Mobile Forensics and Digital Solutions:
Current status, challenges and future directions

Nikolaos Papadoudis
Hellenic Police Forensic Science Division & Department of Computer Science and Engineering, European University Cyprus[1]

Alexandros Vasilaras
Ilias Panagiotopoulos
Hellenic Police Forensic Science Division.
Department of Informatics and Telematics, Harokopio University of Athens

Panagiotis Rizomiliotis
Department of Informatics and Telematics, Harokopio University of Athens

Abstract
Mobile devices have become an indispensable part of modern society and are used throughout the world on a daily basis. The proliferation of such devices has rendered them a crucial part of criminal investigations and has led to the rapid advancement of the scientific field of Mobile Forensics. The forensic examination of mobile devices provides essential information for authorities in the investigation of cases and their relative importance advances as more evidence and traces of criminal activity can be acquired through the analysis of the corresponding forensic artifacts. Data related to the device user, call logs, text messages, contacts, image and video files, notes, communication records, networking activity and application related data, among others, with correct technical interpretation and correlation through expert analysis, can significantly contribute to the successful completion of digital criminal investigations. The above underline the necessity for advanced forensic tools that will utilize the most prominent achievements in Data Science. In this paper, the current status of Mobile Forensics as a branch of Digital Forensics is examined by exploring the most important challenges that digital forensic examiners face and investigating whether Artificial Intelligence and Machine Learning solutions can revolutionize the daily practice with respect to digital forensics investigations. The utilization of these emerging technologies provides crucial tools and enhances the professional expertise of digital forensic scientists, paving the way to overcome the critical challenges of digital criminal investigations.

Keywords: Mobile Forensics, Artificial Intelligence, Big Data, Forensic Science, Digital Forensics.

1 Corresponding author, email Address: nikos.papadoudis@gmail.com

Introduction

Mobile Forensics is the field of Digital Forensics that deals with the acquisition, examination and analysis of mobile devices, in order to recover digital evidence in a forensically sound manner, respecting the chain of custody and ensuring that they will be admissible in a court of law. The term "mobile devices" is usually used to refer to mobile phones, but in reality, it can be extended to include any digital device which can store data in local memory and act as a means of communication. Therefore, Mobile Forensics is also related to the acquisition, examination and analysis of tablet computers, GPS devices and Personal Digital Assistants (PDAs).

Mobile devices contain plenty of data in a digital format, which includes, but is not limited to, call logs, messages, contacts, pictures, videos, web browsing information and location data. Mobile devices play a very critical role in criminal investigations, and therefore, there is an increasing demand for reliable software and hardware tools to assist digital forensics investigators in their efforts.

In recent years there has been an increasing interest in mobile devices, due to their expanding capabilities, the multiple benefits they provide in personal and professional communication, the ability to transmit and access information quickly, as well as recent developments, such as access to online banking. The advancements in mobile technology in combination with the acceptance and widespread adoption of mobile devices by the community have led to a significant rise in mobile forensics cases. The digital forensics market is expected to grow from $4.62B in 2017 to $9.68B by 2022, an annual compound growth rate of almost 16%. The anticipated market drivers are government regulations, increasing cyber incidents experienced by businesses, and the rapidly growing presence of Internet of Things (IoT) applications and devices.[2]

Artificial Intelligence (AI) already has several applications in mobile devices, such as smart voice assistants, smart cameras, facial recognition for security purposes, improved graphics in augmented reality applications, improved search functions and power efficiency. The utilization of AI algorithms has significant benefits in general towards automation in the analysis of digital evidence. According to Homem, I. (2018), a pilot study has demonstrated how automation can be advanced in digital forensics in identifying and acquiring forensic evidence, as well as in the phase of forensic analysis.

Another study related to the subject by Mohammed, Clarke and Li (2016) focused on an automation-based approach for Big Data analysis regarding specifically digital forensic investigation. Jarrett and Choo (2021) proposed the term Intelligent Automation in their research on the impact of automation and AI in digital forensics. They concluded that Intelligent Automation can provide cost-reduction, improved efficiency and speed of forensic investigation, more accurate data and information processing, and increased probability of solving a higher number of cases in limited amounts of time.

Following the above research efforts, the present study aims to explore the current applications of AI in Mobile Forensics and the corresponding solutions it provides to the challenges that investigators face, as well as indicating particularly useful AI research topics that would benefit the field in the long term.

Regarding the structure of the paper, section 2 provides an examination of the current status of mobile forensics as a subfield of digital forensics and the associations with cloud forensics, network forensics and the domain of IoT. Section 3 inspects the most important challenges that mobile forensics investigators face in the examination of cases, whereas section 4 presents AI tools and solutions available at the present time for mobile forensic investigations in conjunction with legal issues related to their practice in Digital Forensics, as well as an overview of the main evaluation metrics for AI classification models. Finally, conclusions and recommendations for future work are presented in Section 5.

