






# The Use of Machine Learning in Digital Forensics: Review Paper

Yusra Al Balushi<sup>(✉)</sup> , Hothefa Shaker , and Basant Kumar 

Modern College of Business and Science, 3 Bawshar St, Muscat 133, Oman  
{20202196,hothefa.shaker,basant}@mcbs.edu.om

**Abstract.** With the increase of cybercrimes in the current years, digital forensics has become an important matter to study in order achieve quality evidence. Forensic investigators face difficulties with data collection and analysis to reconstruct events. Due to humans' immense interaction on a daily basis, machine learning allows investigators to perform more effective and efficient investigations using various algorithms. Machine learning is a subset of the artificial intelligence field. It is a scientific discipline focusing on developing computer models and algorithms that can perform specific tasks without programming, such as dataset training and testing, and it's potential to aid in investigations. This paper reviews various machine learning techniques that examine and analyze digital evidence during the investigation process. Each machine learning algorithm works on a specific area of digital forensics based on the features, it overcomes complexity, data volume, time-lining, correlation, consistency, etc. moreover, this study compares machine learning algorithms in terms of standard criteria.

**Keywords:** Digital Forensics · Machine learning Algorithms · Investigation · Digital Evidence · Swarm Intelligence

## 1 Introduction

Digital forensics (DF) is a process utilized to analyze and present digital evidence gathered from various sources such as databases, computers, and digital images [1]. The increasing number of smart devices in our daily life results in a wide variety of data, with different categories and characteristics. The digital forensics investigation process collects and analyzes data to help investigators identify and prevent unauthorized access to the collected information [2]. In most cases, the data and evidence collected from a device can be deleted after the crime has occurred. This process is very important for investigators as it can help them determine the exact nature of the crime, and identify the victims [3]. Unfortunately, insufficient human resources to perform a thorough investigation can take a long time.

Although many techniques can be used to manage the massive amount of data collected by a digital forensics investigator, such as Hadoop, they do not function

as efficient as the human brain. Instead, investigators use a machine learning (ML) to analyze and collect data efficiently [4]. This system can learn from various examples and experiences and decide based on the data [5]. It contains different algorithms such as Support Vector Machine (SVM), Decision Tree (DT), K-Means, K-Nearest Neighbor (KNN), Naïve Bayes (NB), Principal Component Analysis (PCA), Logistic Regression (LR), Singular Value Decomposition (SVD) and Apriori. Each algorithm is responsible for a specific task like extracting features, classifying network attacks, detecting manipulated images, etc. [6].

This paper is organized as follows: Sect. 2 provides an overview of digital forensics and machine learning, followed by the proposed machine learning algorithms used in digital forensics in Sect. 3. Section 4 discuss the limitations of machine learning algorithms in digital forensics.

## 2 Digital Forensics and Machine Learning

Digital forensics is a branch of science that focuses on analyzing and preserving the data that's collected and stored in various forms of media. Although its roots can be traced back to the 1980s, the field's evolution was accelerated during the 1990s with the emergence of multi-user, multi-tasking, and wide-area networks [7]. Due to the rise of cyber threats and attacks, it has become one of the most critical areas of security. Machine learning is a branch of artificial intelligence focusing on developing computers that can learn from data. This technology is commonly used in the areas of data mining and analysis, as well as in the prediction of future behavior [8]. This section describes the digital forensics challenges, models, and investigation stages and also explains different machine learning algorithms.

### 2.1 Digital Forensics

The discipline of digital forensics is a branch of criminalistics that focuses on the legal procedures related to analyzing and protecting digital information. It involves identifying and extracting information from various sources. After that, it can be used to evaluate the data in a civil or a criminal trial [9]. This process involves using scientific and technological methods to analyze the data that various digital objects have created [10]. Digital forensics is a process that aims to collect evidence that can be used to determine the facts surrounding an incident. The 5WH questions are commonly asked in investigations, such as who was involved, where the incident occurred, and how and when it happened. The answer to these questions and assists the investigators in confirming the incident [11].

**A. Digital Forensics Investigation Process.** According to the National Institute of Standards and Technology, the four procedures and methodologies used in the digital forensics process are designed, as shown in Fig. 2, to help organizations understand the significance of their investigations. They can be

performed in different ways depending on the complexity of the study [12]. Due to the rise of digital technology, there has been an increase in the number of data sources that can be collected. Figure 1 illustrates the digital forensics investigation process. Each stage is explained below.

*a) Data Collection:* The first stage in conducting an investigation, is identifying the potential sources of this data. Usually, the data is collected from laptops, desktops, and servers. In addition to traditional sources, analysts should consider other data sources when analyzing an organization’s operation. For instance, they can gather information about an organization’s activities through the logs of its Internet service provider [13].

