AI IN DIGITAL FORENSICS

Liam Maher

I. INTRODUCTION

In today's technological landscape, both Artificial Intelligence (AI) and digital forensics are rapidly evolving fields. AI refers to the production of programs and machines that can mimic, and eventually surpass, human intelligence; this allows for complex problem-solving, data analysis, and day-to-day processes to be automated or improved. On the other hand, digital forensics refers to the process of recovering, analyzing, and preserving digital evidence, while following certain procedures and protocols so that the evidence can be used in legal proceedings if needed.

The integration of AI into digital forensics can greatly streamline and enhance the investigative process. In the past, investigators dealt with relatively small amounts of data, but today's cybercriminals can store and manipulate several terabytes of information, presenting a massive challenge for forensics teams. AI offers a solution to this by automating data analysis, rapidly sifting through large quantities of evidence, and identifying patterns within the data. The use of AI in digital forensics allows forensic teams to focus more on the critical insights from the data as it makes the processes faster and more efficient.

II. HISTORY AND EVOLUTION

The concept of digital forensics began as early as the late 1970's, when personal computers started to become more common and law enforcement noticed the potential for computers to be used in criminal activities. It was not until the early 1980's where the importance of handling digital evidence in criminal investigations was fully realized and acted upon. According to Carrie Whitcomb, the Director of the National Center for Forensic Science, "As early as 1984, the FBI Laboratory and other law enforcement agencies began developing programs to examine computer evidence" [1]. As personal computers and digital evidence became more prominent, formal methodologies and tools began to emerge, particularly in response to the increasing complexity of cybercrimes. One of the pivotal developments with regards to digital forensics was the establishment of the Computer Analysis and Response Team (CART) by the FBI, which then influenced other law enforcement agencies to develop similar organizations and groups [1]. By 1995, the United States Secret Service conducted a survey finding that "48 percent of the agencies had computer forensic laboratories and that 68 percent of the computer evidence seized was forwarded to the experts in those laboratories" [1].

By the late 1990's and early 2000's, the need for more complex forensics tools and practices became clear. After the events of September 11, 2001, the importance and funding for digital forensic investigation increased in dramatic proportions, with the hopes of having better capabilities to combat terroristic and criminal attacks [2]. According to Mark Pollitt, former FBI agent and Director of the Regional Computer Forensic Laboratory Program, this led to an evolution of forensic tools, "The first of the new tools was Expert Witness, a product designed by Andy

Rosen for Macintosh forensics that evolved to EnCase. EnCase, along with Forensic ToolKit (FTK), became commercial successes and are now standard forensic tools" [2].

Since then, forensic tools and processes have continued to evolve to meet new technologies and the criminal processes that follow with them. AI has become an increasingly pivotal tool in addressing the complexity and scale of various digital crimes. Initially, digital forensics relied on many manual processes for recovering files, analyzing logs, and more. However, with the rise of data volume and increased sophistication to cybercrimes, the need for automation of processes and analysis became apparent.

Today, AI is integrated into many different forensic tools for the use of automating processes. Forensic tools that incorporate AI can help forensic teams to detect fraudulent activity, recover corrupted or deleted files, and also identify certain images that may contain illegal content. With the popularity and resources devoted to the fields of Artificial Intelligence and Machine Learning today, we are seeing an increase in forensic tools utilizing these AI abilities to facilitate tasks.

III. Current Applications of AI in Digital Forensics

AI has played an evolutionary role in the field of digital forensics by automating once manual and time-consuming processes. This integration of AI has enhanced efficiency, accuracy, and the overall speed of forensic investigations. There are several specific applications of AI in digital forensics that are currently making a significant impact. In this paper, we will be discussing three of these applications: image and video analysis, malware detection, and data recovery.

