Paweł Olber[1]
ORCID: 0000-0002-4614-9527

Artificial intelligence and future crime in the context of computer forensics

Introduction

The dynamic development of new technologies affects many aspects of the modern world. We are currently witnessing the development of innovative solutions which certainly include artificial intelligence. Dynamic technological development also contributes to a significant increase in the amount of information being processed. The constant increase in digital data and the increasing capacity of storage media have meant that modern electronic mobile devices serve as repositories for vast amounts of personal information, which, for many reasons, is of interest to criminal groups. A natural consequence of new technology dynamic progress is therefore the development of crime.

An important element in combating modern crime is the examination of digital evidence characterised by its time-consuming nature due to the huge amounts of data to be analysed. This, in turn, results in a backlog in the forensic examination of digital evidence and has a negative impact on the criminal trial duration.

The aim of the research, the results of which are presented in this paper, was to identify the role, tasks and challenges of computer forensics in the context of developments in artificial intelligence and crime.

Given this, a hypothesis was formulated according to which the future of computer forensics is the automation of expert witness's tasks based on artificial intelligence technology which will contribute to the optimisation of the processing of large digital data sets.

The research hypothesis has determined the structure of the paper. Separate sections of the article present issues of computer forensics, including the ones related to contemporary and future challenges that are associated with the development of artificial intelligence. Certainly, on one hand AI brings many promising benefits, but on the other, it may also contribute to the development of existing threats or give rise to new ones. Therefore, the

[1] Dr Paweł Olber — senior lecturer at the Institute of Criminal Service, Faculty of Security and Legal Sciences, Police Academy in Szczytno.
Contact with the author via the editorial board.

article presents the potential malicious use of artificial intelligence which will have an impact on the development of crime and thus on computer forensics. The development of computer forensics will be linked to the creation of solutions based on artificial intelligence algorithms. Furthermore, artificial intelligence technology will define new scopes of computer forensics related to the analysis of neural network models and learning datasets.

The monographic method with the critical literature analysis were applied to the research. Discussion and conclusions are presented at the end of the paper.

Computer forensics

Computer forensics is a field of forensic science that aims to provide digital evidence. Computer forensics involves the identification, collection, acquisition and examination of digital evidence, as well as the analysis of revealed artefacts, while preserving the integrity of the information and maintaining the continuity of the chain of custody[2].The chain of custody is defined as the verifiable source and record of possession of digital evidence from the moment it is secured at the scene until it is presented in court[3].

The main task of computer forensics is the examination of digital media and digital environments to reveal traces of the crime[4] and to establish the circumstances which are relevant to the case[5]. Computer forensics is a relatively new field of forensic science compared to other branches of traditional forensic science. Furthermore, it is one of the fastest growing branches of forensic science.

Contemporary challenges in computer forensics

Computer forensics is facing a number of problems today that arise from the popularity and widespread use of information and communications technologies (ICT). These challenges are related to the increasing amount of data and devices that are examined in computer forensics, the existence of different operating systems, the use of encryption and new technological paradigms: cloud computing and the Internet of Things[6].

[2] Kent K, Chevalier S, Grance T, and Dang H, Guide to integrating forensic techniques into incident response. Recommendations of the National Institute. Gaithersburg, 2006, s. 16.

[3] Lone A.H, Mir R.N, Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer, *Digital Investigation* 2019, No. 28, p. 45.

[4] JKävrestad J, Fundamentals of digital forensics. Theory, methods, and real-life applications. Cham, 2020, p. 3.

[5] CLKP, Badania informatyczne, <Centralne Laboratorium Kryminalistyczne Badania Informatyczne. *Electronic source:* https://www.clkp.policja.pl/clk/badania-i-projekty/langnodata/badania-informatyczne/153011,Badania-Informatyczne.pdf, a*ccessed:* 14.02.2022.

[6] Al Fahdi M, Clarke N.L, Li F, and Furnell S.M, A suspect-oriented intelligent and automated computer forensic analysis, *Digital Investigation* 2016, Vol 18, p. 65.

The use of technology in almost all aspects of life has led to an increasing requirement for digital device analysis in criminal cases, which results in a backlog of examinations commissioned to law enforcement agencies[7]. Computer forensics experts are responsible for undertaking the cognitively difficult and time-consuming process of identifying and analysing relevant artefacts. Due to the large number of crimes dependent on cyberspace (*e.g.* hacking) and crimes committed in cyberspace (*e.g.* online fraud), there is a need to investigate multiple devices which in turn results in a large backlog of cases[8]. Computer forensic examinations are characterised by their time-consuming nature and variety, due to the multiplicity of types of digital storage media analysed in police forensic laboratories and the wide range of criminal investigations for which these devices are secured. In some cases, the waiting time for the examination of secured digital evidence is longer than 12 months[9].

In parallel with the exponentially increasing number of computer devices, the requirements for optimising the time taken to analyse digital evidence are increasing. There is, therefore, a need to fully automate the activities performed in computer forensics to speed up the process. However, it is not a simple task as the analysed data comes from various sources and is unstructured in nature[10].

Automation exists, but only for certain tasks such as data recovery and file signature analysis[11]. We are currently witnessing the partial implementation of automation in the detection of objects (human, car or weapon) in analysed images or video recordings. Such solutions have been implemented in tools designed for expert witnesses in the field of visual recording examination[12].

The future of computer forensics

In the context of future automation of computer forensics activities, it is essential to develop solutions to efficiently generate structured data from hybrid data that is stored in different formats. Future work should also include building advanced computer forensics tools, developing solutions to secure data quickly, reducing data complexity and using

[7] Scanlon M, Battling the Digital Forensic Backlog through Data Deduplication, [in:] 2016 Sixth International Conference on Innovative Computing Technology (INTECH). Dublin, 2016, p. 2.

[8] Al Fahdi M, et al, A suspect-oriented..., op. cit., p. 66.

