can pick up where simple automation no longer helps, in other words complex and cognitively demanding processes such as identifying relevant metadata and data artifacts. Use cases appear to be similar, but they can differ considerably in detail. Therefore, depending on the case, a separate model, framework, tool or method is required and must be developed.

Therefore, Al Fahdi et al. [1] conducted a study to investigate the benefits of Self Organizing Maps (SOMs)[2] and Automated Evidence Profiling (AEP) and ultimately found them to be very effective in terms of unsupervised clustering of data fragments. This also makes it possible to create profiles of criminal activities, as depending on the crime, different behavior and more likely certain data can be recognized. These profiles can then be used by intrusion detection systems (IDS) to prevent future attacks. Various AI-based models for incident response have been developed for this purpose.

Hasan et al. [17], created a incident response model, that uses the capabilities of AI. It is based on the approach of integrating previous and occurring case studies and their results into the system. For this purpose, existing systems and methods such as incident response support systems (IRSS), COPLINK[3], model-based reasoning and a decision support system built on case-based reasoning (CBR) were examined and combined to create a model that can collect, identify, sort and analyze critical information supported by AI. The data is stored in databases and through clustering, relationships to previous solved crimes can be created and considered. The proposed model can therefore be used specifically at crime scenes. [17] There are many other approaches for this purpose, for example Rughani's framework [39], which aims to develop intelligent tools. For this reason, ML and AI is used in every step of the DF process to make it more intelligent and thus create smart processes (Smart Acquisition, Smart Analysis and Smart Presentation).

An overview of computational forensics is given by Franke and Srihari [15], where they highlighting the challenges and demands in forensic science on the one hand and giving concrete examples of the integration of algorithms and computational methods on the other hand. Some of the listed application examples are

- handwriting and signature analysis,
- robots used for synthesis of data samples,
- fully automatic computer-based link analysis (used by banks and insurances in examining credit-card fraud and money laundry),
- crime-scene reconstruction using computer graphics,
- human identification (finger print and speech recognition),
- linguistic and
- decision making.

The challenges of DF have already been highlighted and the demands, according to Franke and Srihari, include *"sufficient quality of trace evidence, objective measurement/analysis, robustness & reproducibility, secure against falsification"*. In the following section, we will see that AI fulfills much of the demands in DF.

[2]A SOM is an ANN that maps a high-dimensional input onto a low-dimensional array of nodes, based on their similarities.

[3]COPLINK is a knowledge management system for intelligent analysis and creating connections between information, used by law enforcement.

4.2 Advantages

One of the main arguments in favor of using AI in DF is the cost savings, because every cyber security incident is monetized. This includes both the direct damage caused by the loss of money or the costs associated with a cyber crime, as well as the indirect damage caused by a ruined image. At the very least, the costs for DF experts can be reduced or saved. These may vary between $5,000 and $15,000 for a simple image analysis, but can quickly exceed $100,000 for analysing complexe images or videos [29]. The size of a company and its systems, the amount of data and the number of locations affected also play a role. Depending on the difficulty and complexity, a different merchant and therefore more qualified experts are required, ranging from the low Level 4 to the high Level 1 [13]. The costs are correspondingly higher. An overview of the costs depending on the classification can be seen in Table 1. So, it is worth investing this money upfront in the implementation of AI-supported DF-software, in order to save the costs for personnel and working time [23]. In addition, the readiness of the systems is covered so that an incident can be dealt with at any time for a quicker recovery and enhanced business continuity [27].

Table 1: Overview of investigation cost by complexity [23].

Investigation complexity	Cost
Level 4	$10,0000
Level 2 to 3	$10,0000 to $100,000
Level 1	$100,0000+

Given the time factor, the duration of an investigation is greatly reduced by AI-based methods, as AI works with greater speed and efficiency, which further increases accuracy. Scalability and robustness are further benefits of AI. But how good these methods are and which of the various AI techniques is most suitable needs to be determined in advance. [24] For this reason, several AI techniques were tested and compared on these points in an experiment conducted by Kadage et al. [24]. This resulted in the highest accuracy of 95% when using natural language processing (NLP) for text analysis. Although machine learning and deep learning approaches were only in the middle of the field, they were able to outperform NLP in terms of speed and efficiency with 85%-90%. The winner in all areas, with an average score of 93%, was the Proposed Predictive Analytics based TimeLine Forecasting Analysis (PATF)[4] Approach. Based on these figures, AI-supported systems can be considered reliable and error-resistant.