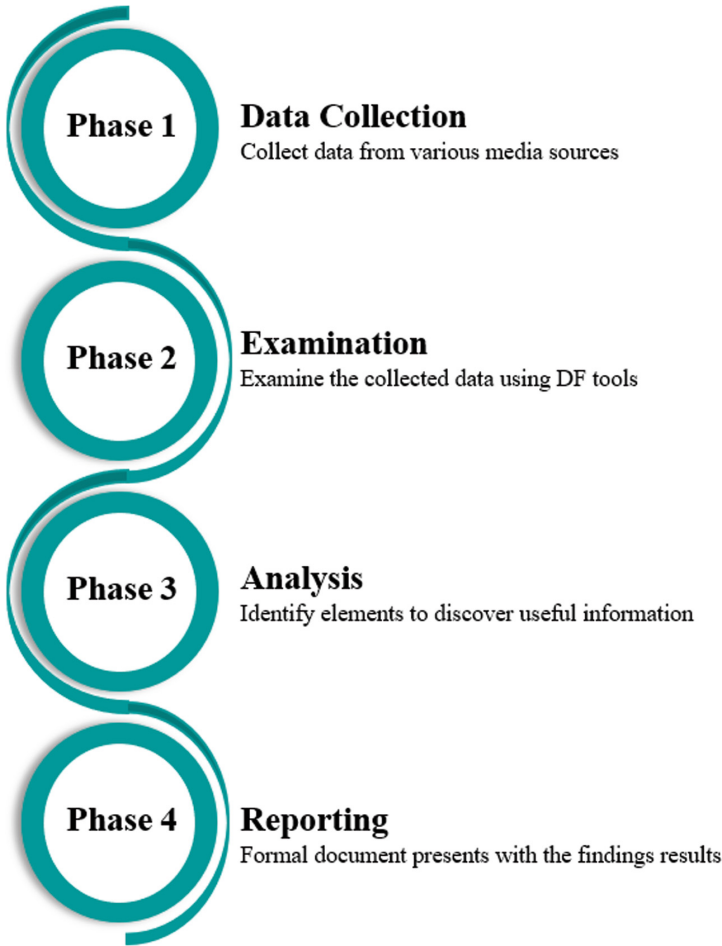


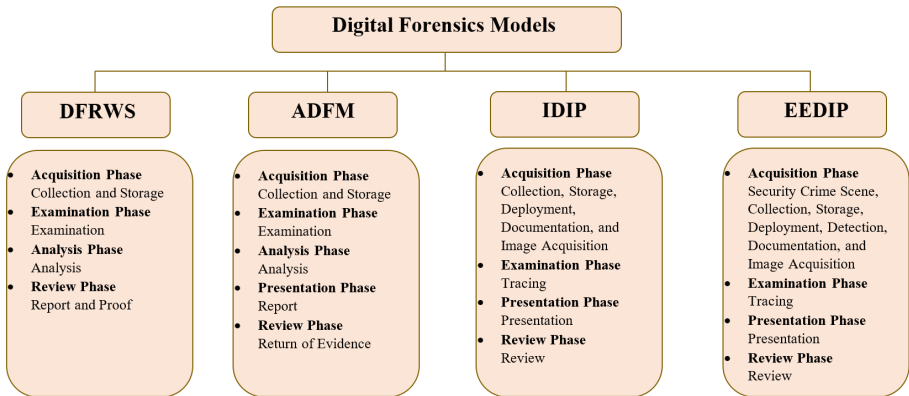
Fig. 1. Digital Forensics Investigation Process

*b) Examination:* The second stage aims to examine the data that has been collected. Through the use of digital forensics techniques and tools, the necessary pieces of information from the data are extracted. Moreover, defining the data files that contains information of interest, including information concealed through file compression, access control, and encryption [13,14].

*c) Analysis:* An analysis is a process that involves carrying out scientific procedures in a scientific setting to produce elements such as identifying people, places, and events, as well as determining how these elements are related [15]. This process involves analyzing data collected from various sources. For instance, an IDS log may contain information about a specific user, while audit logs may include details about a particular host, with the help of tools such as security event management software, it can be easy to correlate and gather data [14].

*d) Reporting:* The final phase of the investigation is reporting, this step involves analyzing the data collected during the analysis phase and presenting the findings to the analyst in a formal documentation. It can be challenging to determine the cause of an event or provide an accurate explanation, however, by gathering information from the data, an analyst can improve their understanding of the event and to also prevent any recurrence in the future [15].

**B. Digital Forensics Models.** Digital Forensics has several investigation models, such as Digital Forensics Research Workshops Model (DFRWS), Abstract Digital Forensics Model (ADFM), Integrated Digital Investigation Process Model (IDIP), and End-to-End Digital Investigation Process Model (EEDIP) [16]. Each model is designed for a specific phase and activity. Figure 2 illustrates the digital forensics models with the related activities.



**Fig. 2.** Models of the Digital Forensics

**C. Threads of the Digital Forensics.** The increased number of digital devices has continuously challenged the development of digital forensics. The complexity of the hardware, software platforms, and smartphones that use encryption poses an immense challenge in collecting digital evidence. This has resulted in the need for new strategies and methods to address the challenges faced by the industry. According to Montanari et al., the increasing variety of file formats and operating systems hampers the International Journal of Organizational and Collective Intelligence from developing standardized digital forensics tools, and processes [17]. Due to the increasing complexity of digital technology, the amount of data that can be collected and analyzed has become more challenging. With new data formats, such as the low binary, it is now possible to collect and analyze large volumes of data [18].

Based on Horsman et al., complexity is another challenge. As the data collected increases, developing tools that can analyze the data collected quickly becomes more challenging. Furthermore, lack of standardization in the formatting and storage of digital evidence is also a significant issue. It is challenging to share digital proof. This issue could affect the efficiency of investigations by having a standardized set of procedures; law enforcers could exchange information more effectively [19].

According to Quick et al., correlation and consistency are the biggest challenges when developing digital analysis tools. Since the evidence is collected from different sources, the data must be analyzed and correlated correctly. This can be time-consuming and drain an investigation's resources [20].

Pandey studied those digital forensics professionals face the time-lining challenge, which occurs when multiple sources provide conflicting interpretations of the data. This issue can affect the efficiency of an investigation. The lack of knowledge about the latest digital forensics tools is also a significant issue that threatens the development of the industry and data accuracy. Due to the rapid evolution of forensic science, the individuals working in the field must be equipped with the necessary skills to use the new technology effectively. This issue can prevent the development of new digital [21].