Mobile Investigations and Digital Forensics

Links between mobile investigations and Digital Forensics field

Digital forensics has grown rapidly due in part to the increase in mobile devices (Harrill & Mislan, 2007). Forensic investigators face numerous challenges dealing with digital evidence obtained from mobile devices,

2 Market Insider, Digital Forensics Market – Global Forecast to 2022, (16 March 2018)
Available at "https://markets.businessinsider.com/news/stocks/digital-forensics-market-global-forecast-to-2022-1018885400"

which are correlated with several other branches of the field, such as Computer Forensics, IoT Forensics, Cloud Forensics and Big Data Forensics. The efforts to examine mobile devices originated from traditional digital forensic techniques, but, along the way, new, specialist tools, commercial and open-source, have been developed to provide solutions and automation in the extraction, examination and analysis of mobile device data.

In the modern world of competition new mobile device manufacturers are coming into the market every day with the same operating system but with their own variations, in their implementation, resulting in a myriad of file system and structural permutations (Roy, Khanna & Aneja, 2016). Meanwhile, mobile devices receive data from many sources, such as computers, cloud servers, social media platforms, network components, drones, smart vehicles, wireless cameras and smart home devices, as illustrated in Figure 1, while new technologies come into existence and are integrated into this diverse ecosystem with the progression of science and industry.

Figure 1. Mobile Phones and Data Sources

Cloud Computing

Mobile cloud computing uses cloud computing to deliver applications to mobile devices[3] and bring rich computational resources to mobile users, network operators, as well as cloud computing providers (Khan et al. 2014). The technology offers many advantages to mobile device users, such as flexibility in the transmission of information and the creation of applications, device and location independence, resource sharing among multiple users which results in increased productivity, as well as easier maintenance and advanced security. With regards to mobile forensic investigations, cloud computing provides large amounts of data that can be utilized by examiners to discover valuable artifacts for criminal cases.

In a study done by IDC, it is expected that by 2025 we will have more than 175 zettabytes of data (Reinsel, Gantz & Rydning, 2017). In addition to the ever-increasing need for data storage services, the availability of high-capacity networks, low-cost computers and storage devices, as well as the widespread adoption

3 https://www.ibm.com/cloud/learn/what-is-mobile-cloud-computing.

of hardware virtualization, service-oriented architecture and autonomic and utility computing has led to growth in cloud computing (Soric, 2021).

According to Forbes Contributor Louis Columbus (2014), a key point from an IBM study was that "Cloud computing has rapidly accelerated from 30% of Chief Information Officers (CIOs) mentioning it as a crucial technology for customer engagement in 2009 to 64% in 2014".

Other than the three standard models of cloud computing, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)[4], a relatively recent model in cloud computing is the Mobile backend as a Service model (MBaaS). This model provides web app and mobile app developers with a way to link their applications to cloud storage and cloud computing services[5]. Trends indicate that these services are gaining significant mainstream traction with enterprise consumers (Boyd, 2014). Taking into consideration the afore-mentioned models of Cloud Computing, we can understand that it is closely related to mobile technology and therefore the advancements in the field are of great interest to forensic investigators.

Internet of Things

The Internet of Things (IoT) describes the network of physical objects that are embedded with sensors, software and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet (Boyd, 2014). It is particularly important for mobile forensic examiners, as IoT devices generate high-quality artifacts that can be critical to the outcome of mobile forensic examinations and serve as important evidence in a court of law.

Internet of Things includes multiple different categories, such as Wireless Sensor Networks, use of mobile phones to interact with the real world (e.g. sensing), devices that connect via Bluetooth enabled mobile phones to the Internet, connected homes & connected Cars, RFID enabled tracking, low power embedded systems and Internet-connected wearables[6]. IoT utilizes many connectivity methods and technologies, the most important of which are presented in Figure 2 below:

Figure 2. IoT Connectivity Methods and Technologies

Wireless 101	RF 101	ZigBee PRO, ZigBee 3.0 and ZigBee IP	6LowPAN	RFID	Bluetooth LE or Bluetooth Smart Technology
Z-Wave	Home Automation (HA) Profile	Smart Energy (SE) Profile	Health Care	IEEE 802.15.4, IEEE 802.15.4e, 802.11ah	802.11ah,Wi-Fi HaLow
Relay Access Point (AP)	Grouping of stations	Target Wake Time (TWT)	Speed Frame Exchange	Sectorization	GSM, CDMA, GPRS, 3G, LTE, small cells, SATCOM
Sensors and sensor networks	Serial communication	Power consumption and optimization	MIPI, M-PHY, UniPro, SPMI, BIF, SuperSpeed USB Inter-Chip (SSIC), and SPI	Mobile PCIe (M-PCIe)	Wired connectivity
IPv4/IPv6 • Ethernet/ GigE	Real-time systems and embedded software	Big data	Analytics	Cloud computing and storage	Augmented Reality