[9] Mayor of London, Backlog of mobile phones and computers awaiting forensic analysis. E*lectronic source:* https://www.london.gov.uk/questions/2019/12159#:%01:text=Digital%20Forensics%20currently%20have%20approximately,will%20take%20over%2012%20months, a*ccessed*: 14.02.2022.

[10] Sikos L.F, AI in digital forensics: Ontology engineering for cybercrime investigations, *WIREs Forensic Science*, Vol 3, No. 3, p. 2.

[11] Al Fahdi M, et al, A suspect-oriented..., op. cit., p. 65.

[12] Javed A.R, Ahmed W, Alazab M, Jalil Z, Kifayat K, and Gadekallu T.R, A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions, *IEEE Access*. 2022, Vol 10, p. 11080.

blockchain technology[13] to handle digital evidence. Another challenge is to standardise the ontology of computer forensics – a set of concepts and descriptions of the relationships between them, as most of the schemas and techniques used in computer forensics relate to non-standard applications and domains[14].

Automated forensic tools using machine learning algorithms and deep learning[15] are truly required in the era of the current technological development. Artificial intelligence is the future of computer forensics. Researchers should therefore carefully define the roles and tasks of artificial intelligence at the stage of digital evidence content analysis as the technology in question will autonomously process data and develop hypotheses[16].

Artificial intelligence

The term artificial intelligence was first proposed by John McCarthy, then a professor of mathematics at Dartmouth University. It is considered to have been the first step towards further research into the simulation of human thinking and acting by machines[17]. The development of new technologies, including artificial intelligence, has brought enormous economic benefits to mankind and positively influenced all aspects of human life, as well as significantly contributed to social development[18].

Artificial intelligence is a broad term that can be defined as the ability of a computer system to perform tasks that require human intelligence. One subset of artificial intelligence is machine learning, which enables the system to learn and improve from data, without the need for explicit programming. Machine learning uses various algorithms that iteratively learn from input data (also referred to as training datasets) to evaluate, improve and predict unknown data. There are different categories of machine learning, such as supervised learning, unsupervised learning, reinforcement learning and deep learning based on artificial neural networks[19]. They differ in the level of human supervision and intervention that the machine learning process requires[20]. In supervised learning, the

[13] Blockchain – a distributed database consisting of blocks containing information on transactions carried out on the Internet.

[14] Javed A.R, et al., A Comprehensive Survey on Computer Forensics..., op. cit., p. 11084.

[15] Iqbal S, and Abed Alharbi S, Advancing Automation, Digital Forensic Investigations Using Machine Learning Forensics, [in:] Suresh Kumar Shetty B, and Pavanchand Shetty H, (Eds), Digital Forensic Science. London, 2019, p. 4.

[16] Javed A.R, et al., A Comprehensive Survey on Computer Forensics..., op. cit., p. 11084

[17] Zhang C, and Lu Y, Study on artificial intelligence: The state of the art and future prospects, *Journal of Industrial Information Integration*. 2021, Vol 23, p. 1.

[18] Lu Y, and Xu L.D, Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics, *IEEE Internet Things*. 2019, Vol 6, No. 2, p. 2.

[19] Hurwitz J, and Kirsch D, Machine Learning For Dummies. Hoboken, New York, 2018, p. 5.

[20] Matulionyte R, Australian Copyright Law Impedes the Development of Artificial In-

machine is trained on a predefined set of training examples, which facilitates its ability to make precise and accurate conclusions when provided with new data. In unsupervised learning, the machine is given a set of data and must find some common patterns and relationships between the data on its own[21]. Reinforcement learning involves teaching the system through interaction with the environment in order to ultimately achieve the desired goal. It is a type of trial-and-error learning. Each time a neural network is successful, it is reinforced by updating its internal parameters. Deep learning is a specific method of machine learning that uses complex neural networks that contain hidden layers. The more complex the problem, the more hidden layers the model being trained will have[22].

Computer forensics in the context of artificial intelligence

Artificial intelligence plays an essential role in social development, bringing revolutionary effects in terms of improving labour productivity, reducing labour costs, optimising the structure of human resources and creating new professional requirements. Although the aforementioned technology offers many benefits to citizens and the economy, it simultaneously poses new challenges and risks[23]. A wide range of artificial intelligence applications include crime prevention and detection systems (Dilek et al.[24]; Li et al, 2010[25]; Lira Cortes and Fuentes Silva, 2021[26]), but the technology also has the potential to be misused for the benefit of crime (Kaloudi and Li, 2021[27]; Sharif et al., 2016[28]; van der Wagen and Pieters, 2015[29]).

In the fight against crime, a momentous task falls to forensic science which must keep pace with developments in science and crime, inter alia

telligence: What Are the Options?, *IIC - International Review of Intellectual Property and Competition Law.* 2021, Vol. 52, p. 421.

[21] Shah N, Bhagat N, and Shah M, Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention, *Visual Computing for Industry, Biomedicine, and Art.* 2021, Vol 4, No. 1, p. 9.

[22] Hurwitz J, and Kirsch D, Machine Learning..., op. cit., p. 18.

[23] Cheng L, and Xie F, Yadong Cui, Artificial Intelligence and Judicial Modernization, *International Journal for the Semiotics of Law.* 2021, Vol 34, No. 1, p. 296.

[24] Dilek S, Cakır H, and Aydın M, Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review, *International Journal of Artificial Intelligence & Application.* 6(1), pp. 21–26.

[25] Li S.T, Kuo S.C, and Tsai F.C, An intelligent decision-support model using FSOM and rule extraction for crime prevention, *Expert Systems with Applications.* 2010, Vol 37, No. 10, p. 7110.

[26] Lira Cortes A.L, and Fuentes Silva C, Artificial Intelligence Models for Crime Prediction in Urban Spaces, *Machine Learning and Applications: An International Journal.* 2021, Vol 8, No. 1, pp. 3–7.