## 2.2 Machine Learning

One of the most common approaches to artificial intelligence (AI) is machine learning, which allows systems to learn and analyze without requiring additional training [22]. It can automatically classify and predict inputs it has received [23]. This technology can use appropriate algorithms in various areas, such as security and fraud detection. Machine learning is divided into four main categories: supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning. The supervised learning process examples are mapping an input to an output. It takes advantage of training data labeled with various training examples. Regression and classification are the most popular techniques used in this process [24]. Unsupervised learning, known as the clustering technique, can help identify the hidden structures and patterns within the datasets [25]. While semi-supervised learning is a type of machine learning that focuses on

using unlabeled and labeled data to perform various activities. It is between unsupervised and supervised learning [26]. Reinforcement learning focuses on rewarding behaviors and punishing those who are not good enough, it can solve problems or control certain situations [27]. These algorithms are described as follows:

**A. Support Vector Machine Algorithm.** Support Vector Machine can handle both regression and classification problems. SVM uses the examples within the training data set to classify the objects, it can take structured and semi-structured data and perform complex functions depending on the kernel function. This method considers the number of features in each data item and then identifies a hyperplane that splits them into two classes. It minimizes errors while maximizing the marginal distance between the two classes [28].

**B. Decision Tree Algorithm.** A decision tree is a learning method that can be used for both the regression and classification of tasks. It is easy to interpret and can correspond outcomes from tests to the classification of data items. A decision tree model considers the various decision logic and models them into a tree-like structure. The topmost node in a DT tree which is called the root node. The internal nodes of a decision tree represent tests related to the input variables or attributes. After completing the test, the classification algorithm branches to the appropriate child node. This process continues until the leaf node is ready to decide [29].

**C. K-Nearest Neighbor Algorithm.** The K-Nearest Neighbors algorithm is a non-generalizing learning method that doesn't focus on creating a general model. It stores all instances of training data in an n-dimensional space. It uses data to classify new data points, the K-Nearest Neighbors algorithm can perform various tasks such as regression and classification that handle data training to provide accurate data based on the quality of data [30].

**D. Naïve Bayes Algorithm.** Naïve Bayes is an unsupervised learning algorithm used in classification or clustering tasks. It does not require specification of an outcome and can be implemented as a method for creating clusters [31]. The algorithm requires only a small amount of training data to estimate the necessary parameters. Nave Bayes relies on both the target and input variables, making it a supervised learning technique. As a classifier, it produces a tree composed of Bayesian networks, which are tree models based on outcome probabilities [32].

**E. K-Means Algorithm.** K-Means is a simple and efficient method to classify datasets into K centers. It can be compared to hierarchical clustering because it is more efficient when the variables are significant. Therefore, the efficient elements in this algorithm are the implementation and data interpretation [30].

**F. Principal Component Analysis Algorithm.** The principal component analysis is a procedure that takes into account the observations of various possible correlated variables and converts them into linearly uncorrelated values. It can be performed quickly and simply by implementing an algorithm known as the Orthogonal Transformation. This eliminates the need for a prior information within the computation of the model. In addition to data clustering and classification, PCA provides various other features, such as data feature classification and estimation [33].

**G. Logistic Regression Algorithm.** A logistic regression model is used in machine learning to solve classification problems. It helps in identifying which class is associated with a given instance. Since it is a probability, the model outcome is between zero and one. So, it is possible to use it as a binary classifier [34].

**H. Singular Value Decomposition Algorithm.** The concept of the factorization method known as SVD is widely used in matrixes. The SVD algorithm provides a low-dimensional representation of a high-dimensional data-set by considering the dominant patterns. This method is mainly based on data collected without requiring knowledge or intuition. Invariance features can be extracted using singular values, and the decomposition method can be used from an image, or a signal [35].

**I. Apriori Algorithm.** The Apriori algorithm is widely used in data mining and finds the relationships between various data-sets. It frequently mines item sets using the candidate generation method. It is also designed to perform well in a database with several transactions. However, it's performance could degrade due to various factors, one is the requirement for "n" numbers of frequent item sets in the database scans [36].

## 2.3 Swarm Intelligence

The concept of swarm intelligence refers to the algorithms that are inspired by the habits of various animals in nature. Some of the most prominent examples of this type of metaheuristics include the optimization of artificial bee colonies and particle swarm optimization [37]. The metaheuristic approach has been extensively utilized in developing various computational models and algorithms designed to address the complexity of real-world problems in mathematics, statistics, and blockchain. Some of these include the optimization of artificial neural networks tasks [38]. A review of the literature shows that although the metaheuristic approach has been widely utilized in developing various computational models and algorithms, the swarm intelligence techniques needed to be used more to improve the performance of machine learning models. This is surprising, as the methods have been successfully used in other research areas. One of

the most successful applications of this type of metaheuristics is a pair of algorithms designed to improve the efficiency of Extreme Learning Machine (ELMs) tasks [39].

An adequate number of neurons is required in the hidden layer to achieve fast convergence and good performance when implementing an unsupervised learning algorithm. The difference between traditional machine learning models and ELMs is that while using gradient-descent techniques, the latter uses randomly allocated bias and input weight values [40]. This approach avoids some of the issues commonly occurring with the gradient-descent method. These include the iterative tuning of the bias and weight values and the slowing down of the convergence speed. Despite this, the number of neurons that make up the hidden layer remains an open question for ELMs [41].

### 3 Machine Learning in Digital Forensics

Machine learning plays a role in cybersecurity and digital forensics. Digital forensics investigators use machine learning algorithms to analyze vast amounts of data sets stored in various cloud computing environments and networks [42]. These data sets can then be used to predict the behavior of their users. In addition, these algorithms can also perform pattern recognition. Through the use of machine learning techniques, investigators apply a set of rules and methods that can be used to find interesting data patterns to identify potential criminal activity. This section describes several algorithms proposed to discover digital evidence and improve the investigation process.