However, these figures must first be achieved and are based on high-quality data. Digital evidence is often not available in plain text and if there is no way to decrypt it using the key because the data owner is not present or refuses to do so, this evidence cannot be fully used for an intelligent approach. AI can be used here too, in two possible ways: Creating important insights without decrypting the data and trying to perform key retrieval attacks in order to decrypt the data [12]. To get information about the data without

[4]Predictive Analysis & Time Series Forecasting (PATF) uses statistical techniques and ML in order to create models by analysing current and historical data and its characeristics. These models are then used to make predictions about future values and events. [3]

acutally decrypting it, side-channel observations are made. This is done to collect further information about the specific hardware, software, firmware and their behavior that could provide insights into the inaccessible evidence. When trying to obtain the evidence in plain text, template attacks are often used, in which an identical test device is used, which can be customized as desired [7].

In general, this automated investigation of digital evidence is the intersection of DF and biometrics [40]. In order to ultimately draw conclusions about a suspect from the analyzed evidence and solve criminal cases, biometric modalities are used in today's digital forensics, according to Jarrett and Raymond Choo [23]. They also state that through the integration of automation in DF, *"key biometric modalities, including feature extraction, feature capturing, feature matching, and feature robustness, have been introduced"*. As already mentioned, profiles of criminals and criminal activities are often used in DF, for which biometric data is perfectly suited. This can be used to develop automated systems to proactively detect, track and identify criminals [2]. These work on the basis of unique biometric characteristics such as fingerprints, facial features and iris patterns, but soft biometric characteristics such as hair or skin color and body size can also be used for classification [2].

Digital evidence can come in various forms, as modern cyber criminals use a wide range of media types, such as images, mobile phone applications and various computer software. AI can also be used here, as it is predestined to be trained for certain scenarios and there are already suitable automated tools for different media types and use cases. For example SANS SIFT, CrowdStrike CrowdResponse, and Volatility are all forensic tools, that use AI based technology for DF investigations. Another great example are modern-day intrusion detection systems (IDS) and intrusion prevention systems (IPS), which combine automated data collection, regardless of the media type, with live data acquistion and network forensics to analyze and present the collected data as evidence [32]. [23]

4.3 Challenges

In order for the results presented to have legal validity, they must be reliable and every step in the creation of these findings must be traceable. First of all, the accuracy of the AI's mode of operation and therefore the forensic result depends on the quality of the training data. If this deviates or errors occur in the learning process, evidence may be missed. The examiner must also be skilled in recognizing relevant training data and operating the AI tools correctly. Secondly, automatically generated results and their conclusions must be obtained or at least checked by a DF expert for them to be admissible [22]. As previously mentioned, when using intelligent technologies, especially DL and its hidden layers, it is not always clear how and why the AI has come to the result. On top of that, this can be a reason for the untrustworthiness and inadmissibility of results. This raises the question for many: Are we supposed to use a technology that we do not fully understand? This question has an ethical background because if people do not understand something, they are skeptical about it, reject it or, in the worst case, are afraid of it. But not only ethics is a challenge when using AI in DF, legal issues, privacy and data protection must also be considered, as these areas cross over in many points.

4.3.1 Ethics. Ethics in relation to AI is one of the biggest challenges and must be considered from two perspectives [19]. On the one hand, attention must be paid to the appropriate use of AI, how it is trained, what data is used, how the data is processed and what the results are used for. On the other hand, care must be taken to ensure that AI follows the rules of ethics, is not discriminatory and does not have a negative impact on its environment. First of all, the use and processing of personal data is a question of privacy and data protection. This is not only a general challenge of data protection, but also when working with automation technologies. Furthermore, it may not be clear how the data has been processed and incorrect results must not harm anyone. For example, when using automated fingerprint examination and profile matching, no innocent person may be suspected, so the result must be checked manually [18]. However, the use of biometric features harbors further threats, namely that certain groups of people could be discriminated against by external characteristics such as skin color or gender. This would be a violation of the principle that AI should support people and not restrict or even threaten them [33]. The degree to which AI is a help plays an important role here, because existential fears originate from the fact that AI can not only be an extension of human abilities, but could replace them entirely [6]. However, the use of evidence whose origin is not completely traceable or which was even obtained illegally is not only ethically questionable, but also questionable in terms of admissibility in court [38].

