International Journal of
Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
www.computersciencejournals.com/ijcai
IJCAI 2024; 5(1): 85-95
Received: 02-01-2024
Accepted: 09-02-2024

Hardi Sabah Talabani
Department of Computer, College of Science, Charmo University, Kurdistan Region, Iraq

The current landscape of digital forensics employing machine learning approaches: A Review

Hardi Sabah Talabani

DOI: https://doi.org/10.33545/27076571.2024.v5.i1a.86

Abstract

This paper discusses and evaluates the present state of digital forensics, as well as how machine learning techniques are used in this field. The paper covers technological advances in forensics medicine and how we may gain from the performance of machine learning algorithms to compare their performances for improvement on data collection, analysis and investigation. The focus is on the benefits and challenges that may arise while adopting algorithms: Naive Bayes (NB), K-Nearest Neighbor (K-NN), Support Vector Machine (SVM), Principal Component Analysis (PCA) and K-means. Apart from analyzing the latest research and studies in this subject area. Furthermore, tracing new trends in the digital forensics' domain and outline ways that machine learning can be used for better performance.

Keywords: Machine learning, digital forensic, naive bayes, k-nearest neighbor, support vector machine, principal component analysis, k-means

Introduction

The technological and digital revolution is the product of a number of current world events that have to do with development in information technology as well as high use by smart electronic appliances. The wide use and necessity of internet content in our everyday life [1]. With the increase in cybercrimes and developing digital technologies, have led to emergence of a new practice known as forensics. This pertains to the reaction of the legal system and criminal investigations in response to the advancements in technology and the shift of illegal activities towards the realm of digital data [2].

In general, digital forensics is a subdivision of the forensics field that employs digital methodologies and technology to collect and analyze evidence within the framework of legal processes [3]. Furthermore, digital forensics is the application of contemporary technology to investigate and evaluate digital evidence pertaining to criminal activities and situations. In the legal context, the objective of digital forensics is to furnish reliable and precise proof that can be relied on in a court of law to bolster legal investigations Figure 1.

Accordingly, the volume of data in this field is very large, diverse, comprehensive and very accurate, and is constantly increasing as a result of rapid technological progress and the increasing use of smart devices. Moreover, is no human capacity, and traditional methods do not have sufficient capacity to manage and analyze this huge and accurate amount of data [5].

Therefore, investigators thought about employing faster and more accurate methods in digital forensics for the purpose of collecting and analyzing data, which is machine learning ML methods.

Accordingly, the aim of this study is to state how the employing of techniques based on ML enables efficient handling of vast quantities of data, facilitating the identification of patterns and trends within various types of data, such as electronic medical records, digital photographs, and genetic data. This helps to identify the connections and variables that are relevant for investigations.ML includes several algorithms, including: Naïve Bayes Algorithm, K-Nearest Neighbor Algorithm, Support Vector Machine and Principal Component Analysis and K Means Algorithm.

Corresponding Author:
Hardi Sabah Talabani
Department of Computer, College of Science, Charmo University, Kurdistan Region, Iraq

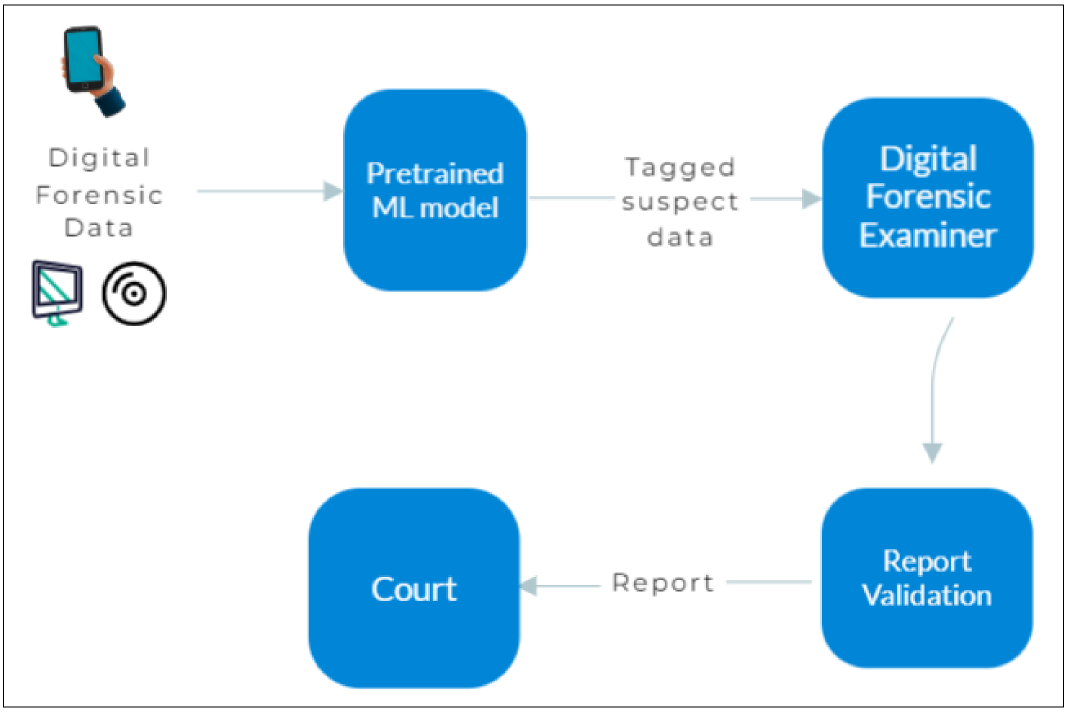

Fig 1: Machine Learning in Digital forensic- State of Art

Machine Learning

Machine learning ML is one of the most important subfields for artificial intelligence. It particularly focuses on the development of systems that learn and improve their performance without human intervention [6]. ML is an essential element of AI technologies, as it helps systems learn how to adjust and improve themselves based on changes in the environment or received data. ML relies on developing mathematical models and algorithms that enable the use of information by computer systems to identify patterns in data for automatic decision-making without explicit programming [7]. This involves the activities of data analysis and decoding, information acquisition, as well as performance improvement by automatic processes. Machine learning comprises three main techniques as shown in Figure 2 below.