4 The NIST Definition of Cloud Computing, SP800-145, September 2011.

5 https://en.wikipedia.org/wiki/Cloud_computing#Mobile_%22backend%22_as_a_service_(MBaaS)

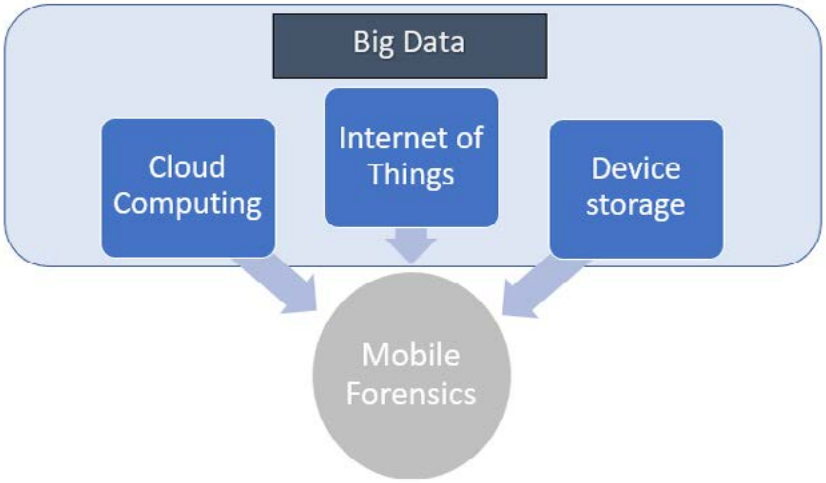
6 See IoT Forensics, eForensics Magazine 2019, 8 (6), p. 37.

Through the usage of these technologies, the IoT environment is deeply interconnected with smartphones and the respective applications, which are used for communication between devices and transmission of data. Besides, the IoT's major significant trend in recent years is the explosive growth of devices connected and controlled by the Internet (Nordrum, 2016). By the definition of the IoT ecosystem, as well as the respective connectivity methods and technologies involved, we can infer that the Internet of Things is deeply connected to recent technology advancements and that, alongside Cloud Computing and Storage, it is of particular importance for the field of Mobile Forensics.

Big Data

Due to the conjunction of Big Data with Information Technology, Cloud computing and the IoT ecosystem, it is a particularly important research subject in the domain of Digital Forensics. Big data sets come with algorithmic challenges that previously did not exist. Hence, there is seen by some to be a need to fundamentally change the processing ways (Sejdić, 2014). In addition, the ability of Internet of Things devices to gather sensory data and utilize them in everyday activities in modern society, along with the fact that data extracted from these devices reveal the device inter-connectivity, suggests that further exploring Artificial Intelligence and Big Data principles in the context of Internet of Things forensics could provide significant solutions to many challenges in the field of Mobile Forensics and Digital Forensics in general. A representation of the correlations indicated above is provided in Figure 3.

Figure 3. Big Data correlations with Mobile Forensic Investigations



Mobile devices play a key role as a terminal point of computer communication systems, collecting data from a variety of different sources and exist as most significant factors in criminal investigations. From the analysis of the current status of Mobile Forensics, we can conclude that it is affiliated with all aspects of Digital Forensics, most notably with Cloud Forensics, IoT and Big Data Forensics.

Issues in Mobile Forensics

Mobile forensics incorporates many different, but inherently interconnected, sub-branches of modern science. Forensic specialists need to navigate into this multidisciplinary field and make use of effective and efficient modern techniques to successfully combat ever more sophisticated crime. While the number and individual importance of challenges that mobile forensic experts face on a daily basis, may vary, there are some issues that every professional in the field has come across to a certain degree. The most important ones from a practitioner's perspective are analyzed below.

Volume of data

The volume of data and complexity of investigation are among the major issues in Mobile Forensics (Alzaabi, Jones & Martin, 2013). Gartner Glossary defines big data as high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation[7]. Big Data requires a new generation of technologies and architectures, designed to efficiently extract value from very large volumes of a wide variety of data, by enabling high-velocity capture, discovery and/or analysis (Gantz & Reinsel, 2011).

Therefore, one of the main characteristics of Big Data is Volume, which refers to the amount of data that is available for processing. If the size of data is sufficiently large, then it can be considered as Big Data. Even though in most cases the concept is approximate and relative to many factors, such as computing power and available technology, the effects on mobile investigations have become apparent in recent years.

In the context of mobile forensics, the meaning and value of the data volume to be examined and analyzed is inherently interconnected to the requirement for fast, efficient procedures and techniques, as well as accurate and concrete results. Hence the solutions to this problem need to account for the legal timeframes and the information flow in a criminal investigation.