4.3.2 Legal issues. The use of AI and the admissibility of evidence in court is subject to clear rules and procedures. However, these do not always correspond to the current state of the technology, as this technology often develops faster than the regulations are adapted. This means that evidence may be inadmissible in court only due to outdated regulations. But also the reliability of a system, which depends on the known margin of error, plays a role here, as does transparency, so that decisions made can be justified. However, it is not only errors that can be caused by AI that need to be taken into account, but also human errors, which can be caused, for example, by prejudices, preferences, personal beliefs and emotional stress. As already mentioned, despite the use of AI, humans have a high influence on the results achieved. [38] DF experts are usually required to know and comply with the law, but even when this is the case, the investigator may exceed certain boundaries out of ignorance or carelessness and endanger the investigation. The legal issues overlap in many ways with privacy and data protection, because in all areas it is important where the data was stored during the investigation. For example, if it was stored on servers hosted abroad, other legal and privacy issues may apply. [34]

4.3.3 Privacy and data protection. Privacy and data protection have not always been as important and clearly regulated as they are today. With the introduction of the General Data Protection Regulation (GDPR)[5] and other data protection regulations, these regulations have been clearly defined. Even though AI and DF are subject to these requirements, they are certainly not always respected, whether intentionally or unintentionally.

[5]The General Data Protection Regulation (GDPR) defines how the personal data of individuals may be processed and transferred.

Table 2: Digital forensics practices and privacy concerns [34].

Digital forensic procedures	Privacy issues
Indiscriminate acquisition/collection of digital data	Third party privacy breach (TPPB) must be avoided
Full disk images are created and analysed	Deleted files can lead to false accusations
Data can be collected from personal devices	Need for informed consents complete and understandable by the users
During the investigation, the data to be acquired may be hosted on servers in different countries	Different jurisdictions can understand privacy differently
Warrants can be necessary during private investigation	Matching of privacy policies and warrants (formally defined) for automated analysis
Correlation is needed in order to build a timeline	Multi-device context (more and more data)
Digital forensics tools and methodologies must be accepted and tested by abroad group of experts in the field	Privacy requirements must be integrated by design in existing tools and methodologies
Digital forensic principles must be guaranteed	The manipulation of data (e.g. encryption) to protect privacy must be done considering digital forensic principles

In order to minimize these violations, privacy impact assessments (PIA) must be conducted. One part of the PIA is the privacy analysis, which lists all functional and technical aspects of a system. This includes general characteristics, such as data systems and data sharing, as well as technical characteristics, such as the observation of individuals and communication via untrusted media. The collection and storage of personal data poses data protection risks and is subject to the GDPR. Should this nevertheless be breached, the data subjects and the competent data protection authority must be informed. [9] A list of some privacy challenges can be seen in Table 2.

5 OUTLOOK AND FUTURE WORK

Although this paper provides an introduction and overview of the topics of DF and AI and research into these areas is progressing steadily, there are still a number of approaches for future research work. With the breakthroughs in research into automation technologies in recent years, artificial intelligence has enjoyed an upswing and the associated public enthusiasm. More and more companies from different industries are integrating artificial intelligence into their processes and systems. It is therefore to be expected that this research will continue to be supported and driven forward. There is no point in trying to prevent progress, so this energy would be better invested in establishing and integrating artificial intelligence. For this to gain further acceptance, the barriers relating to ethics must be overcome through further research in this area. Transparent solutions can help to ease ethical concerns about data protection and privacy [11]. Involving ethics experts in this research could have a positive impact. Because at a certain point, AI could become self-aware and this leads to new, difficult challenges about how such a system should be treated. Research into traditional DF and existing automation should not be excluded. However, in order to cope with the growing threat of cyber attacks and the resulting accumulation of forensic cases, the course should be set for intelligent DF. [23] The Government must take action in this regard, as the integration of AI into DF is supported by a revision of regulations and the promotion of international cooperation [23]. Not least because public and state institutions have also been involved in and affected by cyber attacks.