1) **Supervised Learning:** In supervised machine learning, the computer model is trained to find correlation between inputs and outputs by being fed with a dataset containing sample data that already exist. Basically, the goal is to improve performance by training and extracting knowledge from existing instances allowing it thus—to predict outcomes of unknown inputs [8]. A training set is formed, where known samples are included and each input (output) takes with past features. This dataset is used for training the model which then compares its prediction with a known output to refine internal parameters. After that, its effectiveness is measured by using a dataset on which the model has not yet been trained and then cementing whether it can perform new data sample [9]. The training and assessment methods are repeated to improve the performance of the model incrementally.
2) **Unsupervised Learning:** It is a process where computer systems learn to extract information from data without any help or supervision from outside. This shows that the information fed to the system does not have any attached labels or prior guidance given to it by a model. On the contrary, the model uses statistically significant patterns or hidden structures form data [10]. The primary ideas that underlie unsupervised learning are discovering hidden clusters or structures within data with no previous information automatically recognizing patterns and classifications inside the data, and teaching the model to cluster samples that share certain properties based on their intrinsic similarities. Moreover, unsupervised machine learning is essential in fields such as data mining, understanding the trends from big databases and image processing [11]. It assists in the design of smart prototypes to address a wide range of challenges.
3) **Reinforcement Learning:** Focuses on the development of intelligent models that are capable to make interactive decisions under an uncertain environment. Reinforcement machine science aims at increasing the efficacy of a system by interacting with its environment, using rewards or penalties to control decision-making. The fundamental principles of reinforcement machine learning encompass the following elements: agent, environment, state, action reward policy and value [12]. The worker is an identifying factor that interacts with the environment and makes a decision. An agent is a set of mechanical objects, including robots and computer programs or any other highly sophisticated system that has capability to learn and reason. The environment encompasses the physical and social environments in which the worker engages. The environment encompasses both the physical world and the virtual realm, comprising all the necessary variables for the agent to engage with. The term "state" refers to a description of the agent's present condition in the environment [13]. This encompasses all essential data that delineates the worker's circumstances and the surrounding milieu. Action refers to the specific movement or decision made by an actor within its surrounding environment. Action is regarded as an integral component of the worker's strategic approach to attaining the intended objectives. The model policy is

a set of regulations or tactics that dictate the worker's decision-making process. Reinforcement machine learning seeks to improve policies in order to obtain the greatest rewards. Value, in essence, represents a calculated approximation of the anticipated outcome resulting from the execution of a certain course of action within a given set of circumstances [14]. The worth of acts is contingent upon the anticipated long-term rewards.

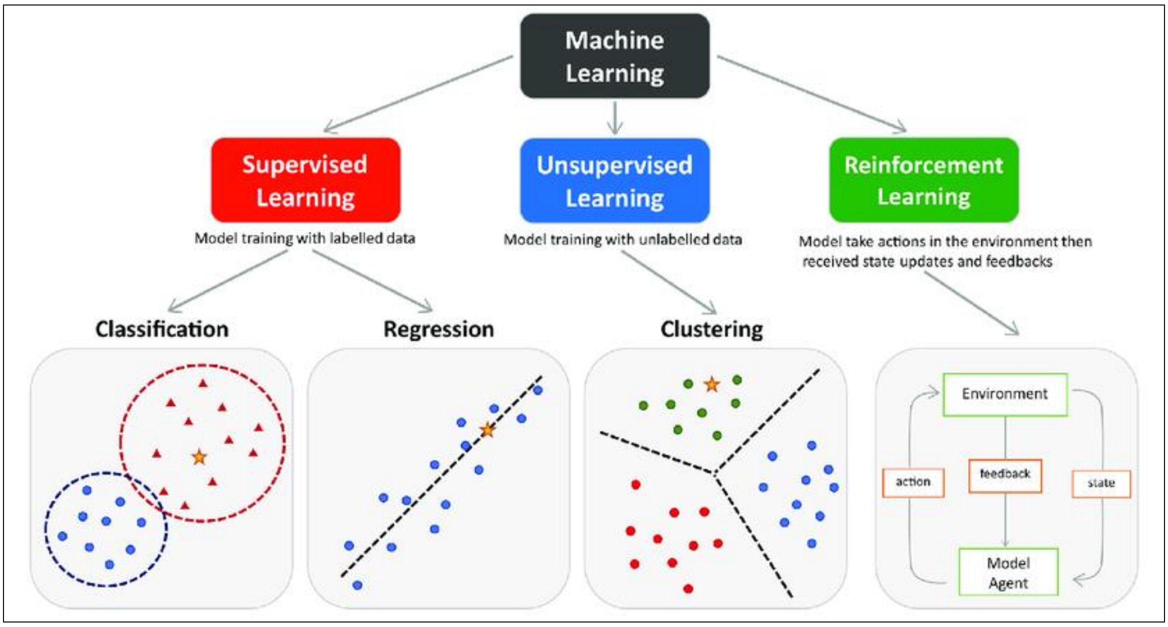

Fig 2: Machine Learning Types [15].

Digital Forensics

Digital forensics is a significant transformation in the area of forensics, since it merges traditional forensic ideas with contemporary information technology [16]. This integration facilitates the use of digital technologies and data analysis to enhance forensic procedures and deliver precise and complete reports derived from an analysis of digital data extracted from videos, images, and electronic medical records by following different methods, including:

a) **The use of imaging methods:** Digital forensics requires the use of high-resolution imaging and radiography to study corpses and other forms of evidence for a postmortem. By doing so, it becomes possible to control physiological consequences and determine the causes of death [17].

b) **Digital Image Analysis:** Digital forensics today is based on the analysis of digital photographs to distinguish between natural and criminal evidence, thereby enhancing diagnostic precision and investigation [18].

c) **Video Analysis:** Digital video analysis allows tracking movements and individual behavior, thus making criminal activity investigation possible in addition to providing powerful court evidence [19].

d) **Medical Data Analysis:** Big data analysis methods may be implemented into electronic medical records to analyze diseases and accurately provide deaths and disease numbers [20].

e) **Employing Modern Technology:** Encompasses the cooperation with contemporary technology like artificial intelligence and machine learning to enhance the examination of evidence and expedite investigation procedures [21].

f) **Digital fingerprint analysis:** Digital forensics allows for the examination of digital fingerprints and facial features in order to prove identity and aid in the identification of remains [22].

g) **Developments in Machine Learning:** The accuracy of medical judgements in the forensic sector is being improved by advances in machine learning and data analysis techniques [23].