[27] Kaloudi N, and Li J, The AI-Based Cyber Threat Landscape: A Survey, *ACM Computing Surveys.* 2021, Vol 53, No. 1, pp. 2–3.

[28] Sharif M, Bhagavatula S, Bauer L, and Reiter M.K, Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition, [in:] Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Austria, 2016, p. 1528.

[29] Van der Wagen W, and Pieters W, From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks, *The British Journal of Criminology*. Vol 55, No. 3, p. 578.

by adapting the achievements of other sciences, modifying the methods and means and developing its own solutions. This also applies to computer forensics whose development will take into account the AI-enabled future crime.

Malicious use of artificial intelligence

Crime opportunities arising from artificial intelligence exist both in the specifically computational domain (which overlaps with traditional notions of cyber security) and in the wider world. Some of these hazards come as extensions of existing criminal activity, while others may be new. In order to adequately prepare for potential AI threats, it is important to identify the types of threats and how they may affect our lives and societies. There have been a number of recent attempts to identify and classify the potential future risks of AI-enabled crime.

Miles Brundage et al. discuss possible scenarios for the malicious use of artificial intelligence in the short term (up to 5 years) and make some strategic policy recommendations[30]. The recommendations emphasise the importance of multilateral cooperation between a wide range of parties, both on the policy-making and technology side. Alex Wilner assesses contemporary cybersecurity threats with a particular focus on the increasing connectivity of Internet of Things devices[31]. Thomas King et al. undertake a systematic literature review to identify foreseeable risks associated with artificial intelligence, providing ethicists, policymakers and law enforcement with a synthesis of current problems and possible solutions[32]. Peters presents four fictional threat scenarios and discusses possible response strategies. The speculative nature of the aforementioned authors' deliberations means that no single set of correct scenarios can be expected and the existence of each should be seen as complementary to the others[33].

A similar effort was undertaken in February 2019 by a team of independent experts attending a workshop on Artificial Intelligence and Future Crime held at University College London. A total of 31 delegates invited for their interest in the topic and expertise attended the workshop. The majority of participants were UK-based, with 3 delegates private sector from Poland[34].

[30] Brundage M, Avin S, Clark J, Toner H, Eckersley P, Garfinkel B, Dafoe A, et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *Electronic source:* https://doi.org/10.17863/CAM.22520, a*ccessed:* 16.02.2022.

[31] Wilner A.S, Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation, *International Journal.* 2018, Vol 73, No. 2, p. 309.

[32] King T.C, Aggarwal N, Taddeo M, and Floridi L, Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions, *Science and Engineering Ethics.* 2020, Vol 26, No. 1, pp. 90–92.

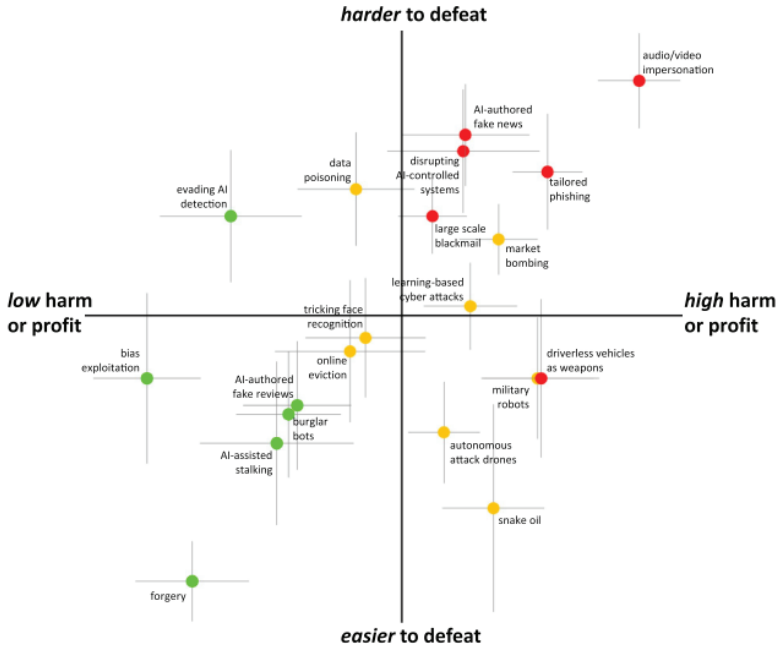
[33] Peters K.M, 21st century crime: how malicious artificial intelligence will impact homeland security. California, 2019, p. 7.

[34] Caldwell M, Andrews J.T.A, Tanay,T, and Griffin L.D, AI-enabled future..., op. cit., p. 2.

The workshop reviewed potential AI-based crimes of the future and assessed them according to four categories: the degree of social harm, criminal profit and how easy and difficult the crime is to defeat. All potential crimes and risks are shown in Figure 1.

Fig. 1

Potential risks and crimes associated with the use of artificial intelligence



Source: M. Caldwell et al, AI-enabled future crime, *Crime Science,* 2020, No 9 (14), p. 11.

The experts considered the following crimes to be the most troublesome and most likely: a) impersonation, b) use of autonomous vehicles as weapons, c) tailored phishing, d) disruption of AI-controlled systems, e) large-scale blackmail, f) fake news[35].

a) a) impersonation

The use of artificial intelligence and machine learning makes it possible to modify or generate digital content that creates a false reality. This is because the technologies in question allow still and moving images to be combined and superimposed on source images or videos. This creates among other things, recordings of statements and behaviours of people who did not actually do what the viewer saw36.

[35] Ibid, pp. 7–9.

[36] Frank J., Eisenhofer T, Schönherr L, Fischer A, Kolossa D, and Holz T, Leveraging Frequency Analysis for Deep Fake Image Recognition, [in:] Proceedings of the 37th International Conference on Machine Learning 2020, p. 1. *Electronic source*: http://proceedings.mlr.press/v119/frank20a/frank20a.pdf, a*ccessed:* 20.02.2022.