6 CONCLUSION

The purpose of this literature review was to answer the question: What is the impact of AI used in digital forensics?

Based on the information collected and analyzed from comparable scientific papers, it can be concluded that despite open challenges that need to be addressed, the automation of DF can benefit in many ways from the use of artificial intelligence. The main arguments in favor of this use are the cost reduction of a DF investigation, increase in accuracy, efficiency, scalability and compatibility of DF tools and an expansion of the application areas of DF. Considering the viewed use cases, it can be seen that the main application of AI in DF is aimed at the automated and intelligent collection of information and its analysis in order to establish relationships between the data and other cases. Conclusions can then be drawn from these findings in order to prevent or counteract future incidents. To reach this conclusion, we have also looked at the process of DF using a model consisting of the steps perparation, incident, incident response, physical investigation, digital forensic investigation, presentation and documentation. These serve the purpose of answering the six questions that an investigator asks himself during an investigation. The associated challenges are the approach to integrating AI into DF. Looking at how AI and its subsets ML and DL work, big data can be processed without supervision and intelligence is used to recognize dependencies and patterns between evidence. However, given the challenges of DF and AI, which overlap in many ways, AI cannot yet be fully applied to DF. Additionally, the combination of the two sub-areas brings with it new challenges, which must first be solved in future research in order to achieve full benefit. In addition, continuous research is necessary to meet the constantly changing conditions and new technologies.

REFERENCES

[1] M. Al Fahdi, N. L. Clarke, F. Li, and S. M. Furnell. 2016. A suspect-oriented intelligent and automated computer forensic analysis. *Digital Investigation* 18 (2016), 65–76. DOI: http://dx.doi.org/10.1016/j.diin.2016.08.001

[2] Ali Ismail Awad and Aboul Ella Hassanien. 2014. Impact of Some Biometric Modalities on Forensic Science. In *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, Azah Kamilah Muda, Yun-Huoy Choo, Ajith Abraham, and Sargur N. Srihari (Eds.). Studies in Computational

Intelligence, Vol. 555. Springer International Publishing, Cham, 47–62. DOI: http://dx.doi.org/10.1007/978-3-319-05885-6{_}3

[3] Syed Muzamil Basha, Yang Zhenning, Dharmendra Singh Rajput, Ronnie D. Caytiles, and N. Ch. S.N Iyengar. 2017. Comparative Study on Performance Analysis of Time Series Predictive Models. *International Journal of Grid and Distributed Computing* 10, 8 (2017), 37–48. DOI: http://dx.doi.org/10.14257/ijgdc.2017.10.8.04

[4] Richard Bassett, Linda Bass, and Paul O'Brien. 2006. Computer forensics: An essential ingredient for cyber security. *Journal of Information Science & Technology* 3, 1 (2006).

[5] Nicole Lang Beebe and Jan Guynes Clark. 2005. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation* 2, 2 (2005), 147–167.

[6] Paula Boddington. 2017. Does AI Raise Any Distinctive Ethical Questions? In *Towards a Code of Ethics for Artificial Intelligence*, Paula Boddington (Ed.). Springer International Publishing, Cham, 27–37. DOI: http://dx.doi.org/10.1007/978-3-319-60648-4_3

[7] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. 1999. Template Attacks. In *Cryptographic Hardware and Embedded Systems - CHES 2002*, Gerhard Goos (Ed.). Lecture Notes in Computer Science, Vol. 2523. Springer Berlin Heidelberg, Berlin/Heidelberg, 13–28. DOI: http://dx.doi.org/10.1007/3-540-36400-5_3

[8] K. R. Chowdhary. 2020. *Machine Learning.* Springer India, New Delhi, 375–413. DOI: http://dx.doi.org/10.1007/978-81-322-3972-7_13

[9] James Curzon, Tracy Ann Kosa, Rajen Akalu, and Khalil El-Khatib. 2021. Privacy and Artificial Intelligence. *IEEE Transactions on Artificial Intelligence* 2, 2 (2021), 96–108. DOI: http://dx.doi.org/10.1109/TAI.2021.3088084

[10] Alpana M Desai, David Fitzgerald, and Bogdan Hoanca. 2009. Offering a digital forensics course in Anchorage. *Inform Syst Edu J* 7, 35 (2009).