Cloud services further exacerbate this challenge for forensic investigators, as there are multiple issues created by the widespread adoption of this technology, such as the rapidly increasing storage space available and the sheer amount of data transmissions for mobile device users. Other relevant factors contributing to the issue are preserving the chain of custody, resolving jurisdiction problems, overriding encryption technologies, the lack of log framework for many Cloud Service Providers, as well as the lack of cloud specific forensic tools.

Variety and variability of data

Big Data examination incorporates both structured and unstructured data processing, which are fundamental to the case analysis by the digital evidence examiner. When discussing structured data, it is usually referred to data that has a defined known structure. This could be numbers, dates, groups of words or strings accessed within the storage medium. It is data regularly tapped into during an investigation and generally stored in database files[8].

Unstructured data is information that either does not have a pre-defined data model or cannot be structured in an orderly fashion (such as in ordered rows and columns as found in databases). Unstructured data can include text in all forms, emails, video, audio files, web pages and social media.

One of the main contributors to the variety and variability of data in mobile forensic investigations is the IoT ecosystem. IoT devices can be an important source of artefacts for forensic investigations, but they pose several challenges for forensic examiners. The most important ones are data storage, data format, the diversity of IoT devices, as well as the support for these devices by current digital evidence software.

Collection, examination and analysis of data in an IoT environment becomes difficult as some of the device data is stored on the provider's cloud platforms, which may also be located in another country. Accessing the data for an investigation can be an issue if the cloud stored data is in another jurisdiction, privacy issues are not carefully considered, and maybe subject to security measures (Quick & Choo, 2018), which aggravates the complexity of an investigation, in combination with the ever-expanding storage space size.

Furthermore, within the IoT environment, evidence can be extracted from sensors and appliances, of which most of the data can be unstructured. To add to that, proprietary data formats, protocols, and physical interfaces all complicate the process of evidence extraction (Miorandi et al., 2012). The variety of data formats also makes it difficult to define a standardized approach to extracting and analyzing, as some devices may require specific approaches.

Then there is a challenge that evidence needs to be extracted from a wide range of IoT devices, such as smart refrigerators, smart watches and wireless cameras. In their study, Yaqoob et al. (2019) consider various broad groupings of IoT devices with a view to constructing an IoT digital forensics taxonomy. Their groupings are

7 https://www.gartner.com/en/information-technology/glossary/big-data

8 https://www.msab.com/blog/big-data-in-digital-forensics-the-challenges-impact-and-solutions/

smart home, smart vehicles, smartphones, drones, BitTorrent Sync peer-to-peer cloud storage service, and general IoT systems. They then go onto elucidate the taxonomy: 1) forensics phases, 2) enablers, 3) networks, 4) sources of evidence, 5) investigation modes, 6) forensics models, 7) forensics layers, 8) forensics tools, and 9) forensics data processing.

Extracting information from these devices becomes challenging as various manufacturers use different software platforms, operating systems, and hardware, leading to variation in file format of the devices. Thus, proper retrieval of artefacts from the storage devices still remains a challenge. Additionally, digital forensics tools and technologies are meant for conventional computing and are incapable of fitting forensic analysis within the IoT environment.

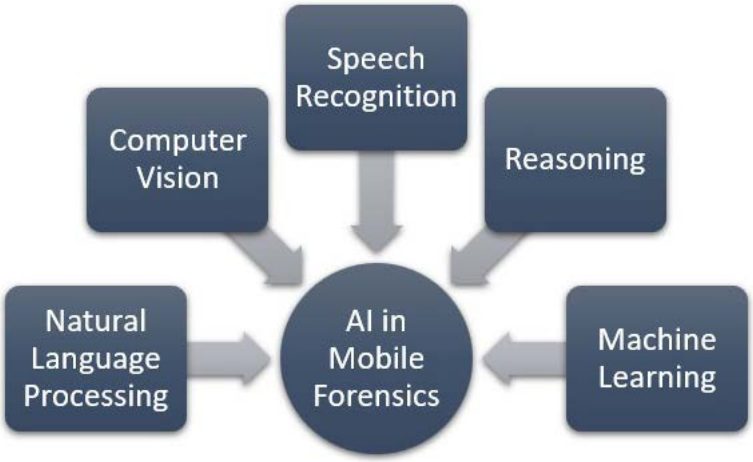
The challenges detailed in this section are derived from fields directly correlated with mobile forensics and significantly affect the work of forensic experts. While these issues became apparent with the conception of the corresponding branches of Digital Forensics, the evolution of mobile phones and the rapid advancements in related cutting-edge technology make the discussion over possible solutions more relevant than ever before. The following section features the tools that Artificial Intelligence provides us with to address these challenges and explore the current status of the AI related technologies in the field of mobile forensics.