Real-time impersonation is expected to be a problem in the future. Such a measure will be widely used in crime based on trust in another person. An example of this type of activity could be the impersonation of an elderly person's child during a video conference in order to gain access to their funds. Another example would be impersonating a specific person during a phone call in order to gain access to secure systems or obtain other important information37.

b) b) crimes involving autonomous vehicles

Motor vehicles have long been used both as a delivery mechanism for explosives and as kinetic weapons of terror, with the latter increasing in prevalence in recent years. Vehicles are much more readily available than firearms and explosives in most countries, and attacks using vehicles can be carried out at relatively low organisational overhead. Such tactics have gained particular popularity following a series of attacks carried out in 2016 - 2017 in Nice, Berlin, London, Barcelona and New York38.

Although fully autonomous AI-controlled vehicles are not generally available yet, numerous car manufacturers and technology companies are racing to develop them. A number of autonomous vehicle manufacturers have agreed to conduct tests on public roads. The laws of many countries allow the use of public roads for the purpose of conducting such tests. Autonomous vehicles would potentially allow expansion of vehicular terrorism by reducing the need for driver recruitment, enabling single perpetrators to perform multiple attacks, even coordinating large numbers of vehicles at once. Driverless cars are certain to include extensive security systems that criminals will need to breach or override in order to commit crimes. Nevertheless, experts have rated this type of attack as highly achievable and harmful39.

c) c) tailored phishing

Phishing is a social engineering attack that aims to collect sensitive information (*e.g.* user account login details, payment card numbers, etc.) or installing malware using fake websites and messages purporting to be from a trusted party, such as the user's bank. The attacker exploits the existing trust to get the user to perform certain actions. Phishing has long been ranked as one of the most popular methods of cyberattack[40].

Currently phishing attacks do not target individuals. They are most often carried out on the basis of generic messages, sent in groups to end-users of mobile devices who generally do not exercise due caution[41].

[37] Caldwell M, Andrews J.T.A, Tanay T, and Griffin L.D, AI-enabled future..., op. cit., s. 6.

[38] Jasiński A, Protecting public spaces against vehicular terrorist attacks, *Czasopismo Techniczne.* 2018, No. 2, pp. 47–48.

[39] Caldwell M, Andrews J.T.A, Tanay T, and Griffin L.D, AI-enabled future..., op. cit., p. 7.

[40] Basit A, Zafar M, Liu X, Javed A.R, Jalil Z, and Kifayat K, A comprehensive survey of AI-enabled phishing attacks detection techniques, *Telecommunication Systems.* 2021, Vol 76, No. 1, p. 140.

[41] Sahingoz O.K, Buber E, Demir O, and Diri B, Machine learning based phishing detection from URLs, *Expert Systems with Applications.* 2019, Vol 117, p. 346.

Artificial intelligence has the potential to improve the effectiveness of phishing attacks by profiling victims and tailoring content or attack methods to specific profiles. It will use, among other things, more reliable messages containing information directly related to the individual. This information will be extracted automatically from a variety of sources, such as social networks. In addition, artificial intelligence methods will be able to use active learning to adapt attacks and thus increase their effectiveness[42].

Tailored phishing has been rated very high by experts in terms of criminal profit and the feasibility of this type of crime. According to experts, tailored phishing based on artificial intelligence mechanisms would be extremely difficult to stop[43].

d) d) disrupting AI-controlled systems

As the use of artificial intelligence increases in many areas of public life, the possibility of attacks targeting the confidentiality, integrity and availability of information systems will proliferate[44]. Systems responsible for all aspects of public safety are likely to become key targets for cyber-attacks, as are systems overseeing financial transactions. According to experts, this type of crime will be characterised by a high rate of harm and a high rate of profit[45].

e) large-scale blackmail

Traditional blackmail involves extortion under the threat of exposure of evidence of a crime or minor offence, or embarrassing personal information. A limiting factor in traditional blackmail is the acquisition of such evidence and information and the profitability of such actions. This type of behaviour will only be beneficial if the victim pays more to suppress the evidence or embarrassing information than the cost of obtaining it[46].

Artificial intelligence can be used for blackmail on a much larger scale, gathering information about a person (which in itself does not necessarily constitute incriminating material) and identifying specific vulnerabilities for a large number of potential victims and tailoring messages to each of them. Artificial intelligence can also be used to generate false evidence and compromising information[47].

Large-scale blackmail has been rated high by experts in terms of criminal profit. Counteracting and combating large-scale blackmail has been considered as highly problematic. The harm has been assessed as average, since the crime by nature is directed against individuals[48].

[42] Bahnsen A.C, Torroledo I, Camacho L.D, and Villegas S, DeepPhish: Simulating Malicious AI, pp. 7–8. Electronic source: https://albahnsen.files.wordpress.com/2018/05/deepphish-simulating-malicious-ai_submitted.pdf., accessed: 16.02.2022.

[43] Caldwell M, Andrews J.T.A, Tanay T, and Griffin L.D, AI-enabled future..., op. cit., pp. 7–8.

[44] Surma J, (Ed.), Hakowanie sztucznej inteligencji. Warsaw, 2020, pp. 23-34.

[45] Ibid, p. 8.

[46] Bairmani H.K, Al Asfer N.N.S, Persuasion in Cyber Blackmail's Emails: A pragma-dialectical Study. 2021), *Review of International Geographical Education Online*, 11(5), p. 2121.

[47] Peters K.M, 21st century crime..., op. cit., p. 61.

[48] Caldwell M, Andrews J.T.A, Tanay T, and Griffin L.D, AI-enabled future..., op. cit.,

f) f) fake news

The term *fake news* has no formal or uniform definition. In a loose sense, the term means the deliberate presentation of (usually) false or misleading claims and opinions. In addition to providing false content, such messages can distract from real information[49].

Artificial intelligence can be used to generate multiple versions of a particular content, from multiple sources, to increase its visibility and credibility. In addition, artificial intelligence algorithms can personalise the content of messages in order to boost their impact[50].