I. IMAGE AND VIDEO ANALYSIS

AI has become an essential tool in the process of analyzing images and videos in digital forensics. Forensic investigators often have to search through many gigabytes, sometimes even terabytes, of multimedia data that must be carefully analyzed for evidence related to the alleged crimes. AI and deep-learning technologies can automate this process by recognizing faces, identifying objects, and detecting content that has been altered, such as deepfakes. These models are trained on a large amount of content, which can significantly reduce the amount of time it takes for the forensic investigator to find relevant evidence. For example, AI features, such as those in Magnet AXIOM, "Automatically detect potential pictures of illicit content like child abuse, drugs, and weapons with machine learning tools" [3]. Furthermore, the use of deepfakes have significantly increased recently, with Magnet Forensics stating that there were "an estimated 500,000 video and voice deepfakes shared on social media in 2023". Deepfakes in digital forensics can cause a multitude of problems when trying to supply evidence in legal proceedings. With recent AI developments, such as those in Magnet AXIOM, being able to identify deepfakes has become a much easier task for forensic investigators.

The usage of AI in the digital forensic process for analyzing images and videos presents many advantages, as well as limitations. As for advantages, AI tools, such as those in Magnet AXIOM, can significantly help speed up the process of searching for evidence related to a multitude of cybercrimes. This rapid processing of data can save time for the forensic investigators, as well as helping to collect evidence in a more efficient manner if the prosecuting party needs information within a narrow timeline. However, these advantages also bring fourth limitations and hesitations for its usage. Deep learning requires a very large and

diverse dataset in order to correctly identify people and objects. If a model is not trained on enough data, there is the potential that it will misidentify or not identify a piece of evidence that could be value to the investigation. If the forensic investigators do not manually look through the evidence at all when utilizing AI tools, they run the risk of not identifying valuable evidence.

II. Malware Detection

AI is currently playing a crucial role in digital forensics through malware detection. Traditional methods for malware detection can allow for new and zero-day threats to remain undetected. AI powered tools, such as those used in software like Malwarebytes, utilize machine learning techniques to identify suspicious behaviors and patterns. This incorporation of AI and machine learning into the tool helps to identify zero-day threats that an investigator might have overlooked [4]. Not only can AI help to detect zero-day threats and attacks that have not yet been researched, in the case of Malwarebytes, it does not require "any human interaction to correctly identify malware" [4].

AI usage in malware detection presents many advantages, but also comes with limitations that must be discussed. As for advantages, AI can facilitate the process of detecting zero-day threats, reducing the reliance on comparing suspected malware with previously known instances. Due to malware detection AI tools such as Malwarebytes analyzing behavioral patterns instead of predefined malware signatures, it allows for a much more accurate and faster detection of zero-day attacks. However, such tools come with similar limitations to AI tools for image and video analysis. If a model is not trained on enough data, it can lead to errors in detecting malware, thus leaving the attack undetected. Furthermore, if cybercriminals

are able to obtain the data that the model is trained on, they could possibly design malware that will go undetected by the system, leaving the model open to vulnerabilities.

III. Data Recovery and Analysis

AI has made significant strides in improving data recovery and analysis in digital forensics. Traditional methods of data recovery and analysis often struggled with data fragmentation or corruption. Convolutional Neural Networks (CNNs) have shown promising results in recovering lost image and video data. Recurrent Neural Networks (RNNs), are showing similar results in recovering text and time series data, by learning the dependencies and contexts, which can help forensic investigators to reconstruct incomplete sequences [5].

Moreover, AI is also being used to facilitate the analysis of large data sets, using Generative Adversarial Networks (GANs). The algorithms being used with the GANs can provide the forensic investigators with meaningful insights about the data being recovered. One such example is that the AI can sort and categorize the data into different groups, allowing the investigators to focus only on the group that is required for the investigation.

AI usage for the purpose of data recovery and analysis presents many advantages to the forensic investigators, but it also comes with many limitations. As for advantages, AI enables a much faster recovery process, while reducing human error withing the recovery steps. Another advantage is in the categorization of large data sets, which reduces the analysis time for forensic investigators significantly. However, there are also many concerns and limitations with regards to AI usage in data recovery and analysis. One such limitation is that of reliability and interpretability. When utilizing AI tools, it is common for them to draw different conclusions each time you use them, even if it is within the same data set. This runs

the risk of missing certain data that might have been valuable to recover, as well as categorizing data in an incorrect manner. These concerns must be addressed in order for the tools to be widely utilized and accepted by forensic investigators, as well as for the findings of these tools to be accepted in a legal proceeding.