Digital forensics investigation process

Due to the diversity and large number of sources of data that can be collected and the continuous increase in this data, and in order for the investigation to be of a nature that is understood by the relevant companies [24]. Consequently, the investigation process must pass through four main stages depending on the complexity of the data. Below is Figure 3 illustrating the stages of a digital forensic investigation. Each stage is as below.

a) **Collection:** This stage of the investigation typically involves collecting various types of digital evidence, including images, videos and electronic medical records – across different settings such as smart devices; computers & servers) [25]. The data is scrupulously documented and stored to ensure its authenticity and legality. Data collecting technology includes modern technologies in digital imaging and image analysis that allow providing accurate and reliable sources for medical workers or investigators [26].

b) **Examination:** This step is also an important part of the digital forensic investigation procedure, in which advanced technologies are used to inspect and decode the available pieces of the digital evidence. Furthermore, this analysis involves supervising photos and videos with the utmost scrutiny of electronic medical records while ensuring their source veracity. In addition, it indicates the particular field that has relevant information for the investigation method and assures no data will be lost due to compression or encryption procedures. This helps in distinguishing clinical implications and understanding situations that relate to the study [28]. Hence, through this painstaking analysis medical personnel and investigators have more precise answers to medical and forensic issues.

c) **Analysis:** This phase is an essential stage where correct and reliable conclusions are obtained from digital evidence. The analysis is concerned with using advanced technology to analyze photos and videos, picking out physical evidence, and determining the temporal context of events [29]. Also, it includes the analysis of EMR using computational methods especially machine learning and artificial intelligence techniques. This helps to identify and determine the medical factors for accidents or crimes. Besides, proficiency in the field of forensics and data analysis is obligatory at this point to ensure accurate and reliable results that can be used as compelling evidence for judicial processes [30].

d) **Reporting:** The final stage of digital forensics is the summary and presentation with accuracy, methodology on collected proofs and culmination. Moreover, for this task it is important that accuracy and detail are maintained as the report forms a legally binding document which serves to interpret findings and inform their application in court or other settings [31]. The report refers to the documentations of evidence that is collected and digital analyzes utilized, with emphasis on important medical/forensic details. Furthermore, it requires integration between findings and analyses to provide a summary overview together with an accurate understanding of the data being analyzed. The purpose of this report is to elucidate medical and forensic issues in a manner that is comprehensible to investigators and judges [32]. Consequently, it plays a crucial role in attaining justice and comprehending the intricacies of challenging cases.

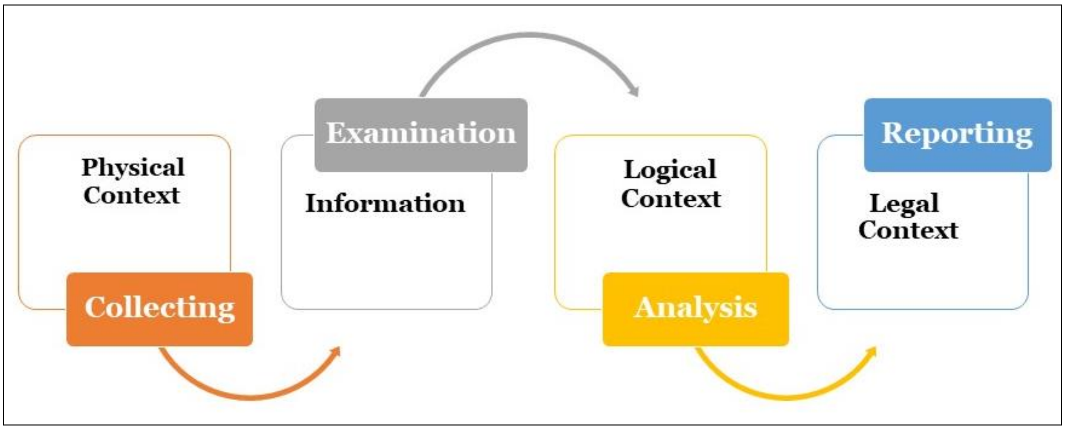

Fig 3: The Stages of Digital Forensics Investigation Process

Digital forensics models

According to the National Institute of Standards and Technology the process of investigating digital forensic evidence include four designed methodologies [33]: 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). Each version is specifically tailored for a certain phase and process Figure 4.

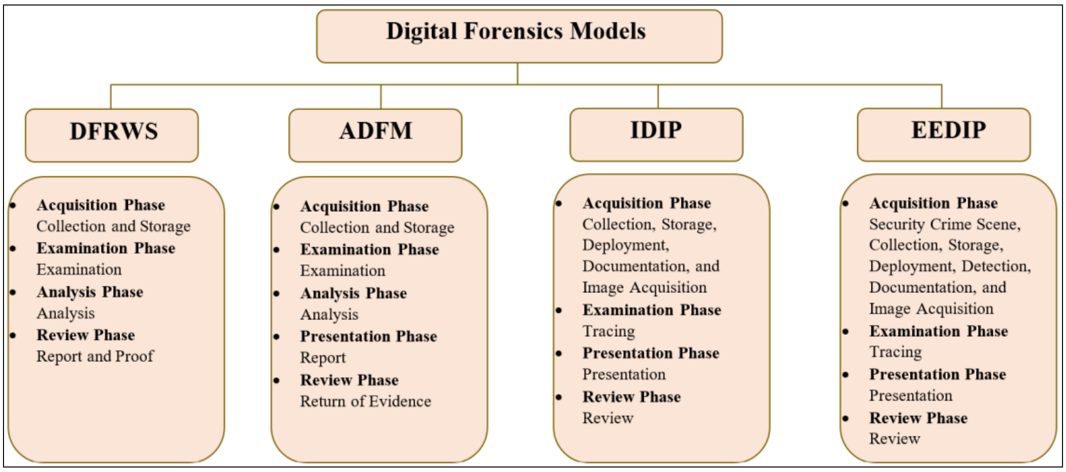

Fig 4: Digital Forensics Models [33]

Digital forensic challenges

Currently, the field of digital forensics encounters several obstacles stemming from swift advancements in technology and changes in the digital landscape. One of the notable issues is the growing amount and intricacy of digital data, necessitating meticulous analysis and sophisticated resources to guarantee effective comprehension. Challenges encompass security and privacy concerns, as investigators must guarantee the authenticity of data and digital evidence while safeguarding the secrecy of sensitive information. Furthermore, digital investigation encounters difficulties in the realm of legislation and regulations, as the utilization of digital technology necessitates complete adherence to legal norms and the assurance of accurate documentation of evidence and findings. Table 1 includes a comparison between current studies in the way they survey the challenges facing digital forensics specialists, represented by different types of security and quality standards, the volume and quality of data in this field, the extent of the complexity of the methods for extracting information from it, and other standards related to the aforementioned challenges Table 1.