Mobile Forensics and AI Solutions

Current tools

Artificial Intelligence has the potential for providing the necessary expertise and helps in the standardization, management and exchange of a large amount of data, information and knowledge in the forensic domain[9]. In the process of addressing the most important issues that we have examined, in the context of Big Data and the associated fields and domains of Forensic Science, AI could provide significant, efficient and effective solutions. Important Artificial Intelligence domains that are utilized in Mobile Forensic investigations are depicted in Figure 4 below.

Figure 4. Artificial Intelligence Domains in Mobile Forensics



Applications of AI in the Digital Forensics domain have already been present in research, such as the use of MADIK, a Multi-Agent System to assist the experts during computer forensic examinations. The study pointed out that the combination of the reduction in the volume of evidence to be examined by the expert and the reduction in execution times obtained with the distributed processing of the evidence already show the potential of the tool and the productivity gains it can offer to computer forensic experts and to investigators facing an ever-increasing volume of digital evidence (Hoelz et al., 2008). Another AI model that uses machine learning techniques has been proposed by Platzer, Stuetz and Lindhofer (2014) in their study that provides a potential solution to detecting nudity or pornography by using, among others, an SVM (Sup-

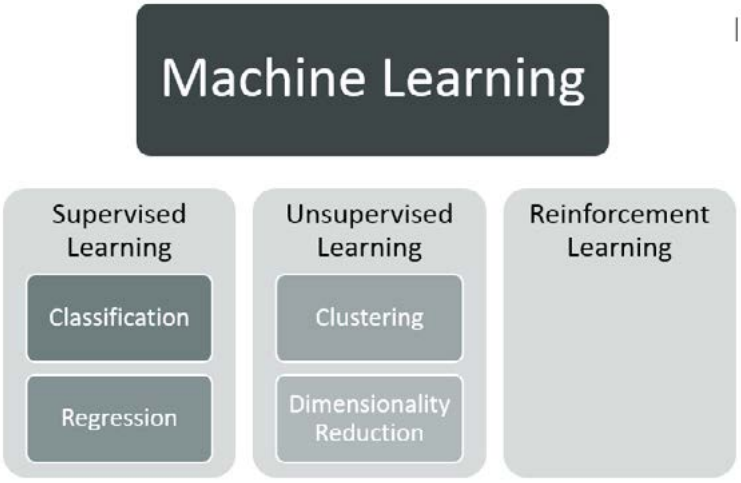
9 https://en.wikipedia.org/wiki/Digital_forensics.

port Vector Machine) algorithm for the classification of images.

In the subject of Knowledge representation and knowledge engineering, which are central to classical AI research (Poole, Mackworth & Goebel 1998; Russell & Norvik 2010), the implementation of systems that can reduce human knowledge into a set of standardized rules would be beneficial to digital forensics practitioners, as they could use the concepts and relations interpreted by software agents to discover more relevant artifacts in the investigation of cases. A recent approach to the subject is the COST Action DigForASP, a system that aims at creating a research infrastructure for the application of Artificial Intelligence (AI), in particular from the area of Knowledge Representation and Reasoning, together with other complementary areas, in the field of Digital Forensics (Constantini, Lisi & Olivieri, 2019).

By categorizing data with labels through supervised learning and identifying patterns in data sets via unsupervised learning, the process gives devices the ability to help us make decisions quicker and with greater accuracy. With reinforcement learning methods, a process which resembles how people and animals learn through trial and error, machines and devices can expand their capabilities independently without explicit programming[10]. A special part of machine learning algorithms, which is capable of assisting human expert performance and even surpassing it in certain cases, is Deep Learning. This class of AI systems generally refers to Artificial Neural Networks and it is prominently featured in modern research. The main approaches of Machine Learning, which correspond to learning paradigms, are outlined in Figure 5.

Figure 5. Machine Learning



Artificial Intelligence techniques that can be applied in digital forensics in general, as well as mobile forensics in particular, include Case Based Reasoners (CBRs), Pattern Recognition, Knowledge Discovery, System Adaptation, Refinement of Knowledge and Machine Learning (Symbolic Learners and Sub Symbolic Learners) (Mitchell 2010). There are several commercial tools and forensic software that have implemented features related to Artificial Intelligence and Machine Learning, which are provided by companies such as Magnet, Cellebrite, Belkasoft, Grayshift, Oxygen Forensics and MSAB. The respective software enables image and video categorization in an automated way, based on media classification algorithms, for predetermined categories.

The available categories generally correspond to important artifacts for examiners and include, but are not limited to, drugs, weapons, documents, nudity, faces and vehicles. These features that are provided with mobile forensics software allow for quick sorting and analysis of large volumes of data, resulting in a substantial improvement in examination speed and efficiency.