IV. AI-Driven Forensic Tool Case Study: Magnet AXIOM

Magnet AXIOM is a widely used digital forensics tool developed by Magnet Forensics. AXIOM integrates AI capabilities to facilitate the process of recovering and analyzing digital evidence from various sources including mobile devices, computers, and cloud environments. The tool uses machine learning algorithms to automate several parts of the forensic investigation. This capability allows investigators to rapidly filter through large volumes of data, reducing the workload on the investigator while also improving efficiency.

According to Magnet AXIOM's official documentation, Magnet.AI can detect specific categories of images, such as handwriting, hate symbols, weapons, and more. Magnet.AI also can compare images that are imbedded into other files, such as .doc files [6]. Another key feature of Magnet.AI picture comparison, where you can identify similar objects across different photos, as well as identify photos taken in the same room or location. AXIOM also can incorporate Thorn AI for image comparison and categorization. Thorn AI is a tool that is free-of-charge for law enforcement agencies to help identify images that can contain sensitive content of child pornography or child abuse [6].

Magnet AXIOM provides numerous benefits to forensic investigators, particularly law enforcement agencies. The use of Magnet.AI within AXIOM provides automation for typically labor intensive tasks, such as image comparison and categorization. Furthermore, the use of Thorn AI within AXIOM can help investigators to accurately and efficiently identify child pornography and child abuse evidence, which are two cases where timely recovery of data is essential for the welfare of the children. However, as stated in the official documentation for Magnet AXIOM, Magnet.AI and Thorn AI are very resource intensive [6]. If the forensic investigators do not have GPU's that can be utilized while running the AI, it can take a very long time for the analysis to complete. It is also worthy to note that the benefits of both Magnet.AI and Thorn AI are both dependent on the quality of their training data.

V. Ethical Implications

While the integration of AI into digital forensic investigations can offer numerous advantages, there are many ethical concerns that must be addressed first. The three main categories for concern in this area would be the accuracy of the forensic investigations, the potential for biases, as well as privacy concerns.

In the topic of AI in digital forensics, the first ethical concern to be raised is the accuracy of the investigation when using AI to extract, analyze, or categorize the data. When it comes to AI and deep learning models, they depend almost entirely on the data they were trained on. If a model is trained on poor or incorrect data, it could lead to faulty answers being provided. In criminal investigations, the room for error is little-to-none, and if the AI model misses an important piece of evidence, or is somehow able to distort the evidence, this could lead to a suspect being wrongfully convicted or acquitted. For this reason, it is imperative that forensic investigators

manually review the results from the AI program. It is also very important for the forensic investigators to check the entirety of the data that was uploaded into the AI program to ensure no evidence was missed.

Another ethical concern with regards to AI in digital forensics is that of biases in the data. As mentioned before, the AI models and their accuracy depend greatly on the data in which they are trained. AI algorithms are prone to picking up biases within the training data, which could affect their results in a forensic analysis. Biases in these tools can lead to disproportional and unfair treatment to certain demographics. It is crucial to identify and prevent these biases in AI systems in order for them to be accurate and unbiased when aiding in forensic investigations.

Perhaps the most prominent ethical concern when it comes to AI and digital forensics is the lack of privacy that comes with it. AI tools can process a large amount of data, much more than a human could process in the timeline of an investigation. This can lead to AI tools potentially knowing sensitive information about people, even those who were just victims in a cybercrime. Additionally, the content of which the AI tools are trained on is also of concern. For example, in the case of Thorn AI, many ethical questions are raised because in order to identify child pornography, it is reasonable to assume that it has been trained on a lot of data from within that category. This raises the following questions: Who saw the data? Where did the data come from? Were the victims in the data notified that their personal photos were being used? Although Thorn AI, and other AI technologies like it, are being used for ethically and morally right purposes, it is important to take into consideration the ethical concerns related to their creation.

VI. Future Of AI in Digital Forensics

As with most technology, we can almost guarantee that the future will hold advancements to the AI tools used in digital forensics. One key area of development is the use of real-time AI-driven forensics, where AI models will be able to analyze the data immediately when it is being collected. This advancement would lead to even faster turnaround time for digital forensic investigations.