Table 1: Digital Forensic Challenges and Considerations

Ref.	Challenges	Data Volume	Privacy concern	Technical Complexity	Resource Constraints	Forensic Tools Sophistication	Rapid Technological Changes
[34]	Volatile Memory Analysis	High	Moderate	Moderate	Limited	N/A	Rapidly Evolving
[35]	Encryption / Decryption	High / homogenous	Very High	High	Limited	High	Rapidly Evolving
[36]	Big Data Forensics	Very High/ heterogeneous	N/A	High	Moderate	Moderate	Large-Scale Data Analysis
[37]	Digital Evidence Integrity	Moderate	High	High	Moderate	High	Advanced Manipulation
[38]	Social Engineering Attacks	High	High	Moderate	Moderate	Moderate	Manipulation of Users
[39]	Insider Threats	Moderate / homogenous	N/A	Moderate	Moderate	N/A	Insider Misuse
[40]	Forensic Analysis Automation	High / heterogeneous	N/A	High	Moderate	N/A	Automated Threats
[41]	Cloud Storage Forensics	High / heterogeneous	N/A	Moderate	Limited	High	Diverse Cloud Providers
[42]	Anti-Forensic Techniques	Moderate / homogenous	N/A	Moderate	Limited	High	Constant Innovation

Literature search strategies

The literature search technique for this review is derived from well-established academic frameworks. The main objective was to incorporate an extensive compilation of research related to the employment of machine learning in the digital forensic domains and its many contexts during the past eight years. A comprehensive examination of academic databases, such as Science Direct, Google Scholar, IEEE Xplore, and Scopus, was carried out to guarantee the incorporation of a wide range of sources beyond the conventional academic domain.

The search terms included various versions of “machine learning” “Digital forensic” and related phrases. Additionally, we used free text keywords such as “applying on machine learning in digital forensic” to find papers that addressed closely related ideas. This methodology helped us to understand different aspects of machine learning techniques in the digital forensic domains.

Machine learning approaches in digital forensics

Machine learning is an important aspect of digital forensic processes since it enables systems and software to analyze data and extract pertinent information with greater accuracy and efficiency. Machine learning is applied in several domains of digital forensics, such as the analysis of medical images and the interpretation of large-scale medical data [43]. Machine learning approaches may reliably detect physical evidence in forensic images, hence aiding in the precise determination of causes of death. Learning models may utilize electronic medical data to recognize patterns and correlations within data sets, hence facilitating significant findings in the realm of medical research [44].

Furthermore, Academic studies dealing with the use of machine learning algorithms in the field of digital forensics is constantly increasing, especially in recent years. Whereas, by conducting statistics on the number of research papers published in the database for academic research (Google Scholar) and following the search query “machine learning” in “digital forensic” as a search method in the last four years, it became clear to us that research in this field is constantly increasing, Figure 5.

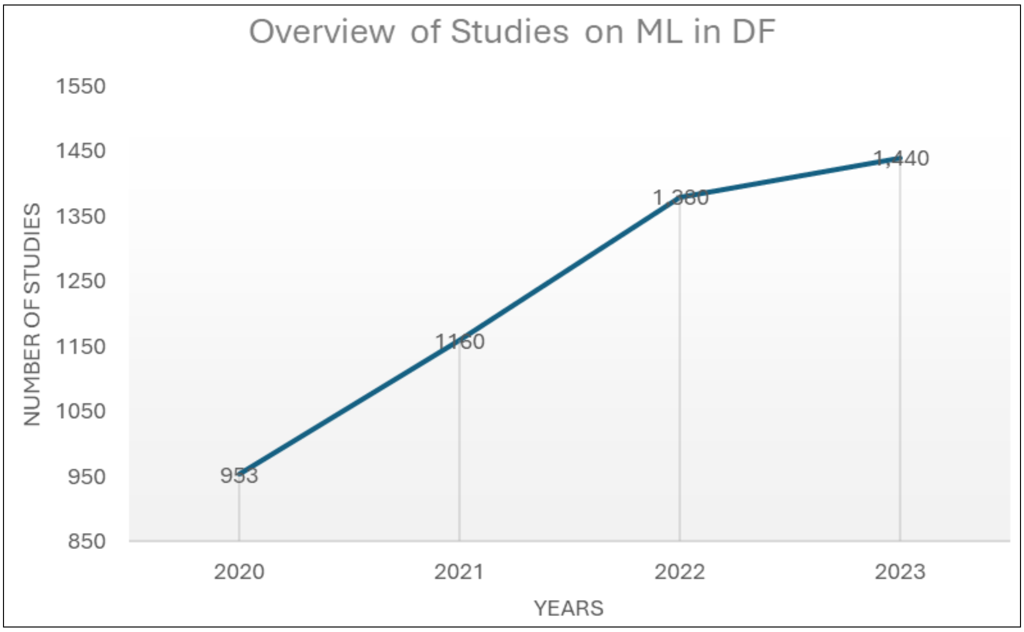

Fig 5: Overview of Studies on Machine Learning in Digital Forensics (2020 - 2023)

Machine learning may enhance diagnostic accuracy, expedite analytical procedures, and enhance comprehension of intricate digital evidence in the field of digital forensics, consequently facilitating reliable and accurate outcomes. The following explains the basics of five machine learning algorithms and the performance of each of them when used in the field of digital forensics.

Naïve bayes algorithm in digital forensics

The Naive Bayes NB method is well recognized as a prominent algorithm in the domain of machine learning and data analysis. This algorithm is used for classification applications, and it classifies the data into different classes based on given attributes. The name of the algorithm "naive" is based on its underlying assumption that all features used for classification are strictly independent. This assumption helps simplify calculations and speeds up the training and classification process.