#### 3.1 Support Vector Machine Algorithm in Digital Forensics

Islam et al. proposed a model that can detect copy-move and splice attacks in color images using local binary pattern (LBP) and discrete cosine transformation (DCT) operators. The proposed system was evaluated using the SVM kernel. The DCT and LBP operators capture the changes in the local frequency distribution and detect micro-patterns. The proposed method considers the inter-cell values of the LBP blocks and arranges them as feature vectors. The resulting images are then classified into authentic and tampered ones using the SVM and radial basis function (RBF). The study results show that the proposed method is well-suited for image forgery detection and accuracy metrics [43].

Barni et al. proposed a system that can detect contrast enhancement using an adaptive histogram in JPEG compression. This method is based on the color SPAM features of an SVM detector. It can then be trained to recognize JPEG-compressed images with enhanced contrast. The researchers tested the systems performance by training it against a set of JPEG-compressed images with different quality factors (QFs). It only works well if the QF used matches the one used in the test and the QFs are more extensive than 80 [44]. The proposed system can be applied to multimedia analysis forensics.



Ferreira et al. proposed a method to distinguish between fake and genuine digital photos and videos. It uses an SVM-based method to extract the features from the data collected by a discrete fourier transform (DFT) calculation. Using the Scikit-Learn library in Python 3.9, the SVM processing could create a classification model for the generated data. This model then predicts the photos in the testing dataset. A set of Python programs were designed to process photos' features and extract frames from videos. They were also used to create an SVM model that can be used to classify images. The proposed model is based on two modules for Autopsy. The DFT-SVM algorithm was used to analyze the photos and videos, and the result shows that it takes less time to perform the analysis than convolutional neural network (CNN) [45]. The DFT-SVM method's low processing time and high performance make it an ideal tool for detecting fake multimedia content in the digital forensic analysis phase. The study results were auspicious and followed the same procedure as previous studies [46].

### 3.2 Decision Tree Algorithm in Digital Forensics

Chhabra et al. proposed an architectural framework that combines the MapReduce framework, the Hadoop Distributed File System, and the decision tree algorithm. The proposed framework handled the vast amount of data that can be collected and stored. It consists of four steps: capturing network traffic, converting it into a human-readable format, filtering packets, analyzing the data for malicious activities, and finally, presenting a threat analysis and visualization. A decision tree labels malicious and non-malicious traffic, improving accuracy and time efficiency in each phase. The study's results revealed that the model could detect 99% of all malicious and non-malicious traffic [47].

In 2021, a hybrid approach was proposed by Usman et al. to address the issues related to the IP reputation system by combining the capabilities of various data forensics techniques such as machine learning, Dynamic Malware Analysis, and Cyber Threat Intelligence. Using big data forensics, it can predict the likelihood of a particular attack happening before it occurs and then classifies it according to its behavioral characteristics. The proposed system was evaluated against various existing reputation systems using multiple ML techniques such as DT, SVM, and NB. The DT performed well in the recall, F-measure, and precision scores [48].

### 3.3 K-Nearest Neighbor Algorithm in Digital Forensics

Kachavimath et al. presented a framework for analyzing and detecting distributed denial of service attacks using the K-Nearest Neighbor and naive Bayes algorithms. The method utilizes statistical techniques to improve the detection performance of anomalous network traffic. The KNN algorithm is based on the statistical features of the KDD Cup 99 and network security laboratory (NSL-KDD) data-sets. Compared to the Naive Bayes algorithm, the KNN algorithm performs better in accuracy, recall, and precision [49].

Barra et al. proposed a method for gender classification consisting of three steps: data extraction, feature creation, and selecting the best classifiers, the first step involves extracting body keypoint sequences, followed by the design of body features using OpenPose. The second step requires training four different classifiers: the K-Nearest Neighbors, Adaptive Boosting, Random Forest, and Support Vector. The most accurate method to determine gender, even in the dark is the Random Forest followed by K-Nearest Neighbors [50].

### 3.4 Naïve Bayes Algorithm in Digital Forensics

Yudhana et al. analyzed the data collected from the network traffic log to identify the accuracy of the distributed denial of service attack. Through the Wireshark application, they collected network traffic datasets and extracted network features to identify patterns in the data. After that, they performed a network package classification procedure using the Naive Bayes algorithm and trained it using several neurons using via Neural Network algorithm. The analysis and testing revealed that the neural network had an accuracy of 95.2381% while the Naive Bayes had an accuracy of 99.999%. The researchers believe that using artificial neural networks and the Naive Bayes algorithm in network forensics can help improve the accuracy of the results during investigations [51].

### 3.5 K-Means Algorithm in Digital Forensics

Sudha et al. developed a framework that uses the K-Means algorithm to analyze the data collected from various sources. The data collected from multiple forms of cybercrime analysis can be easily sorted, to make it easier to extract the features. In the Clustering stage, the K-means algorithm detects the interactions between features. The proposed method can then provide actionable steps to prevent these types of crimes from reoccurring in the future [52].

Ruriawan et al. developed a system that can identify digital evidence and classify the contents of storage media using the K-Means clustering algorithm. The classification system for digital evidence is split into two parts: the digital evidence collector and the digital evidence file. The duplicator will then copy and store the user's specified data. The proposed system can be used to recover files stored in the media. This system is used to help forensic investigators prepare the related evidence more efficiently [53].

### 3.6 Principle Component Analysis Algorithm in Digital Forensics

Roy developed a digital forensic framework to analyze the source and origin of an image. The framework was able to classify it using random forest. The main advantage of this feature is that it allows investigators to identify the multiple camera sources that produce different JPEG compression artifacts. The framework also improved its classification accuracy by implementing the PCA algorithm. This method was used to drastically reduce the dimensionality of the features [54].