[11] Lubna Luxmi Dhirani, Noorain Mukhtiar, Bhawani Shankar Chowdhry, and Thomas Newe. 2023. Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors (Basel, Switzerland)* 23, 3 (2023). DOI: http://dx.doi.org/10.3390/s23031151

[12] Xiaoyu Du, Chris Hargreaves, John Sheppard, Felix Anda, Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2020. SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, Melanie Volkamer and Christian Wressnegger (Eds.). ACM, New York, NY, USA, 1–10. DOI: http://dx.doi.org/10.1145/3407023.3407068

[13] David Ellis. 2018. What Does a Cyber Forensic Investigation Do and How Much Does It Cost? SecurityMetrics Inc.. (2018). https://www.securitymetrics.com/blog/what-does-cyber-forensic-investigation-do-and-how-much-does-it-cost

[14] Wolfgang Ertel. 2021. *Grundkurs Künstliche Intelligenz.* Springer Fachmedien Wiesbaden, Wiesbaden. DOI: http://dx.doi.org/10.1007/978-3-658-32075-1

[15] Katrin Franke and Sargur N. Srihari. 2008. Computational Forensics: An Overview. In *Computational forensics*, Sargur N. Srihari and Katrin Franke (Eds.). Lecture Notes in Computer Science, Vol. 5158. Springer, Berlin and Heidleberg, 1–10. DOI: http://dx.doi.org/10.1007/978-3-540-85303-9_1

[16] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. 2018. *Deep Learning. Das umfassende Handbuch: Grundlagen, aktuelle Verfahren und Algorithmen, neue Forschungsansätze.* MITP-Verlags GmbH & Co. KG.

[17] Raza Hasan, Akshyadeep Raghav, Salman Mahmood, and M. Asim Hasan. 2011. Artificial Intelligence Based Model for Incident Response. In *2011 International Conference on Information Management, Innovation Management and Industrial Engineering*. IEEE, 91–93. DOI: http://dx.doi.org/10.1109/ICIII.2011.307

[18] Ido Hefetz. 2023. Mapping AI-ethics' dilemmas in forensic case work: To trust AI or not? *Forensic science international* 350 (2023), 111807. DOI: http://dx.doi.org/10.1016/j.forsciint.2023.111807

[19] Muhammad Hermansyah, Ainun Najib, Any Farida, Rian Sacipto, and Bagus Setya Rintyarna. 2023. Artificial Intelligence and Ethics: Building an Artificial Intelligence System that Ensures Privacy and Social Justice. *International Journal of Science and Society* 5, 1 (2023), 154–168. DOI: http://dx.doi.org/10.54783/ijsoc.v5i1.644

[20] Hiscox. 2023. Anteil der Unternehmen, die in den letzten 12 Monaten eine Cyber-Attacke erlebt haben, in ausgewählten Ländern im Jahr 2023. Statista. Statista GmbH. (2023). https://de.statista.com/statistik/daten/studie/1230157/umfrage/unternehmen-die-in-den-letzten-12-monaten-eine-cyber-attacke-erlebt-haben/

[21] INTERPOL. 2024. Cybercrimes cross borders and evolve rapidly. INTERPOL Website. (2024). https://www.interpol.int/Crimes/Cybercrime

[22] Joshua I. James and Pavel Gladyshev. 2013. Challenges with Automation in Digital Forensic Investigations. (2013). DOI: http://dx.doi.org/10.48550/arXiv.1303.4498

[23] Aaron Jarrett and Kim-Kwang Raymond Choo. 2021. The impact of automation and artificial intelligence on digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science* 3, 6 (2021), e1418.

[24] Anushka Deepak Kadage. 2024. AI-Enhanced Digital Forensics: Automated Techniques for Efficient Investigation and Evidence Collection. *Journal of Electrical Systems* 20, 1s (2024), 211–229. DOI: http://dx.doi.org/10.52783/jes.766

[25] Nickson M. Karie and Hein S. Venter. 2015. Taxonomy of Challenges for Digital Forensics. *Journal of forensic sciences* 60, 4 (2015), 885–893. DOI: http://dx.doi.org/10.1111/1556-4029.12809

[26] Joakim Kävrestad, Marcus Birath, and Nathan Clarke. 2024. *Fundamentals of Digital Forensics.* Springer International Publishing, Cham. DOI: http://dx.doi.org/10.1007/978-3-031-53649-6

[27] Victor R. Kebande, Nickson M. Karie, Kim-Kwang Raymond Choo, and Sadi Alawadi. 2021. Digital forensic readiness intelligence crime repository. *SECURITY AND PRIVACY* 4, 3 (2021). DOI: http://dx.doi.org/10.1002/spy2.151

[28] Michael D Kohn, Mariki M Eloff, and Jan HP Eloff. 2013. Integrated digital forensic process model. *Computers & Security* 38 (2013), 103–115.