Bayesian probability concepts are implemented by NB to obtain the conditional probabilities for data classification via training datasets [45]. To implement the training, a dataset that contains pre-defined features and associated classifications is used. After that, the model uses these probabilities to classify new data. NB, despite being relatively straightforward, has strong performance in several contexts, particularly in text classification tasks like postal categorization and linguistic analysis. They have applications in several domains like machine learning, data science, and information security. While it implies the independence of features, this method may be highly effective in classifying data, especially when there is a substantial quantity of training data available. The research team in [46] utilized a heterogeneous dataset with a wide range of network traffic patterns, spanning from innocuous to malevolent. Subsequently, the classification techniques employed include Naïve Bayes, K-Nearest Neighbours (KNN), and Random Forest approaches. The approaches enhance the mean class error, showing a 6.58% error rate for GenClass, in contrast to the error rates of 32.59% for the Bayes method, 18.45% for KNN, and 30.70% for Random Forest. Furthermore, in [47] the researchers conducted a study where they analyzed the NSLKDD Dataset, with a special emphasis on ICMP Attack, TCPSync Attack, and UDP Attack. They analyzed these attacks inside the present dataset as well as in other available datasets. They then performed network packet classification employing MLP, Random Forest, and Naive Bayes algorithms. The accuracies obtained were 98.63%, 98.02%, and 96.91%, respectively. The researchers used Python Anaconda and Kappa statistic tools to confirm the acquired findings. In addition, in [48] the researchers use KDD99 dataset, produced by the Defense Advanced Research Projects Agency at his MIT Lincoln American Laboratory. After that, they performed a network package classification employing SVM, and Naive Bayes, the obtained accuracies were 99.68%, 92.34%, respectively. the researchers used Python were used to implement the model. NumPy and the sklearn libraries are included in the Python packages.

K-nearest neighbor algorithm in digital forensics

The K-Nearest Neighbor KNN algorithm is a straightforward and efficient machine learning algorithm widely used in several domains, particularly for data classification. This technique operates on the fundamental concept of "similarity implies proximity", in which an unclassified point inside a certain domain is categorized based on the classification of nearby points [49].

KNN is founded on a straightforward principle: while attempting to determine the class of a new point, it is logical to examine the points in close proximity to it. The "K" in K-Nearest Neighbor denotes the quantity of neighbors employed in the categorization procedure. For instance, when K is equal to 5, the new point will be evaluated and ranked according to the viewpoints of the five nearest points. Dimension scales, such as the European Dimension Scale, are utilized for quantifying the distance separating various points. The closest neighbor technique is easily comprehensible and well-suited for several circumstances, particularly when dealing with limited and straightforward data. Nevertheless, one may face difficulties when handling extensive data sets or when there is an unbalanced distribution of effects across classes. the authors in [50] building a machine learning approach using KNN and gaussian SVM to investigate mobile sensors dataset collected through a Matlab App. the accuracies obtained were 81% with KNN and 78% with Gaussian SVM.

Support vector machine algorithm in digital forensics

The Support Vector Machine (SVM) is a very effective technique in the field of machine learning, commonly employed for tasks including classification and predictive analysis. The primary purpose of SVM is to address problems with classification, however, it may also be used to other tasks such as numerical analysis and temporal analysis. In general, the primary objective of the SVM method is to identify a linear separator that effectively distinguishes between two sets of data. The interval is chosen to minimize the margin, which is the shortest distance between the interval and the closest point of each class. Support Vectors are the chart points that are closest to the break and play a crucial role in deciding the break [51].

In addition, SVM incorporates several kernels to facilitate the transformation of data into a higher-dimensional space, enabling the identification of nonlinear separations. Once the model has been trained using the data, it may be employed to categories additional, unclassified data points. Furthermore, this algorithm offers the benefit of effectively managing data sets with a large number of dimensions and the capability to handle data that is not linearly separable. Nevertheless, some factors, such as kernel adoption and the assignment of the aggregate parameter value, need meticulous adjustment in order to achieve the best performance possible. To summaries, the SVM method is a potent tool in machine learning, applicable in several domains, particularly when classifying sophisticated and multidimensional data is required. In [52] the authors the authors build ML framework employing SVM and Convolutional Neural Networks (CNN) in deepfake detection using 140k real and fake faces collected from Kaggle. The classification accuracies obtained were 81.69% with SVM and 88.33% with CNN. Furthermore, the authors in [53] the authors employed trained SVM in classifying MySQL and PostgreSQL datasets collecting a total of 500 memory snapshots for each DBMS. SVM has applied for both datasets and its classification accuracy was 92% classifying MySQL dataset and 90% classifying PostgreSQL dataset. The researchers used the Python based Pandas, scikit-learn and Seaborn libraries for visualize and framing the used datasets. Moreover, in [54] the authors conducted a comparison between the framework utilizing Support Vector Machines (SVM) for binary classification and the Xception and CNN+RNN models as deep feature extractors in the detection of deepfake videos. The evaluation was performed on the FF++ dataset, which consists of 1000 original video sequences that were manipulated using four automated face manipulation methods: Deepfakes, Face2Face, Face Swap, and Neural Textures. The use of handcrafted features with SVM yields a maximum accuracy of 74.26%, which decreases considerably to an average of 56% in the presence of mismatches between the training and test sets. Although deep features extracted using CNN perform exceptionally well, with accuracy rates over 99% when the data comes from the same sub-dataset, the performance significantly decreases when there is a mismatch between the training and test sets.

Principal component analysis algorithm in digital forensics

Principal components analysis (PCA) is a crucial method utilized in the fields of data analysis and dimensionality reduction. (PCA) is employed to perform a linear transformation on a group of variables that are intercorrelated. This transformation results in a new collection of variables known as principal components. The objective of PCA is to ensure that these components capture as much variation as possible from the original data. The primary objective of (PCA) is to decrease dimensionality, enabling the retention of maximum information while employing a reduced number of variables [55]. The efficacy of PCA is ascribed to its capacity to discern prominent patterns of variability in data, hence facilitating a clearer comprehension of the data's structure and offering a more complete perspective on the interrelationships between variables. (PCA) is widely employed in several domains like image analysis, signal processing, and economic data analysis. Its application in these sectors greatly enhances the comprehension and examination of vast and intricate datasets. The researchers in [56] showed that how PCA for dimensionality reduction affected improve in classifying 1403 samples of various repositories like virus dataset collected from Github, and the Canadian Institute of cyber security using several machine learning classifiers. the accuracy of employed classifiers for naive bayes (76%), Bagging Decision Tree (68%), SVM (76%), Logistic Regression (69%) and KNN (76%) has been raised to 77%, 76%, 78%, 75% and 80% respectively after using PCA. the researchers used the google Colab platform for implementing the logistic regression using the sklearn kit. and used Numpy and Pandas packages for implementing the mathematical approach. Furthermore, the authors in [57] employed KNN and density-based algorithm and random forest in classifying 25 clusters of ransomwares with several different family variants using PCA for feature extracting and dimensionality reduction. The results obtained 98% for KNN and density based and 99% for random forest. The researchers used Python programming language under the Jupyter platform for implementing their model codes. In additional, in [58] employed seven machine learning classifiers (Naïve Bayes, SVM, Decision, Random Forest, KNN, Nearest Centroid and Gradient Boost) in classifying 29,797 samples of Portable Executable (PE) malware collected from various sources including files from Windows installation. The best obtained accuracy was with Random Forest with PCA as dimensionality reducer reached 99.41%. For running the experiments, the researchers use Python.