### 3.7 Logistic Regression Algorithm in Digital Forensics

Ali et al. identified the types of malware commonly encountered in the Windows operating systems that target the registry. Malware can cause a loss of precious time during the investigation process. They provided valuable insight into how these types of malware interact with the registry. The researchers tested different classifiers, such as the Neural Network, the Decision tree, and the Logistic regression. The results of their study revealed that it is possible to perform digital forensics analysis using modified timestamps and ML techniques. The authors identified the 47 locations in the registry commonly targeted by malware. The researchers determined that the Boosted tree correctly classified over 72% of the malware through their study. This method allows investigators to quickly identify which type of malware is present and which isn't [55].

Hina et al. proposed a multi-label approach that can be used to organize and analyze emails. This method can help conduct forensic investigations related to the illegal use of email. This approach is implemented in stages: data pre-processing, which involves removing the most repeated words in a sentence such as "we", "am,", etc. Then, various machine-learning techniques extract regular email features from harmful emails, based on the experimental result, the Logistic Regression algorithm performed better than the other machine learning techniques regarding the accuracy and analyzing email classification [56].

### 3.8 Singular Value Decomposition Algorithm in Digital Forensics

Ahmed et al. proposed a new method for detecting copy-move forgery based on the singular value decomposition and the Kolmogorov-Smirnov test. It involves extracting image features from various blocks using a steerable pyramid then the original blocks' indices are stored with feature vectors, which correspond to the pixel's corresponding features. Four processing techniques are examined in digital image forensics: brightness adjustment, contrast adjustment, image blurring, and color reduction. The proposed method performed well regarding its recall, precision, and F1\_score. For brightness adjustment, it scored at 95%, while for image blurring, it was at 77.5%, 82.7%, and 75% [57].

Varghese et al. proposed an algorithm to detect a copy-move forgery in images by extracting features from each block through a combination of singular value decomposition and discrete orthonormal Stockwell transform. The resulting features are lexicographically sorted and can be distinguished from other images by two threshold values. According to the simulations, the proposed algorithm is more robust and invariant than other state-of-the-art techniques for detecting copy-move forgery. It also performed well in various operations, such as rotation, with a high accuracy rate [58].

Tuncer et al. proposed a method that can be used to classify different types of malware and develop an effective anti-malware model. The proposed method utilizes a local binary pattern (LBP) and SVD to extract features and reduce their complexity using PCA. Based on the LBP-SVD-LTPNet framework, the proposed method achieved an 88.08% success rate. It performed better than the deep learning methods in terms of accuracy [59].

### 3.9 Apriori Algorithm in Digital Forensics

Huan et al. developed a mobile forensics system using the Apriori and K-means algorithms. The Apriori algorithm improves the mining efficiency using mining rules in two parts: generating frequent item sets and extracting the rules that meet the minimum confidence requirement. Furthermore, it enhances the intimacy of the database by using a vertical structure to represent the data. The clustering results are classified according to the relationship between the various individuals. The researchers used the association rules to analyze the data. They found that the high confidence rules indicate that the user's daily habits are consistent with the characteristics of the data [60] (Table 1).

**Table 1.** Summary of Machine Learning Algorithms in Digital Forensics Investigation

Focused Area	ML Algorithm	Forensic Type	DF Phase	Advantage	Disadvantage
Copy-move and splice attacks [43]	SVM	Image forensics	Examination	High accuracy and trained both semi-structured and structured dataset	Less performance on overlapping images
Contrast enhancement and identify JPEG-Compressed image [44]	SVM	Image forensics	Examination	Fast data analysis	The detector (QF) work well in a specific QF only
Detect manipulated videos and photos [45,46]	SVM	Image and video forensics	Analysis	High accuracy	Required more processing time
Labelled malicious and non-malicious traffic [47]	DT	Network forensics	Analysis	Accurate data and time efficiency	Complex calculation
Classify attack behavioural [48]	DT, SVM and Naive Bayes	Network forensics	Analysis	High performance on unknown samples and reduces security issues	Long time to train
DDoS attack [49]	KNN, Naive Bayes	Network forensics	Examination and analysis	Flexible classification	Lazy learner and not working with another attack rather than DDoS Attack
Gender classification [50]	RF, KNN, RF, AB, SVM	Video forensics	Examination and analysis	High accuracy in the dark videos	Low performance on the prediction stage
DDoS attack [51]	Naive Bayes	Network forensics	Analysis	Simplicity	Zero-frequency problem
Features classification [52]	K-Means	Network forensics	Examination and analysis	High accuracy rate	Set K value in advance
Identify and recover digital evidence [53]	K-Means	File system/memory forensics	Analysis	Discover hidden evidence	Low performance on the noisy dataset
Determine image source [54]	PCA, RF	Image forensics	Examination	Improve accuracy and reduce the dimensionality of the features	Loss of data if the components are not set correctly
Determine malware location in Windows Registry [55]	LR, DT	Malware forensics	Analysis	Possible to build it into existing forensic tools without requiring frequent updates	Used for prediction feature
Email classification [56]	LR, SVM, RF, DT	Email forensics	Analysis	High accuracy with bi-gram features	Each variable requires a minimum of 10 data points
Image falsification [57]	SVD	Image forensics	Examination and analysis	High precision	Reduce the block size on the low-quality image
Extract features for copy-move forgery in images [58]	SVD	Image forensics	Analysis	High performance and less computational	-
Anti-malware framework for forensics analysis [59]	SVD, PCA	Malware forensics	Examination and analysis	High accuracy	Not understanding data transformation
Mobile forensics application [60]	Apriori, K-Means	Mobile forensics/database forensics	Analysis	High confidence and improve data mining efficiency	Required further resources

## 4 Machine Learning Limitations in Digital Forensics

The lack of model transparency and testing methodologies is a significant issue that affects the development and implementation of machine learning models. Research labs often create new models that can be quickly implemented in real-world applications but can also fail in these instances. Having the tools and resources to reproduce models can help various industries and professionals solve their problems faster, it can also help prevent them from experiencing issues such as bias, unfortunately, many machine learning models must be designed to provide forensic practitioners with the necessary transparency and testing methods. This issue can prevent them from effectively explaining different outputs via their systems [61].