The ability for AI to process large datasets will also increase, as the data contained in cloud services, mobile devices, and computers continues to grow. This will occur concurrently with the technological advancements in computing power and special GPU's and CPU's designed specifically for running AI algorithms. This increase in computing power will not only allow the AI tools to handle more data, but also to be more efficient in the categorization and analysis of smaller data sets. Furthermore, AI tools in digital forensics will become even more accurate in identifying, analyzing, and categorizing data. As time goes on, and the AI tools are fed more information, they will be able to more accurately identify and categorize different types of digital evidence.

As with all technology that is trying to combat crime, there are sure to be countermeasures, as well as new methodologies created by criminals in order to hinder the efficacy of AI tools in digital forensics. Although it may be too early to speculate, an increasing ease of analyzing digital evidence could lead to criminals reverting to physical copies of illicit material to avoid the potential risks of keeping it in digital format. Another concern that must be raised is that of leaving hidden commands in data to throw off the AI, as well as tampering with the training material, to make the AI tools ineffective. One example of this happening with current AI models is teachers using hidden white text in their homework and test questions. When a student goes to copy a problem

and put it into a model such as Chat GPT, the white text is not seen and has a phrase like “include ‘unicorn’ in your response”. If the teacher notices the word “unicorn” in the answer, they know that the student used an AI model to complete the assignment. Criminals could potential use methodologies like this to tell the AI to not show a specific file in their report. This is an issue that must be addressed in order for AI to be effectively used in digital forensic investigations.

VII. Conclusion

The integration of Artificial Intelligence into the field of digital forensics marks a significant advancement in the efficiency and accuracy of forensic investigations. AI’s ability to handle large datasets, automate time-consuming tasks, and detect patterns in digital evidence provides crucial support to forensic investigators. In applications such as image and video analysis, malware detection, and data recovery, AI has transformed how forensic teams process and analyze evidence.

However, the implementation of AI in digital forensics is not without its challenges. Ethical concerns such as bias in models, potential for errors, and privacy issues must be addressed to ensure the technology is being used responsibly. As forensic investigations increasingly rely on AI, it is essential that transparency, accountability, and fairness are prioritized, and that investigators continue to review and validate AI-generated results.

AI has the potential to revolutionize the field of digital forensics, but its successful implementation will depend on addressing technical, ethical, and legal challenges that accompany its use. As these challenges are met, AI-driven digital forensics will play an increasingly critical role in maintaining the integrity and effectiveness of forensic investigations.

REFERENCES*

[1] C. M. Whitcomb, "An Historical Perspective of Digital Evidence: A Forensic Scientist's View," *International Journal of Digital Evidence*, vol. 1, no. 1, Spring 2002. [Online]. Available: https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf. [Accessed: 22-Sep-2024].

[2] M. Pollitt, "A History of Digital Forensics," in *Advances in Digital Forensics VI*, 2010. Available: https://dl.ifip.org/db/conf/ifip11-9/df2010/Pollitt10.pdf. [Accessed: 22-Sep-2024]

[3] "Magnet AXIOM: Digital Investigation Software," Magnet Forensics. [Online]. Available: https://www.magnetforensics.com/products/magnet-axiom/. [Accessed: 22-Sep-2024].

[4] "Malwarebytes Detects Unknown Threats as Zero-Day Malware," Malwarebytes, [Online]. Available: https://www.malwarebytes.com/blog/detections/malware-ai. [Accessed: 22-Sep-2024].

[5] A. Singh, A. Joshi, M. S. Sankhla, K. Saini, and S. K. Choudhary, "AI in Data Recovery and Data Analysis," in *Artificial Intelligence in Forensic Science*, 1st ed., CRC Press, 2024, p. 23.

[6] Magnet Forensics, *Magnet.AI Picture Categorization and Comparison*, Magnet Forensics Documentation, 2024. [Online]. Available: https://www.magnetforensics.com/products/magnet-axiom/. [Accessed: 22-Sep-2024].

*Word will not allow for the changed formatting of the citations, each tab is supposed to be a space