K-means algorithm in digital forensics

The "K-Means" algorithm is a well-known algorithm in the domain of machine learning and data segmentation. This method is mostly employed in the domain of data analysis and comprehension of its diverse structures [59]. In general, the fundamental purpose of the K-Means method is to divide a collection of data points into distinct subsets, sometimes referred to as "clusters". The objective of this division is to identify the centroids of clusters in order to minimize the average distance between points within each cluster. The procedure of verifying points and establishing cluster centroids is iterated until a satisfactory balance is achieved between the cluster point distances and the cluster centre distances. K-Means is a very efficient technique for data analysis that finds extensive use in several domains, including data exploration and categorization [60]. In addition, the primary purpose of this algorithm is to streamline the task of categorizing and arranging a collection of information, allowing for the identification of patterns and a deeper comprehension of their underlying structures. the authors in [11] the authors employed K-means and k-medoids algorithm for clustering 1,000 documents of crime reports collection from housebreaking crime reports from 2010 to 2013 including both local and online repositories. The best performance accuracies obtained for used algorithms were 86% for k-means and 87% for k-medoids. The researchers used w RapidMiner to conduct the experiments.

Table 2 includes a summary of the mentioned studies and the main findings that researchers reached during their application of the aforementioned algorithms to data in the field of digital forensics.

Table 2: Summary of selected Machine Learning Algorithms in various Digital Forensic types

Ref.	Year	DF Phase	DF type	ML algorithms	Main Findings
[46]	2023	Analysis	Networking Forensic	Naïve Bayes, KNN, Random Forrest	Engaging in research on Software-Defined Networking (SDN), investigating a dataset that covers a wide range of network traffic patterns, with grammatical evolution as the classification mechanism.
[47]	2022	Analysis and investigate	Networking Forensic	Naïve Bayes, NLP, RF	Design methods of dead/live forensic acquisition and analysis within/outside the ICMP Attack TCP Sync Attack, UDP Attack, and /designed a digital forensic triage for the examination and partial analysis of in the cloud computing systems.
[48]	2022	Analysis	Networking Forensic	Naïve Bayes, SVM	Develop an advanced network intrusion detection system that use ML classifiers to identify and differentiate among malicious and non-

					malicious network packets.
[49]	2022	Investigate	Video Forensic	KNN, SVM	Building a ML approach for investigating crime scenes in mobile phones.
[52]	2023	Analysis	Image Forensic	SVM, CNN	Developing a specialized deepfake detection algorithm that specifically targets the identification of deepfakes in images.
[53]	2023		Database Forensic	SVM	memory snapshot prediction framework using trained ML method
[54]	2022	Analysis	Video Forensic	SVM, CNN	Confirm that the efficacy of handcrafted features may decrease to some extent due to differences between the training and test datasets. Deep features are highly effective when the data originates from the same sub-dataset. The accuracy significantly decreases when there is a discrepancy between the training sets and test sets.
[56]	2023	Investigate	Malware Forensic	PCA, KNN	Reducing the dimensions Emphasizing significant and crucial qualities from the training data set also aids in identifying linear combinations that can serve as countermeasures. Issues related to multicollinearity
[57]	2022	Analysis and investigate	Malware Forensic	PCA, K-Means	Detecting zero-day attacks using ML approaches and feature engineering.
[58]	2023		Malware Forensic	PCA	Static malware detection framework by mining DLLs, and API calls from each DLL using ML approach and feature selecting.
[59]	2022	Analysis, Investigate, Reporting	Forensic linguistics	K-Means	In document clustering, the performance of the k-means algorithm relies on the number of starting clusters, which may be determined by employing the elbow approach to get the optimal cluster number.

Machine learning challenges in digital forensic

The domain of digital forensics encounters serious challenges in comprehending and interpreting the outcomes of intricate algorithms employed for examining medical data. This is explained by the complexity of these models and understanding their decision process. The question arises, how to communicate these results in a logical and understandable way for forensic specialists and legal institutions. An integrated approach of medical knowledge in conjunction with technical competence is required to enhance the expert's interaction with these algorithms within a framework of digital forensics. This method should find the right compromise between model complexity and understandability [62].

Since digital forensics is about handling confidential and personal data of patients, this domain is closely connected with the issues concerning security and privacy protection. This assignment involves reaching a subtle balance between accessibility of medical data and protecting it from unauthorized use. Strict security protocols and data encryption must be introduced adhering to health privacy laws as well. It is necessary to address the challenges that could arise in case of increase cyber threats, and forensic medical systems are under attack. Due to the development of technology, it is paramount in improving security policies and strategies that will be used as access control methods since data can never remain static [63].

An important factor in the successful implementation of machine learning algorithms within digital forensics is variability. This issue refers to divergences that can appear in the quality of data used for model training because there may be biases or inconsistencies within the dataset. It may lead to insufficient improvement of model performance due to the fact that algorithms efficiency depends on how good and diverse data used for their training. In this case, it is essential to achieve the right balance in terms of collecting and using data keeping regional cultural differences as well as demographic divergence into account so that all groups are represented fully and fairly. These problems require care and thoroughness in the choice and preparation of data, as well as correction methods to ensure that models are quality ones which can work with many cases presented by forensic medicine [64]. Table 3 includes the challenges facing the selected algorithms in the field of digital forensics from the studies reviewed in Section 8.

Table 3: Mahine Learning Challenges in Digital Forensic

Ref.	MLs	Challenges	Description
[46]	NB	Assumption of Independence	Data in digital forensics is not often characterized by the independence of the features that the NB algorithm always relies on, which leads to a decrease in the accuracy of its performance.
[49]	KNN	high-dimensional data	KNN algorithm is inefficient in dealing with large-dimensional data, such as forensic data, which is sometimes characterized by a large number of features.
[52]	SVM	Imbalanced Datasets	SVM has difficulties dealing with the imbalanced data set that occasionally characterizes digital forensic data.
[58]	PCA	Assumption of Linearity	The relationships between digital forensic data may be non-linear and therefore may not fit the linearity assumption of PCA algorithm, thus affecting its analytical performance of the data.
[56]	K-Means	Handling Categorical Data	The structure of digital forensic data may be categorical rather than numerical, and thus it takes more time to transform the data into a structure that is compatible with the mechanism of the K-Means algorithm.