AI-authored fake news has been rated high in terms of the harm due to its significant potential to influence specific political events and multidimensional social effects[51].

Computer forensics in the context of future crime

Computer forensics is heavily influenced by new technologies. The rapid digital transformation is generating both many challenges and new opportunities in computer forensics[52]. The challenges in computer forensics will arise from new forms of crime that will emerge in the future and will be based on new technologies. Indeed, forensic science has the momentous role of developing and adapting technical means to detect, secure and examine evidence, which represents one aspect of the fight against crime[53].

New forms of criminal activity will be a motivating factor for law enforcement and justice authorities to develop effective methods and solutions to combat crime. In the above mentioned crimes supported by artificial intelligence algorithms, traditional methods of detecting and combating them will not produce the expected results because they are very slow and inefficient[54].

It is therefore necessary to develop AI-supported solutions to help predict crime and support law enforcement and justice authorities. The use

p. 8.

[49] Gelfert A, Fake News: A Definition, *Informal Logic.* 2018, Vol 38, No. 1, pp. 85–86.

[50] Kim J, Shin S, Bae K, Oh S, Park E, and del Pobil A.P, Can AI be a content generator? Effects of content generators and information delivery methods on the psychology of content consumers, *Telematics and Informatics.* 2020, Vol 55, p. 2.

[51] Caldwell M, Andrews J.T.A, Tanay T, and Griffin L.D, AI-enabled future..., op. cit., pp. 8–9.

[52] Crispino F, Weyermann C, Delémont O, Roux C, and Ribaux O, Towards another paradigm for forensic science?, *Australian Journal of Forensic Sciences.* 2021, p. 1. *Electronic source:* https://wires.onlinelibrary.wiley.com/doi/epdf/10.1002/wfs2.1441, a*ccessed:* 24.02.2022.

[53] Kędzierska G, Kędzierski W, Kryminalistyka. Wybrane zagadnienia techniki, Szczytno 2011, p. 22.

[54] Shah N, Bhagat N, and Shah M, Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention, *Visual Computing for Industry, Biomedicine, and Art.* 2021, Vol 4, No. 1, p. 1.

of machine learning and computer vision techniques can bring many benefits to investigators[55].

With regard to computer forensics experts, this support should consist of the implementation of solutions that allow: a) automatic identification of artefacts, b) automatic generation of structured data, c) automatic categorisation of multimedia content, d) object detection, e) detection and analysis of manipulated software, f) examination of autonomous systems.

a) a) automatic identification of artefacts

One solution to support computer forensics can be the use of automatic pattern recognition based on Self-Organising Map (SOM) to identify noteworthy artefacts. Experimental results show that the analysis of metadata at file system and application level using the Self-Organising Map offers a good level of performance. Research shows that the proposed approach can achieve a success rate of 93%[56].

The ever-increasing volume and variety of digital data requires the automation of tasks performed by the expert. The development of ontology-based tools which are the mainstream of automation in digital forensics is a promising trend. It requires new ways of representing data and applying machine learning to find anomalies and identify patterns in digital data[57].

b) b) automatic generation of structured data

While ontology-based approaches to digital data bring real benefits in terms of searching, aggregating and combining data, their full potential depends on structured data. Therefore, one of the main challenges is to develop a solution to automatically and efficiently generate structured data from a hybrid data set. This requires a holistic approach that takes into account differences in operating systems and formats implemented in numerous devices[58].

The automation of computer forensic examinations, understood as the use of machine learning algorithms (with minimal or no expert supervision), will contribute to reducing human error, biased examinations, increasing the reliability of evidence and reducing the time taken to conduct investigations[59].

Computer forensics automation process should also include the classification of multimedia files. In order to carry out this task, it is important to define a catalogue of thematic categories as selection criteria for multimedia content.

c) c) automatic categorisation of multimedia content

Pornographic content involving minors, which is one of the main concerns of law enforcement agencies, is certainly one of the file categories recovered and secured in computer forensics60. There is a high demand

[55] Ibid, p. 1.

[56] Al Fahdi M, et al, A suspect-oriented..., op. cit., p. 1.

[57] Sikos L.F, AI in digital forensics..., op. cit., p. 8.

[58] Ibid, p. 7.

[59] Al-Dhaqm A, et al., Digital Forensics Subdomains: The State of the Art and Future Directions, *IEEE Access*. 2021, Vol 9, p. 152494.

[60] Dalins J, Tyshetskiy Y, Wilson C, Carman M.J, and Boudry D, Laying foundations

for automatic detection of pornographic content involving children, mainly due to the large amount of data and the possibility of sharing this content on the Internet[61].

A solution to the above (particularly when securing evidence at the scene of an incident) may be to automatically analyse the content of media to identify pornographic files with the participation of minors through software supported by a neural network classifier[62]. Research shows that appropriately trained neural network architectures are able to achieve a high efficiency (of around 99%) in identifying pornographic files based on their content analysis[63]. Similar effectiveness is achieved by pornographic content identification systems based solely on analysis of file names and paths. The advantage of such solutions is that they do not operate directly on the content of image and video files. Certainly, such a solution should be part of the global toolbox used in computer forensics[64].

d) d) automatic object detection

Tools allowing automatic object identification in processed multimedia files should be among solutions used in computer forensics[65]. Identifying relevant files in large datasets and searching for specific objects within them is a tedious and time-consuming task due to the large volume of media. The need for automated object detection, especially in low-quality images, is more than necessary[66]. Identification of objects may include face identification mechanisms[67], but also identification of any other object (human, car or weapon) that may be relevant to the case[68].

e) e) detection and analysis of manipulated software

Computer forensics tools should also implement solutions to automatically identify manipulated content. Counterfeit and manipulated images and videos are increasingly being used for criminal purposes. Despite the need, the implementation of these solutions is a major problem. The

for effective machine learning in law enforcement. Majura – A labelling schema for child exploitation materials, *Digital Investigation*. 2018, Vol 26, p. 1.