10 https://www.samsung.com/semiconductor/minisite/exynos/technology/ai/

Technology Integration – adoption and legal issues

The complete integration of AI related forensic technologies has not yet happened and will be delayed in practice as long as AI is facing the current barriers and challenges. Those challenges include the lack of proper regulatory framework, the general fear and absence of trust for the technology, promoted by inadequate knowledge and information for AI algorithms, as well as the shortage of computer systems capable of supporting AI applications and features. In addition, there is still a lot of complexity in AI and ML algorithms and insufficiency of relevant datasets, which are necessary for machine learning.

As AI research finds its way into digital forensics applications, there are many legal issues that surface and create the need for reliable solutions. First of all, the current legal framework does not have concrete rules regarding the legal value and presentation of artifacts detected and categorized by artificial intelligence systems. Currently, any conclusions reached by artificial intelligence software needs to be analyzed and verified by human investigators, but as artificially intelligent software continues to become more sophisticated and accurate, the traditional rules might prove to be insufficient in the future of Digital Forensics. On a similar note, the lack of algorithmic transparency is a significant issue that is at the forefront of legal discussions on AI (Mitchell, 2010).

Furthermore, the protection of data privacy is a major challenge for forensic software that offers features utilizing machine learning algorithms. In order to train models based on ML techniques, that achieve significant scores using the available evaluation metrics, it is necessary to process extensive datasets of relevant forensic artifacts, such as images. While these models are being developed, it is vital that the techniques used for data processing are compliant with existing legislation and preserve data confidentiality and privacy.

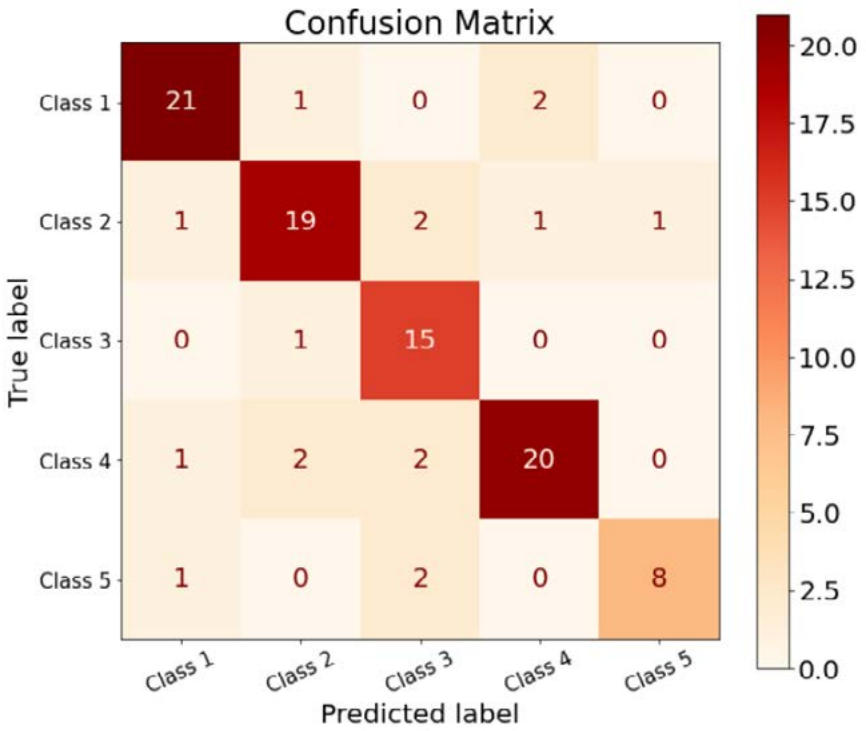
Evaluation metrics

Special reference should be reserved for the aforementioned evaluation metrics that correspond to the ML models, as the related assessment would significantly affect the interpretability and explainability of Artificial Intelligence with regards to digital forensic investigations, with direct correlations to forensic reporting and the presentation of the evidence in a court of law. The most prominent one is accuracy, which refers to the ratio of the number of correct predictions – classifications to the total number of inputs.

Even though a high accuracy score in media classification can provide essential benefits, the cost of misclassification, whether it is a false positive or a false negative, needs to be accounted for, in order to determine the performance and actual contribution of the model. Along with total Accuracy, True Positive Rate (Sensitivity) and True Negative rate (Specificity) can be used as metrics to determine the model's ability to predict the true positives and true negatives, respectively, for each available class. With high Sensitivity, a negative result means that an artifact probably does not belong to the specified category (rate of actual positives which are correctly identified), while with high Specificity a positive result means that an artifact probably belongs to the specified category (rate of actual negatives which are correctly identified).

Additionally, the confusion matrix is a two-dimensional matrix that visualizes the performance of a model and can be used for a complete demonstration of the output results and the explanation of the conclusions, by providing a picture of interrelation between different categories. A confusion matrix example for an image classification of five random image categories (Class 1 – Class 5) is displayed in Figure 6. Each row represents a number of the actual or True class and each column represents a number of the predicted class.