Discussion and Conclusion

Digital forensic investigators have been able to a large extent to analyze heterogeneous data and uncover the facts. But the information development taking place in the world has led to the emergence of new challenges that require the use of automation and machine learning techniques to come up with more accurate and faster decisions and analyses, which facilitates investigation processes for investigators and the court. Consequently, this paper has present the application of five ML algorithms to tackle digital forensic challenges, e.g., NB, KNN, SVM, PCA, K-Means. Based on the proposed reviewed papers been concluded that each of KNN and NB support network forensics. while the SVM and PCA are the best possible practices to be implemented in an image forensics investigation. In contrast K-Means has significant classification performance on language forensic databases. Finally, Despite the progress achieved in investigations into various types of digital forensic evidences using ML mechanisms, there are still some limitations that accompany these mechanisms, such as the size and accuracy of the data, the possibility of penetrating ML systems, the complexity of some ML models, and the sensitivity of dealing with confidential and sensitive information.

References

1. Ombu AI. Role of Digital Forensics in Combating Financial Crimes in the Computer Era. Journal of Forensic Accounting Profession. 2023;3(1):57-75.
2. Wilson-Kovacs D. Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales. Policing: An International Journal. 2021;44(4):669-682.
3. Kumar G, Saha R, Lal C, Conti M. Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. Future Generation Computer Systems. 2021;120:13-25.
4. Karagiannis C, Vergidis K. Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. Information. 2021;12(5):181.
5. Banerjee A, Chakraborty C, Kumar A, Biswas D. Emerging trends in IoT and big data analytics for biomedical and health care technologies. In: Handbook of data science approaches for biomedical engineering. 2020, 121-152.
6. Talabani HS, Jumaa IH. A Review of Various Machine Learning Techniques and its Application on IoT and Cloud Computing. Tikrit Journal of Pure Science. 2024;29(1):185-195.
7. Vatansever S, Schlessinger A, Wacker D, Kaniskan HÜ, Jin J, Zhou MM, *et al*. Artificial intelligence and machine learning-aided drug discovery in central nervous system diseases: State-of-the-arts and future directions. Medicinal Research Reviews. 2021;41(3):1427-1473.
8. Abdulhadi HMT, Talabani HS. Comparative study of supervised machine learning algorithms on thoracic surgery patients based on ranker feature algorithms. UHD Journal of Science and Technology. 2021;5(2):66-74.
9. Vercio LL, Amador K, Bannister JJ, Crites S, Gutierrez A, MacDonald ME, *et al*. Supervised machine learning tools: a tutorial for clinicians. Journal of Neural Engineering. 2020;17(6):062001.
10. Li N, Shepperd M, Guo Y. A systematic review of unsupervised learning techniques for software defect prediction. Information and Software Technology. 2020;122:106287.
11. Du Y, Li S, Sharma Y, Tenenbaum J, Mordatch I. Unsupervised learning of compositional energy concepts. Advances in Neural Information Processing Systems. 2021;34:15608-15620.
12. Levine S, Kumar A, Tucker G, Fu J. Offline reinforcement learning: Tutorial, review, and perspectives on open problems. arXiv preprint arXiv:2005.01643. 2020.
13. Canese L, Cardarilli GC, Di Nunzio L, Fazzolari R, Giardino D, Re M, *et al*. Multi-agent reinforcement learning: A review of challenges and applications. Applied Sciences. 2021;11(11):4948.
14. Nian R, Liu J, Huang B. A review on reinforcement learning: Introduction and applications in industrial process control. Computers & Chemical Engineering. 2020;139:106886.
15. Sabah Talabani HS, Abdulhadi HMT, Ali MH. Obfuscated Malware Memory Detection Employing Lazy Instance Based Learner Algorithm Based On Manhattan Distance Function. Passer Journal of Basic and Applied Sciences. 2024;6(1):130-137.
16. Shaji PS. The Transforming Grid of Digital Forensics to Intelligent Forensics-Relook into the Applicability of Artificial Intelligence in Current Investigation Techniques. Indian Journal of Artificial Intelligence and Law. 2020;1:45.
17. Ferreira WD, Ferreira CB, da Cruz Júnior G, Soares F. A review of digital image forensics. Computers & Electrical Engineering. 2020;85:106685.
18. Du X, Hargreaves C, Sheppard J, Anda F, Sayakkara A, Le-Khac NA, *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; c2020. p. 1-10.
19. Ponsam JG, Gracia SJB, Geetha G, Thenmozhi M, Nimala K. Extraction in Digital Forensic Investigation based on Video Enhancement and Machine Learning. In 2021 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON); c2021. p. 01-06.
20. Jayaraman I, Stanislaus Panneerselvam A. A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud. Journal of Ambient Intelligence and Humanized Computing. 2021;12:4911-4924.
21. Wilson-Kovacs D. Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales. Policing: An International Journal. 2021;44(4):669-682.
22. Yaacoub JPA, Noura HN, Salman O, Chehab A. Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations. arXiv preprint arXiv:2103.17028; c2021.
23. Talabani H, Engin AVCI. Impact of various kernels on support vector machine classification performance for treating wart disease. In 2018 International Conference on Artificial Intelligence and Data Processing (IDAP); c2018. p. 1-6.
24. Yeboah-Ofori A, Brown AD. Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. Journal of Forensic, Legal & Investigative Sciences. 2020;6(1):1-8.
25. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials. 2020;22(2):1191-1221.
26. Koroniotis N, Moustafa N, Sitnikova E. A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. Future Generation Computer Systems. 2020;110:91-106.
27. Reisoğlu İ, Çebi A. How can the digital competences of pre-service teachers be developed? Examining a case study through the lens of DigComp and DigCompEdu. Computers & Education. 2020;156:103940.