[61] Macedo J, Costa F, and dos Santos J.A, A Benchmark Methodology for Child Pornography Detection, [in:] 31st SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI). 2018, p. 455.

[62] Al-Nabki M.W, Fidalgo E, Alegre E, and Aláiz-Rodríguez R, File Name Classification Approach to Identify Child Sexual Abuse, [in:] Proceedings of the 9th International Conference on Pattern Recognition Applications and Methods. Malta, 2020, p. 228.

[63] Moreira D.C, Torres Pereira E, and Alvarez M, PEDA 376K: A Novel Dataset for Deep-Learning Based Porn-Detectors, [in:] 2020 International Joint Conference on Neural Networks (IJCNN). Glasgow, United Kingdom 2020, p. 6.

[64] Moreira D.C, Torres Pereira E, and Alvarez M, PEDA 376K..., op. cit., p. 16.

[65] Javed A.R, et al., A Comprehensive Survey on Computer Forensics..., op. cit., p. 11080.

[66] Brown R, Pham B, and de Vel O, Design of a Digital Forensics Image Mining System, [in:] Khosla R, Howlett R.J, and Jain L.C, (Eds), Knowledge-Based Intelligent Information and Engineering Systems, Vol 3683, Berlin, 2005, p. 397.

[67] Chaves D, Fidalgo E, Alegre E, Jáñez-Martino F, and Biswas R, Improving Age Estimation in Minors and Young Adults with Occluded Faces to Fight Against Child Sexual Exploitation, [in:] Proceedings of the 15th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications. Malta, 2020, p. 721.

[68] Javed A.R, et al., A Comprehensive Survey on Computer Forensics..., op. cit., p. 11080.

difficulties are mainly due to the lack of realistic and well-structured manipulated data sets (photos and videos) that would allow artificial intelligence models to be learned. The diversity and richness of the datasets is therefore a key element for the development of machine learning models designed to identify manipulated content and to assess their usefulness in computer forensics[69].

f) f) studying autonomous systems

In the future, there will be significant opportunities to study the AI-based systems themselves. Determining the cause of a decision made by an autonomous car, an intelligent building or a production management system will be a new area of computer forensics[70]. The concept of studying AI-based systems focuses on the elements of autonomous systems that determine the way they perform, namely the model and its main objective and the learning datasets. In the case of a dataset, the general strategy is to identify the training data that are associated with an incident and examining whether these data help to explain the incident. Another strategy is to identify unusual (anomalous) data that is unexpected. The task of the computer forensics expert will be to explore the training data set and decide whether the system based on artificial intelligence algorithms caused the incident and why it did so[71].

Discussion

Developments in information and communications technology are bound to create new crimes driven by artificial intelligence. It is highly likely that the future crime catalogue will include the offences described in this article, which are currently rated as the most disruptive to society.

When it comes to the future of cybercrime, steps should be taken to prepare law enforcement and the judiciary for new challenges. The dissemination of information about artificial intelligence and attempt to explain how it works, despite the complexity of the issue, should be the basis of current efforts undertaken in this area.

Due to the increase in AI implementation in many sectors, including, but not limited to, healthcare, education, transport, the issues of the transparency of AI-based systems and the possibility to explain how they work are essential[72].

[69] Ferreira S, Antunes M, and Correia M.E, A Dataset of Photos and Videos for Digital Forensics Analysis Using Machine Learning Processing, *Data*. 2021, Vol 6, No. 8, p. 1.

[70] Du X, et al., 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, Virtual Event, Ireland 2020, p. 8.

[71] Schneider J, and Breitinger F, AI Forensics: Did the Artificial Intelligence System Do It? Why?, arXiv:2005.13635 [cs]. *Electronic source:* http://arxiv.org/abs/2005.13635, p.4.

[72] Angelov P.P, Soares E.A, Jiang R, Arnold N.I, and Atkinson P.M, Explainable artificial intelligence: an analytical review, *WIREs Data Mining Knowl Discovery.* 2021, Vol 11, No. 5, p. 2.

In addition, the scope of activities undertaken with regard to artificial intelligence technologies should take into account specific fields of knowledge. In the case of law enforcement and justice, forensic science, in particular computer forensics, is a relevant field. It is, therefore, to be expected that the currently used tools of computer forensics will be supported by artificial intelligence. There are many areas and tasks carried out within computer forensics where artificial intelligence will be applied. These include, for example, the classification of multimedia content, the detection of objects in images and recordings or the detection and analysis of manipulated multimedia content.

This paper certainly does not cover the full catalogue of possibilities for the use of artificial intelligence in computer forensics, but it nevertheless focuses on the identified crimes of the future, which have been assessed as the most onerous, and in this respect, the potential of computer forensics have been discussed. Furthermore, the presented possibilities for the use of artificial intelligence can form the basis for further deliberations, particularly in the context of their advantages, disadvantages and risks, as well as the degree of autonomy and the extent of interference by a technician or an expert in computer forensics. Clearly, the use of artificial intelligence in computer forensics is an important issue, due to the fact that the technology in question will define new scopes of investigation which include the study of autonomous systems involving the analysis of neural network models and learning datasets.

Conclusions

The years-long backlog in digital forensics has become common in law enforcement agencies around the world. Digital forensic examiners are overwhelmed by the high number of assignments, which additionally involve the need to analyse huge amounts of data[73]. Artificial intelligence is often seen as the solution to many problems. AI-based solutions have already shown great potential in many industries and services, often outperforming human performance in terms of accuracy for a range of problems, such as image and speech recognition[74] or foreign language translations[75].

This article describes the potential use of AI-based tools in computer forensics in the context of the most likely and troublesome future crimes. The automated processing of digital evidence using AI-based techniques holds great promise for accelerating the process of examining digital evidence. The work in question confirms that computer forensics requires

[73] Du X, et al., SoK: exploring..., op. cit., p. 1.