Figure 6. Confusion Matrix



The confusion matrix is a table that provides the combinations of actual and predicted values for a certain category and includes the True Positives, True Negatives, False Positives and False Negatives of a classification instance, which can be used to discover further information about the model's effectiveness. These values can be used to calculate Precision and Recall (same as sensitivity), as well as the F1 score, which are also useful evaluation metrics that can offer important insights into the performance of the algorithms. Precision is the number of positive predictions that actually belong to the positive class and Recall is the number of positive predictions out of all positive instances in the data. Higher precision values mean that the model returns more relevant than irrelevant results and higher recall values mean that the model returns most of the relevant results for a specified category. In addition, F1 score is calculated using the values of precision and recall, as the harmonic mean of these metrics, providing a balance between them. All the afore mentioned metrics can be used in determining the efficacy and usefulness of a model in classification problems, which are prevalent in Mobile Forensics cases. It should be noted that the impact of the evaluation metrics is case dependent, and the appropriate usage is vital for the implementation of a transparent and scientifically accurate forensic examination framework.

Conclusion

Artificial Intelligence has become a prominent feature in our lives, with intelligent machines affecting many scientific fields, business environments and everyday life. With the ongoing research showing potential in providing significant solutions in important challenges of our time, the arrival and establishment of AI and Machine Learning techniques in the field of Mobile Forensics seems inevitable and it could revolutionize the practice of digital forensics investigations.

In this paper we have shown that there are already readily available solutions in the market relevant to the advancements in AI technology and that many promising projects are also in progress. The breakthroughs in Artificial intelligence have prompted optimism and further interest from commercial and scientific entities and organizations, but legal issues should be taken into consideration and regulatory measures should be put in place in order to utilize the benefits of the research with respect to legal proceedings, while protecting the individual rights and privacy of the people. The rapid advancements in Mobile Networks, Cloud Computing, Internet of Things and Big Data technologies indicate that a new era in Digital and Mobile Forensics is entering, so the potential and the concerns regarding

Artificial Intelligence should be examined as soon as possible.

The review of the current status of Mobile Forensics, the major challenges and the solutions currently provided for digital forensics investigators indicates the following areas as recommendation for future research.

Research into the automated recognition of patterns and regularities in data and implementation of reliable solutions in forensic software would be very advantageous for analysts. Topics could include optical character recognition, image classification, text classification and data clustering.

In addition, advancements in link analysis could be valuable, since it can be used by machine learning forensics to discover the content and structure of a body of information by transferring the information into a set of interconnected entities or objects that are linked together (Qadir & Valor, 2020). Through this technique, digital forensic investigators can reveal associations between individuals, associations between individuals and organizations, as well as associations between a place and an individual (Mena, 2003). Furthermore, improvements into the accuracy of image and video classification would be very beneficial for the field of Mobile Forensics.

The domain of Digital Forensics could be substantially benefited by research and development regarding the capability of forensic software to read and understand human language. The acquisition of knowledge directly from human created artifacts could lead to faster classification and importance evaluation of data during the examination and analysis of digital evidence. For example, word clustering can be achieved from emails, call site transcripts, instant messages, website forms, chats, phone calls and texts (Mena, 2016).

Specialized software that is publicly accessible and reflects the culmination of a problem-solving initiative in a scientific domain could help reduce the severity of the issues negatively affecting the current state of Mobile Forensics. Open-source tools with AI capabilities can provide examiners with problem-specific solutions in a number of highly technical cases, where available software might prove to be insufficient. Raising awareness of the importance of the development and adoption of such tools should therefore be at the forefront of the mobile forensics' community.

The international standards for forensic sciences and related scientific methods are essential for the credibility and transparency of evidence and legal prosecution of cases. As Artificial Intelligence claims a bigger and more significant role in the forensic examination of mobile devices, the conception and application of new concrete standards and legal procedures, accepted by the scientific community and applied by Forensic Institutes and Law Enforcement Agencies should be considered as developments of utmost importance.

References

- Alzaabi,M. Jones, A. & Martin, T. A. (2013) An ontology-based forensic analysis of mobile devices. Annual ADFSL Conference on Digital Forensics, Security and Law. 5.
  Available at: https://commons.erau.edu/cgi/viewcontent.cgi?article=1245&context=adfsl
- Boyd, M. (2014). built.io Is Building an Enterprise MBaas Platform for IoT. Programmableweb.
  Available at: https://www.programmableweb.com/news/builtio-building-enterprise-mbaas-platform-iot/interview/2014/03/03
- Columbus, L. (2014) Roundup of cloud computing forecasts and market estimates, 2014. *Forbes*.
  Available at: https://www.forbes.com/sites/louiscolumbus/2014/03/14/roundup-of-cloud-computing-forecasts-and-market-estimates-2014/?sh=59f2de4057a2
- Constantini, S., Lisi, F. & Olivieri, R (2019) Knowledge Representation and Reasoning meets Digital Forensics: The COST Action DigForASP (short paper). RCRA/RiCeRcA@AI*IA. January.
  Available at: http://ceur-ws.org/Vol-2538/paper5.pdf
- Gantz, J. & Reinsel, E. (2011) Extracting Value from Chaos. IDC's Digital Universe Study.
  Available at: http://www.kushima.org/wp-content/uploads/2013/05/DigitalUniverse2011.pdf
- Harrill, D.C., & Mislan, R.P. (2007) A Small Scale Digital Device Forensics ontology. *Small Scale Digital Device Forensics Journal*, 1 (1), pp. 1-7.
  Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.444.4475&rep=rep1&type=pdf