One of the most significant issues with deep learning algorithms is their interpretability, this is because machine learning models can be compelling but also powerless if they can't be adequately interpreted. Therefore, it is essential that they can be applied in real world scenarios [62].

Various techniques such as clustering, decision tree, and support vector machine are used to analyze and predict the anonymous behavior of users in big data. Due to the complexity of neural networks, they must have the necessary training data to properly perform their functions. As their architecture grows, so does their data requirement, this means that reusing the data will not produce desirable results. Existing reputation systems can be problematic due to their limited ability to detect zero-day anomalies, reliance on internal sources, and high management costs. The lack of data sources and quality data is a significant issue that needs to be resolved. Although having enough information is sometimes the same as not having it, providing poor-quality data can affect the accuracy of a model [63].

The advantages of trusting computer algorithms are numerous. Humans greatly benefited from their ability to automate processes and analyze vast amounts of data. Unfortunately, they can also be subject to bias, and since algorithms are made and trained by humans, it's tough to remove bias, even though, who should be held accountable if something goes wrong? Despite the immense advantages of machine learning, it is still far from perfect, and in the future, we will have to develop a framework that will allow people to trust computer algorithms [64]. Table 2 shows some of limitations in ML algorithms.

**Table 2.** Machine Learning Algorithm Limitation

ML Algorithm	Limitation
SVM algorithm	Not applicable for huge datasets
DT algorithm	Not adequate for solving regression issues
KNN algorithm	Less effective with large date sets and high number of dimensions
K-Means algorithm	Specify the K value from the beginning

## 5 Conclusion

The digital forensics domain has grown in many aspects. Forensic analysts have proven many difficulties they face in each case to analyze big data, such as images, video, etc., that may assist in revealing events. Over time, some new challenges are emerging in digital forensics. This led to the use of automation and intelligent techniques that facilitate the work of investigators. This research has validated various ML algorithms to solve digital forensic challenges, e.g., SVM, KNN, DT, PCA, SVD, K-Means, NB, ANN, LR and RF. Algorithms categorize authentic data from fake ones for evidence in court. Finally, the paper summarized the best practice for each algorithm in digital forensics according to its features, advantages, and disadvantages. Based on the proposed research papers, K-Means focuses on recovering removed digital evidence from memory locations. The SVM, PCA, and SVD are the best possible practices to be implemented in an image forensics investigation, while the KNN and NB support network forensics. Machine learning developers have made significant progress in making these systems think like humans in the past few years. They now perform complex tasks and make decisions based on in depth analysis. While progress has been made, machine learning still has many limitations such as ethical aspects, lack of interpretability, insufficient data to train machines and lack of reproducibility.

## References

1. Joakim Kävrestad. *Fundamentals of Digital Forensics*. Springer, 2020.
2. Konstantinos Karampidis, Ergina Kavallieratou, and Giorgos Papadourakis. A review of image steganalysis techniques for digital forensics. *Journal of information security and applications*, 40:217–235, 2018.
3. Graeme Horsman. Tool testing and reliability issues in the field of digital forensics. *Digital Investigation*, 28:163–175, 2019.
4. Godson Kalipe, Vikas Gautham, and Rajat Kumar Behera. Predicting malarial outbreak using machine learning and deep learning approach: a review and analysis. In *2018 International Conference on Information Technology (ICIT)*, pages 33–38. IEEE, 2018.
5. Anand Handa, Ashu Sharma, and Sandeep K Shukla. Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 9(4):e1306, 2019.
6. R Saravanan and Pothula Sujatha. A state of art techniques on machine learning algorithms: a perspective of supervised learning approaches in data classification. In *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, pages 945–949. IEEE, 2018.
7. Athanasios Dimitriadis, Nenad Ivezic, Boonserm Kulvatunyong, and Ioannis Mavridis. D4i-digital forensics framework for reviewing and investigating cyber attacks. *Array*, 5:100015, 2020.
8. Sana Qadir and Basirah Noor. Applications of machine learning in digital forensics. In *2021 International Conference on Digital Futures and Transformative Technologies (ICoDT<sup>2</sup>)*, pages 1–8. IEEE, 2021.