[29] Betsy Mikalacki. 2017. WHITE PAPER: How much does Digital Forensic Services Cost? Vestige Ltd.. (2017). https://www.vestigeltd.com/resources/articles/digital-forensic-services-cost-guide-vestige-digital-investigations/

[30] Hussam Mohammed, Nathan Clarke, and Fudong Li. 2016. An Automated Approach for Digital Forensic Analysis of Heterogeneous Big Data. *Journal of Digital Forensics, Security and Law* (2016). DOI: http://dx.doi.org/10.15394/jdfsl.2016.1384

[31] G. Mohay. 2005. Technical challenges and directions for digital forensics. In *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*. IEEE Comput. Soc, 155–161. DOI: http://dx.doi.org/10.1109/SADFE.2005.24

[32] Kara Nance, Brian Hay, and Matt Bishop. 2009. Digital Forensics: Defining a Research Agenda. In *2009 42nd Hawaii International Conference on System Sciences*, Ralph H. Sprague (Ed.). IEEE, Piscataway, NJ, 1–6. DOI: http://dx.doi.org/10.1109/HICSS.2009.160

[33] Rajakishore Nath and Vineet Sahu. 2020. The problem of machine ethics in artificial intelligence. *AI & SOCIETY* 35, 1 (2020), 103–111. DOI: http://dx.doi.org/10.1007/s00146-017-0768-6

[34] Ana Nieto, Ruben Rios, Javier Lopez, Wei Ren, Lizhe Wang, Kim-Kwang Raymond Choo, and Fatos Xhafa. 2019. Privacy-aware digital forensics. In *Security and Privacy for Big Data, Cloud Computing and Applications*, Wei Ren, Lizhe Wang, Kim-Kwang Raymond Choo, and Fatos Xhafa (Eds.). Institution of Engineering and Technology, 157–195. DOI: http://dx.doi.org/10.1049/PBPC028E{_}ch8

[35] FEDERAL BUREAU of INVESTIGATION (FBI). 2023. FEDERAL BUREAU of INVESTIGATION Internet Crime Report 2023. Internet Crime Complaint Center (IC3). (2023). https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[36] Gary Palmer and others. 2001. A road map for digital forensic research. In *First digital forensic research workshop, utica, new york*. 27–30.

[37] Mark M Pollitt. 2001. Report on digital evidence. In *13th INTERPOL Forensic Science Symposium*. Citeseer.

[38] Brighi Raffaella, Michele Ferrazzano, and Leonardo Summa. 2020. Legal Issues in AI Forensics: Understanding the Importance of Humanware. *Proceedings of the International Workshop on Applications of AI to Forensics 2020 (AI2Forensics 2020)* (2020), 13–20.

[39] Parag H. Rughani. 2017. ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK. *International Journal of Advanced Research in Computer Science* 8, 8 (2017), 10–14. DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4571

[40] Sargur N. Srihari, Chen Huang, Harish Srinivasan, and Vivek Shah. 2007. Biometric and Forensic Aspects of Digital Document Processing. In *Digital document processing*, Bidyut Baran Chaudhuri and Bidyut B. Chaudhuri (Eds.). Springer, London, 379–405. DOI: http://dx.doi.org/10.1007/978-1-84628-726-8{_}17

[41] Tom Taulli. 2022. *Deep Learning.* Springer Berlin Heidelberg, Berlin, Heidelberg, 79–102. DOI: http://dx.doi.org/10.1007/978-3-662-66283-0_4

[42] Tom Taulli. 2022. *Maschinelles Lernen.* Springer Berlin Heidelberg, Berlin, Heidelberg, 45–77. DOI: http://dx.doi.org/10.1007/978-3-662-66283-0_3