[74] Mnih V, et al., Human-level control through deep reinforcement learning. *Nature* 2015, Vol 518, No. 7540, p. 530.

[75] Young T, Hazarika D, Poria S, and Cambria E, Recent Trends in Deep Learning Based Natural Language Processing, *arXiv:1708.02709 [cs]* 2022, p. 23. *Electronic source:* http://arxiv.org/abs/1708.02709, a*ccessed:* 25.02.2022.

the implementation of innovative methods and solutions to automate the tasks performed by the expert. The application of full automation in the examination of digital evidence, based on machine learning algorithms, can overcome the present difficulties associated with the analysis of large digital data sets.

References

7. Al-Dhaqm A, et al., Digital Forensics Subdomains: The State of the Art and Future Directions, *IEEE Access* 2021, Vol 9.
8. Al-Nabki M.W, Fidalgo E, Alegre E, and Aláiz-Rodríguez R, File Name Classification Approach to Identify Child Sexual Abuse, [in:] Proceedings of the 9th International Conference on Pattern Recognition Applications and Methods, Malta, 2020.
9. Angelov P.P, Soares E.A, Jiang R, Arnold N.I, and Atkinson P.M, Explainable artificial intelligence: an analytical review, *WIREs Data Mining Knowl Discovery* 2021, Vol 11, No. 5.
10. Bahnsen A.C, Torroledo I, Camacho L.D, and Villegas S, DeepPhish: Simulating Malicious AI. *Electronic source:* https://albahnsen.files.wordpress.com/2018/05/deepphish-simulating-malicious-ai_submitted.pdf.
11. Bairmani H.K, Al Asfer N.S.S, „Persuasion in Cyber Blackmail's Emails: A pragma-dialectical Study" 2021), *Review of International Geographical Education Online*, 11(5).
12. Basit A, Zafar M, Liu X, Javed A.R, Jalil Z, and Kifayat K, A comprehensive survey of AI-enabled phishing attacks detection techniques, *Telecommunication Systems* 2021, Vol 76, No. 1.
13. Brundage M, Avin S, Clark J, Toner H, Eckersley P, Garfinkel B, Dafoe A, et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *Electronic source*: https://doi.org/10.17863/CAM.22520.
14. Brown R, Pham B, and de Vel O, Design of a Digital Forensics Image Mining System, [in:] Khosla R, Howlett R.J., and Jain L.C, (Eds), Knowledge-Based Intelligent Information and Engineering Systems, Vol 3683, Berlin 2005.
15. Caldwell M, Andrews J.T.A, Tanay T, and Griffin L.D, AI-enabled future crime, Crime Science 2020, 9(14), p. 11.
16. Chaves D, Fidalgo E, Alegre E, Jáñez-Martino F, and Biswas R, Improving Age Estimation in Minors and Young Adults with Occluded Faces to Fight Against Child Sexual Exploitation, [in:] Proceedings of the 15th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, Malta 2020.
17. Cheng L, and Xie F, Yadong Cui (2020): Artificial Intelligence and Judicial Modernization, *International Journal for the Semiotics of Law*, 2021, Vol 34, No 1.
18. Crispino F, Weyermann C, Delémont O, Roux C, and Ribaux O, Towards another paradigm for forensic science?, *Australian Journal of Forensic Sciences,* 2021, *Electronic source*: https://wires.onlinelibrary.wiley.com/doi/epdf/10.1002/wfs2.1441.
19. Dalins J, Tyshetskiy Y, Wilson C, Carman M.J, and Boudry D, Laying foundations for effective machine learning in law enforcement. Majura – A labelling schema for child exploitation materials, *Digital Investigation,* 2018, Vol 26.
20. Dilek S, Cakır H, and Aydın M, Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review, *International Journal of Artificial Intelligence & Applications,* 6(1).
21. Du X, et al., 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, Virtual Event, Ireland 2020.
22. Fahdi M, Al, Clarke N.L, Li F, and Furnell S.M, A suspect-oriented intelligent and automated computer forensic analysis, *Digital Investigation,* 2016, Vol 18.
23. Ferreira S, Antunes M, and Correia M.E, A Dataset of Photos and Videos for Digital Forensics Analysis Using Machine Learning Processing, *Data,* 2021, Vol 6, No. 8.
24. Frank J, Eisenhofer T, Schönherr L, Fischer A, Kolossa D, and Holz T, Leveraging Frequency Analysis for Deep Fake Image Recognition, [in:] Proceedings of the 37th International Conference on Machine Learning 2020, p. 1. *Electronic source:* http://proceedings.mlr.press/v119/frank20a/frank20a.pdf.