9. Stefania Costantini, Giovanni De Gasperis, and Raffaele Olivieri. Digital forensics and investigations meet artificial intelligence. *Annals of Mathematics and Artificial Intelligence*, 86(1):193–229, 2019.
10. Eoghan Casey. *Handbook of digital forensics and investigation*. Academic Press, 2009.
11. Owen Defries Brady. *Exploiting digital evidence artefacts: finding and joining digital dots*. PhD thesis, King’s College London, 2018.
12. Karen Kent, Suzanne Chevalier, and Tim Grance. Guide to integrating forensic techniques into incident. *Tech. Rep. 800-86*, 2006.
13. Flora Amato, Aniello Castiglione, Giovanni Cozzolino, and Fabio Narducci. A semantic-based methodology for digital forensics analysis. *Journal of Parallel and Distributed Computing*, 138:172–177, 2020.
14. Karen Kent, Suzanne Chevalier, and Tim Grance. Guide to integrating forensic techniques into incident. *Tech. Rep. 800-86*, 2006.
15. Stefania Costantini, Giovanni De Gasperis, and Raffaele Olivieri. Digital forensics and investigations meet artificial intelligence. *Annals of Mathematics and Artificial Intelligence*, 86(1):193–229, 2019.
16. Gurpal Singh Chhabra, Varinder Pal Singh, and Maninder Singh. Cyber forensics framework for big data analytics in iot environment using machine learning. *Multimedia Tools and Applications*, 79(23):15881–15900, 2020.
17. Reza Montasari, Richard Hill, Simon Parkinson, Pekka Peltola, Amin Hosseinian-Far, and Alireza Daneshkhan. Digital forensics: challenges and opportunities for future studies. *International Journal of Organizational and Collective Intelligence (IJOICI)*, 10(2):37–53, 2020.
18. Darren Quick and Kim-Kwang Raymond Choo. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, 11(4):273–294, 2014.
19. Graeme Horsman and James R Lyle. Dataset construction challenges for digital forensics. *Forensic Science International: Digital Investigation*, 38:301264, 2021.
20. Quick D& Choo K-KR. Impacts of increasing volume of digital forensic data. *Digit. Investig.*, 11:273–294, 2014.
21. Abhishek Kumar Pandey, Ashutosh Kumar Tripathi, Gayatri Kapil, Virendra Singh, Mohd Waris Khan, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. Current challenges of digital forensics in cyber security. *Critical Concepts, Standards, and Techniques in Cyber Forensics*, pages 31–46, 2020.
22. Nasrin Sultana, Naveen Chilamkurti, Wei Peng, and Rabei Alhadad. Survey on sdn based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, 12(2):493–501, 2019.
23. Devanshi Dhall, Ravinder Kaur, and Mamta Juneja. Machine learning: a review of the algorithms and its applications. *Proceedings of ICRIC 2019*, pages 47–63, 2020.
24. Iqbal H Sarker, ASM Kayes, and Paul Watters. Effectiveness analysis of machine learning classification models for predicting personalized context-aware smart-phone usage. *Journal of Big Data*, 6(1):1–28, 2019.
25. Ansam Khraisat, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2(1):1–22, 2019.
26. Jesper E Van Engelen and Holger H Hoos. A survey on semi-supervised learning. *Machine Learning*, 109(2):373–440, 2020.
27. Zhe Wang and Tianzhen Hong. Reinforcement learning for building controls: The opportunities and challenges. *Applied Energy*, 269:115036, 2020.

28. Shahadat Uddin, Arif Khan, Md Ekramul Hossain, and Mohammad Ali Moni. Comparing different supervised machine learning algorithms for disease prediction. *BMC medical informatics and decision making*, 19(1):1–16, 2019.
29. Iqbal H Sarker. Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science*, 2(3):1–21, 2021.
30. Susmita Ray. A quick review of machine learning algorithms. In *2019 International conference on machine learning, big data, cloud and parallel computing (COMIT-Con)*, pages 35–39. IEEE, 2019.
31. Mei Sze Tan, Siow-Wee Chang, Phaik Leng Cheah, and Hwa Jen Yap. Integrative machine learning analysis of multiple gene expression profiles in cervical cancer. *PeerJ*, 6:e5285, 2018.
32. Joshua P Parreco, Antonio E Hidalgo, Alejandro D Badilla, Omar Ilyas, and Rishi Rattan. Predicting central line-associated bloodstream infections and mortality using supervised machine learning. *Journal of critical care*, 45:156–162, 2018.
33. Loong Chuen Lee and Abdul Aziz Jemain. On overview of pca application strategy in processing high dimensionality forensic data. *Microchemical Journal*, 169:106608, 2021.
34. Lian Niu. A review of the application of logistic regression in educational research: Common issues, implications, and suggestions. *Educational Review*, 72(1):41–67, 2020. A review of the application of logistic regression in educational research: Common issues, implications, and suggestions. *Educational Review*, 72(1):41–67, 2020.
35. Steven L Brunton and J Nathan Kutz. *Data-driven science and engineering: Machine learning, dynamical systems, and control*. Cambridge University Press, 2022.
36. M Sornalakshmi, S Balamurali, M Venkatesulu, M Navaneetha Krishnan, Lakshmana Kumar Ramasamy, Seifedine Kadry, Gunasekaran Manogaran, Ching-Hsien Hsu, and Bala Anand Muthu. Hybrid method for mining rules based on enhanced apriori algorithm with sequential minimal optimization in healthcare industry. *Neural Computing and Applications*, pages 1–14, 2020.
37. Dijana Jovanovic, Milos Antonijevic, Milos Stankovic, Miodrag Zivkovic, Marko Tanaskovic, and Nebojsa Bacanin. Tuning machine learning models using a group search firefly algorithm for credit card fraud detection. *Mathematics*, 10(13):2272, 2022.
38. Nebojsa Bacanin, Catalin Stoean, Miodrag Zivkovic, Dijana Jovanovic, Milos Antonijevic, and Djordje Mladenovic. Multi-swarm algorithm for extreme learning machine optimization. *Sensors*, 22(11):4204, 2022.
39. Nebojsa Bacanin, Miodrag Zivkovic, Fadi Al-Turjman, K Venkatachalam, Pavel Trojovský, Ivana Strumberger, and Timea Bezdan. Hybridized sine cosine algorithm with convolutional neural networks dropout regularization application. *Scientific Reports*, 12(1):1–20, 2022.
40. Mohamed Salb, Luka Jovanovic, Miodrag Zivkovic, Eva Tuba, Ali Elsadai, and Nebojsa Bacanin. Training logistic regression model by enhanced moth flame optimizer for spam email classification. In *Computer Networks and Inventive Communication Technologies*, pages 753–768. Springer, 2023.
41. Nebojsa Bacanin, Miodrag Zivkovic, Marko Sarac, Aleksandar Petrovic, Ivana Strumberger, Milos Antonijevic, Andrija Petrovic, and K Venkatachalam. A novel multiswarm firefly algorithm: An application for plant classification. In *International Conference on Intelligent and Fuzzy Systems*, pages 1007–1016. Springer, 2022.