- Hoelz, B., Ralha, C., Geeverghese, R. & Junior, H. (2008) A cooperative multi-agent approach to computer forensics. Proceedings – 2008 IEEE/WIC/ACM International Conference on Intelligent Agent Technology, 2, pp. 477-483.
- Homem, I. (2018) Advancing Automation in Digital Forensic Investigations. *Academic dissertation Stockholm University.* Available at: https://www.diva-portal.org/smash/get/diva2:1259778/FULLTEXT01.pdf
- Jarrett, A. & Choo, K.-K. (2021) The impact of automation and artificial intelligence on digital forensics. WIREs Forensic Science 3, e1418, pp. 1-17. Available at: https://wires.onlinelibrary.wiley.com/doi/epdf/10.1002/wfs2.1418
- Khan, A-U., Othman, M. Madani, S.& Khan, S. (2014) A Survey of Mobile Cloud Computing Application Models. *IEEE Communications Surveys and Tutorials 16 (1), 393-413*.
- Mena, J. (2003) Investigative data mining for security and criminal detection. Butterworth-Heinemann.
- Mena, J. (2016) Machine learning forensics for law enforcement, security, and intelligence. Auerbach Publications.
- Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012) Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10 (7), pp. 1497–1516.
- Mitchell, F. (2010) The use of Artificial Intelligence in digital forensics: An Introduction. *Digital Evidence and Electronic Signature Law Review*, 7, pp. 35-41. Available at: https://sas-space.sas.ac.uk/5533/1/1922-2707-1-SM.pdf
- Mohammed, H.J., Clarke, N., & Li, F. (2016) An Automated Approach for Digital Forensic Analysis of Heterogeneous Big Data. *J. Digit. Forensics Secur. Law*, 11, pp. 137-152.
- Nordrum, A. (2016) Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. *IEEE Spectrum*.
- Platzer, C., Stuetz, M. & Lindorfer, M. (2014) Skin sheriff: a machine learning solution for detecting explicit images, Proceedings of the 2nd International workshop on security and forensics in communication systems. pp. 45-56: ACM Available at: https://publik.tuwien.ac.at/files/publik_273619.pdf
- Poole, D., Mackworth, A., & Goebel, R. (1998) *Computational intelligence: A logical approach*. Oxford: Oxford University Press.
- Qadir, A. & Varol, A. (2020) The Role of Machine Learning in Digital Forensics. Paper presented at the 8th International Symposium on Digital Forensics and Security (ISDFS), June 1-2, Beirut, Lebanon. Available at: https://www.researchgate.net/publication/342193343_The_Role_of_Machine_Learning_in_Digital_Forensics
- Quick, R. & Choo, K.-K. (2018) Big Digital Forensic Data. In Volume 2: Quick Analysis for Evidence and Intelligence. Springer Briefs on Cyber Security Systems and Networks. Springer.
- Reinsel, D., Gantz, J. & Rydning, J. (2017). Data Age. IDC White Paper. Available at: https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf
- Roy, N., Khanna, A. & Aneja, L. (2016) Android phone forensic: Tools and techniques. International Conference on Computing, Communication and Automation (ICCCA2016), 605-610. Available at: https://www.researchgate.net/profile/Nihar-Roy-4/publication/312559420_Android_phone_forensic_Tools_and_techniques/links/5eecdad1458515814a6b45df/Android-phone-forensic-Tools-and-techniques.pdf
- Russell, S. J., & Norvig, P. (2010) Artificial intelligence: A modern approach. *Applied Mechanics & Materials*, 263(5), pp. 2829–2833.
- Sejdić, E. (2014) Correspondence: Adapt current tools for use with big data. *Nature* 507 (7492), p. 306. Available at: https://www.nature.com/articles/507306a.pdf
- Soric, D. (2021) Cloud computing 101. *Digital Reflections*. Available at: https://medium.com/digital-reflections/cloud-computing-101-2b66e54c66c4
- Yaqoob, I., Hashem, I., T. Ahmed, A. Ahsan Kazmi, S. & Hong, C. (2019) Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, 92, pp. 265-275.