25. Hurwitz J, Kirsch D, Machine Learning For Dummies, Hoboken, New York, 2018.
26. Iqbal S, and Abed Alharbi S, Advancing Automation, Digital Forensic Investigations Using Machine Learning Forensics, [in:] B. Suresh Kumar Shetty and Pavanchand Shetty H, (Eds), *Digital Forensic Science*, London, 2019.
27. Jasiński A, Protecting public spaces against vehicular terrorist attacks, *Czasopismo Techniczne*, 2018, No. 2.
28. Javed A.R, Ahmed W, Alazab M, Jalil Z, Kifayat K, and Gadekallu T.R, A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions, *IEEE Access,* 2022, Vol. 10.
29. Li S.-T, Kuo S.-C, and Tsai F.-C, An intelligent decision-support model using FSOM and rule extraction for crime prevention, *Expert Systems with Applications,* 2010, Vol 37, No. 10.
30. Lira Cortes A.L, and Fuentes Silva C, Artificial Intelligence Models for Crime Prediction in Urban Spaces, *Machine Learning and Applications: An International Journal*, 2021, Vol 8, No. 1.
31. Kaloudi N, and Li J, The AI-Based Cyber Threat Landscape: A Survey, *ACM Computing Surveys,* 2021, Vol 53, No. 1.
32. Kävrestad J, Fundamentals of digital forensics. Theory, methods, and real-life applications, Cham, 2020.
33. Kent K, Chevalier S, Grance T, and Dang H, Guide to integrating forensic techniques into incident response. Recommendations of the National Institute, Gaithersburg, 2006.
34. Kędzierska G, Kędzierski W, Kryminalistyka. Wybrane zagadnienia techniki, Szczytno, 2011.
35. Kim J, Shin S, Bae K, Oh S, Park E, and del Pobil A.P, Can AI be a content generator? Effects of content generators and information delivery methods on the psychology of content consumers, *Telematics and Informatics,* 2020, Vol 55.
36. King T.C, Aggarwal N, Taddeo M, and Floridi L, Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions, *Science and Engineering Ethics,* 2020, Vol 26, No. 1.
37. Lone A.H, Mir R.N, Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer, *Digital Investigation,* 2019, No. 28.
38. Lu Y, and Xu L.D, Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics, *IEEE Internet Things,* 2019, Vol 6, No. 2.
39. Macedo J, Costa F, and dos Santos J.A, A Benchmark Methodology for Child Pornography Detection, [in:] 31st SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI), 2018.
40. Matulionyte R, Australian Copyright Law Impedes the Development of Artificial Intelligence: What Are the Options?, *IIC - International Review of Intellectual Property and Competition Law,* 2021, Vol 52.
41. Mayor of London, Backlog of mobile phones and computers awaiting forensic analysis, *Electronic source:* https://www.london.gov.uk/questions/2019/12159#:%01:text=Digital%20Forensics%20currently%20have%20approximately,will%20take%20over%2012%20months.
42. Mnih V, et. al, Human-level control through deep reinforcement learning, *Nature,* 2015, Vol 518, No. 7540.
43. Moreira D.C, Torres Pereira E, and Alvarez M, PEDA 376K: A Novel Dataset for Deep-Learning Based Porn-Detectors, [in:] 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, United Kingdom, 2020.
44. Peters K.M, 21st century crime: how malicious artificial intelligence will impact homeland security, California, 2019.
45. Sahingoz O.K, Buber E, Demir O, and Diri B, Machine learning based phishing detection from URLs, *Expert Systems with Applications*, 2019, Vol 117.
46. Scanlon M, Battling the Digital Forensic Backlog through Data Deduplication, [in:] 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, 2016.
47. Schneider J,. and Breitinger F, AI Forensics: Did the Artificial Intelligence System Do It? Why?, „arXiv:2005.13635 [cs]", *Electronic source:* http://arxiv.org/abs/2005.13635.
48. Shah N, Bhagat N, and Shah M, Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention, *Visual Computing for Industry, Biomedicine, and Art,* 2021, Vol 4, No. 1.

49. Sharif M, Bhagavatula S, Bauer L, and Reiter M.K, Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition, [in:] *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Austria, 2016.
50. Sikos L.F, AI in digital forensics: Ontology engineering for cybercrime investigations, *WIREs Forensic Science*, Vol 3, No. 3.
51. Surma J, (Ed.), Hakowanie sztucznej inteligencji, Warsaw, 2020, pp. 23-34.
52. Wilner A.S, Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation, *International Journal,* 2018, Vol 73, No. 2.
53. Van der Wagen W, and Pieters W, From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks, *The British Journal of Criminology*, .Vol 55, No. 3.
54. Young T, Hazarika D, Poria S, and Cambria E, Recent Trends in Deep Learning Based Natural Language Processing, „arXiv:1708.02709 [cs]" 2022, p. 23, *Electronic source:* http://arxiv.org/abs/1708.02709.
55. Zhang C, and Lu Y, Study on artificial intelligence: The state of the art and future prospects, *Journal of Industrial Information Integration,* 2021, Vol 23.
56. Miscellanea
57. CLKP, Badania informatyczne, <Centralne Laboratorium Kryminalistyczne Badania Informatyczne. *Electronic source:* https://www.clkp.policja.pl/clk/badania-i-projekty/langnodata/badania-informatyczne/153011,Badania-Informatyczne.pdf>.
58. Raport specjalny AI@Enterprise, Praktyczne zastosowania sztucznej inteligencji w biznesie, *Electronic source:* https://www.gov.pl/attachment/3975e783-a888-4417-a562-5ecd453d7625*, accessed:* 15.02.2022.

DOI: 10.5604/ 01.3001.0053.7217
http://dx.doi.org/ 10.5604/ 01.3001.0053.7217

Keywords: Artificial intelligence, machine learning, computer forensics, forensic science, digital evidence, crime

Summary: The aim of this article is to discuss the role, tasks and challenges of computer forensics in the context of the development of AI-enabled crime. The issues described in the article refer to potential future threats that have been identified as the most troublesome for society. The considerations in the article are preceded by a critical analysis of the research that has been conducted in the field of artificial intelligence and computer forensics so far. The literature analysis allows the claim that the future of computer forensics is automation based on machine learning algorithms. It has also been concluded that the development of artificial intelligence will define new areas of computer forensics that take into account the analysis of neural network models and learning datasets.

Palabras clave: Inteligencia artificial, aprendizaje automático, investigación informática forense, evidencias digitales, delincuencia

Resumen: El objetivo de este artículo es discutir el papel, las tareas y los desafíos de la informática forense en el contexto del desarrollo de la criminalidad apoyada por la inteligencia artificial. Las cuestiones descritas en el artículo se basan en las posibles amenazas futuras que se han identificado como las más intratables para la sociedad. Las consideraciones contenidas en el artículo fueron precedidas por un análisis crítico de la investigación existente en el campo de la inteligencia artificial y la informática forense. El análisis bibliográfico realizado permite afirmar que el futuro de la informática forense es la automatización basada en algoritmos de aprendizaje automático. También se concluye que el desarrollo de la inteligencia artificial definirá nuevas áreas de investigación informática forense, fueron análisis de modelos de redes neuronales y conjuntos de datos de aprendizaje.