42. Ehsan Nowroozi, Ali Dehghantanha, Reza M Parizi, and Kim-Kwang Raymond Choo. A survey of machine learning techniques in adversarial image forensics. *Computers & Security*, 100:102092, 2021.
43. Mohammad Manzurul Islam, Gour Karmakar, Joarder Kamruzzaman, Manzur Murshed, Gayan Kahandawa, and Nahida Parvin. Detecting splicing and copy-move attacks in color images. In *2018 Digital Image Computing: Techniques and Applications (DICTA)*, pages 1–7. IEEE, 2018.
44. Mauro Barni, Ehsan Nowroozi, and Benedetta Tondi. Detection of adaptive histogram equalization robust against jpeg compression. In *2018 International Workshop on Biometrics and Forensics (IWBF)*, pages 1–8. IEEE, 2018.
45. Sara Ferreira, Mário Antunes, and Manuel E Correia. Exposing manipulated photos and videos in digital forensics analysis. *Journal of Imaging*, 7(7):102, 2021.
46. Ricard Durall, Margret Keuper, Franz-Josef Pfreundt, and Janis Keuper. Unmasking deepfakes with simple features. *arXiv preprint arXiv:1911.00686*, 2019.
47. Gurpal Singh Chhabra, Varinderpal Singh, and Maninder Singh. Hadoop-based analytic framework for cyber forensics. *International Journal of Communication Systems*, 31(15):e3772, 2018.
48. Nighat Usman, Saeeda Usman, Fazlullah Khan, Mian Ahmad Jan, Ahtasham Sajid, Mamoun Alazab, and Paul Watters. Intelligent dynamic malware detection using machine learning in ip reputation for forensics data analytics. *Future Generation Computer Systems*, 118:124–141, 2021.
49. Amit V Kachavimath, Shubhangeni Vijay Nazare, and Sheetal S Akki. Distributed denial of service attack detection using naïve bayes and k-nearest neighbor for network forensics. In *2020 2nd International conference on innovative mechanisms for industry applications (ICIMIA)*, pages 711–717. IEEE, 2020.
50. Paola Barra, Carmen Bisogni, Michele Nappi, David Freire-Obregón, and Modesto Castrillón-Santana. Gait analysis for gender classification in forensics. In *International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications*, pages 180–190. Springer, 2019.
51. Anton Yudhana, Imam Riadi, and Faizin Ridho. Ddos classification using neural network and naïve bayes methods for network forensics. *International Journal of Advanced Computer Science and Applications*, 9(11), 2018
52. T Satya Sudha and Ch Rupa. Analysis and evaluation of integrated cyber crime offences. In *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*, volume 1, pages 1–6. IEEE, 2019.
53. Muhammad Faris Ruriawan, Bintaran Anggono, Isaac Anugerah Siahaan, and Yudha Purwanto. Development of digital evidence collector and file classification system with k-means algorithm. In *2019 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*, pages 64–68. IEEE, 2019.
54. Dixit Roy. Naskar, & chakraborty.(2020). digital image forensics theory and implementation. *Studies in Computational Intelligence*, 755.
55. Muhammad Ali, Stavros Shiaeles, Nathan Clarke, and Dimitrios Kontogeorgis. A proactive malicious software identification approach for digital forensic examiners. *Journal of Information Security and Applications*, 47:139–155, 2019.
56. Maryam Hina, Mohsan Ali, Abdul Rehman Javed, Gautam Srivastava, Thippa Reddy Gadekallu, and Zunera Jalil. Email classification and forensics analysis using machine learning. In *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, pages 630–635. IEEE, 2021.

57. Belal Ahmed, T Aaron Gulliver, and Saif alZahir. Blind copy-move forgery detection using svd and ks test. *SN Applied Sciences*, 2(8):1–12, 2020.
58. Jobin Varghese and C Sathish Kumar. Robust copy-move forgery detection algorithm using singular value decomposition and discrete orthonormal stockwell transform. *Australian Journal of Forensic Sciences*, 52(6):711–727, 2020.
59. Turker Tuncer, Fatih Ertam, and Sengul Dogan. Automated malware identification method using image descriptors and singular value decomposition. *Multimedia Tools and Applications*, 80(7):10881–10900, 2021.
60. Huan Li, Bin Xi, Shunxiang Wu, Jingchun Jiang, and Yu Rao. The application of association analysis in mobile phone forensics system. In *International Conference on Intelligence Science*, pages 126–133. Springer, 2018.
61. Timothy Bollé, Eoghan Casey, and Maëlig Jacquet. The role of evaluations in reaching decisions using automated systems supporting forensic analysis. *Forensic Science International: Digital Investigation*, 34:301016, 2020.
62. Abiodun A Solanke. Explainable digital forensics ai: Towards mitigating distrust in ai-based digital forensics analysis using interpretable models. *Forensic Science International: Digital Investigation*, 42:301403, 2022.
63. Nighat Usman, Saeeda Usman, Fazlullah Khan, Mian Ahmad Jan, Ahthasham Sajid, Mamoun Alazab, and Paul Watters. Intelligent dynamic malware detection using machine learning in ip reputation for forensics data analytics. *Future Generation Computer Systems*, 118:124–141, 2021.
64. Felix Anda, David Lillis, Nhien-An Le-Khac, and Mark Scanlon. Evaluating automated facial age estimation techniques for digital forensics. In *2018 IEEE Security and Privacy Workshops (SPW)*, pages 129–139. IEEE, 2018.

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 2.5 International License (<http://creativecommons.org/licenses/by-nc/2.5/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