28. Horsman G, Sunde N. Unboxing the digital forensic investigation process. Science & Justice. 2022;62(2):171-180.
29. Prayudi Y, Riadi I. Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation. International Journal of Cyber-Security and Digital Forensics. 2018;7(3):294-305.
30. Al Mutawa N, Bryce J, Franqueira VN, Marrington A, Read JC. Behavioural digital forensics model: Embedding behavioural evidence analysis into the investigation of digital crimes. Digital Investigation. 2019;28:70-82.
31. Sunde N. What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices. Science & Justice. 2021;61(5):586-596.
32. Montasari R, Hill R, Carpenter V, Hosseinian-Far A. The standardised digital forensic investigation process model (SDFIPM). In: Blockchain and Clinical Trial: Securing Patient Data; c2019. p. 169-209.
33. Montasari R. The comprehensive digital forensic investigation process model (CDFIPM) for digital forensic practice. University of Derby (United Kingdom); c2021.
34. Kara I. Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges. Expert Systems with Applications. 2023;214:119133.
35. Sarhan SAE, Youness HA, Bahaa-Eldin AM. A framework for digital forensics of encrypted real-time network traffic, instant messaging, and VoIP application case study. Ain Shams Engineering Journal. 2023;14(9):102069.
36. Talabani HS, Abdulhadi HMT. Bitcoin ransomware detection employing rule-based algorithms. Science Journal of University of Zakho. 2022;10(1):5-10.
37. Maratsi MI, Popov O, Alexopoulos C, Charalabidis Y. Ethical and Legal Aspects of Digital Forensics Algorithms: The Case of Digital Evidence Acquisition. In: Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance; c2022. p. 32-40.
38. Dimitriadis A, Lontzetidis E, Kulvatunyou B, Ivezic N, Gritzalis D, Mavridis I, *et al*. Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks. IEEE Access. 2022;11:728-743.
39. Wibowo DK, Luthfi A, Widiyasono N. Investigation of Fake Insider Threats on Private Cloud Computing Services. International Journal of Science, Technology & Management. 2022;3(5):1484-1491.
40. Michelet G, Breitinger F, Horsman G. Automation for Digital Forensics: Towards a definition for the community. Forensic Science International; c2023. p. 111769.
41. Pichan A, Lazarescu M, Soh ST. A case study on major cloud platforms digital forensics readiness-are we there yet?. International Journal of Cloud Computing. 2022;11(3):268-302.
42. Taneja N, Bramhe VS, Bhardwaj D, Taneja A. Understanding digital image anti-forensics: an analytical review. Multimedia Tools and Applications; c2023. p. 1-22.
43. Abraham S, Alakananda K, Amdalli NA. A Comprehensive Review on Digital Forensics Intelligence. In: Advancements in Cybercrime Investigation and Digital Forensics; c2023. p. 25-48.
44. Talabani H, Engin AVCI. Performance comparison of SVM kernel types on child autism disease database. In: 2018 international conference on artificial intelligence and data processing (IDAP). IEEE; c2018. p. 1-5.
45. Pajila PB, Sheena BG, Gayathri A, Aswini J, Nalini M. A Comprehensive Survey on Naive Bayes Algorithm: Advantages, Limitations and Applications. In: 2023 4th International Conference on Smart Electronics and Communication (ICOSEC). IEEE; c2023. p. 1228-1234.
46. Spyrou ED, Tsoulos I, Stylios C. Distributed Denial of Service Classification for Software-Defined Networking Using Grammatical Evolution. Future Internet. 2023;15(12):401.
47. Sachdeva S, Ali A. Machine learning with digital forensics for attack classification in cloud network environment. International Journal of System Assurance Engineering and Management. 2022;13(1):156-165.
48. Kero A, Arora M, Sharma V, Makkar GD, Semwal P, Sharma HC. Detection and analysis of network traffic in network forensics using machine learning. Journal of Harbin Institute of Technology. 2022;54(12):2022.
49. Shah K, Patel H, Sanghvi D, Shah M. A comparative analysis of logistic regression, random forest and KNN models for the text classification. Augmented Human Research. 2020;5:1-16.
50. Aloni S, Shekhawat D. Crime Investigation with Mobile Sensor Data Using Gaussian SVM and KNN Classification. Neuro Quantology. 2022;20(17):556.
51. Naicker N, Adeliyi T, Wing J. Linear support vector machines for prediction of student performance in school-based education. Mathematical Problems in Engineering; c2020. p. 1-7.
52. Mallet J, Pryor L, Dave R, Vanamala M. Deepfake detection analyzing hybrid dataset utilizing cnn and svm. In: Proceedings of the 2023 7th International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence; c2023. p. 7-11.
53. Nissan MI, Wagner J, Aktar S. Database memory forensics: A machine learning approach to reverse-engineer query activity. Forensic Science International: Digital Investigation. 2023;44:301503.
54. Xu Y, Yayilgan SY. When Handcrafted Features and Deep Features Meet Mismatched Training and Test Sets for Deepfake Detection. arXiv preprint arXiv:2209.13289; c2022.
55. Li L, Zhao J, Wang C, Yan C. Comprehensive evaluation of robotic global performance based on modified principal component analysis. International Journal of Advanced Robotic Systems. 2020;17(4):1729881419896881.
56. Raymond VJ, Raj RJR, Retna J. Investigation of Android Malware with Machine Learning Classifiers using Enhanced PCA Algorithm. Computer Systems Science and Engineering. 2023;44(3):2147-2163.
57. Du J, Raza SH, Ahmad M, Alam I, Dar SH, Habib MA, *et al*. Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection. Security and Communication Networks; c2022. p. 1-16.
58. Yousuf MI, Anwer I, Riasat A, Zia KT, Kim S.

Windows malware detection based on static analysis with multiple features. Peer Journal. Computer Science. 2023;9:e1319.

59. Huang P, Yao P, Hao Z, Peng H, Guo L. Improved constrained k-means algorithm for clustering with domain knowledge. Mathematics. 2021;9(19):2390.
60. Vankayalapati R, Ghutugade KB, Vannapuram R, Prasanna BPS. K-Means Algorithm for Clustering of Learners Performance Levels Using Machine Learning Techniques. Revue d'Intelligence Artificielle, 2021, 35(1).
61. Mohemad R, Muhait NNM, Noor NMM, Othman ZA. Performance analysis in text clustering using k-means and k-medoids algorithms for Malay crime documents. International Journal of Electrical and Computer Engineering (IJECE). 2022;12(5):5014-5026.
62. Ekhande S, Patil U, Kulhalli KV. Review on effectiveness of deep learning approach in digital forensics. International Journal of Electrical & Computer Engineering. 2022;12(5):2088-8708.
63. Casino F, Dasaklis TK, Spathoulas GP, Anagnostopoulos M, Ghosal A, Borocz I, *et al*. Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access. 2022;10:25464-25493.
64. Sharma M, Luthra S, Joshi S, Kumar A. Implementing challenges of artificial intelligence: Evidence from public manufacturing sector of an emerging economy. Government Information Quarterly. 2022;39(4):101624.