# The Machine Learning Approach to Digital Forensics: A Review of Literature

Andrew Simon
ajsimon1818@gmail.com
*College of Computing, University of North Florida*, Jacksonville, FL, USA

***Abstract*—The field of Digital Forensics is currently facing new challenges as the scope of digital evidence scales in both diversity and size. Investigators struggle to efficiently work through evidence, detect malicious intent, and enact justice on criminals. However, professionals in the field of computing have adapted machine learning technology to these efforts as a means of automating this tedious process. In this paper, we discuss the proposed methodology of these researchers, the different regions of forensics that can benefit, and the statistical impact they can create in investigations. Several algorithms, including SVM, Decision Tree, Random Forest, and Naive Bayes Classification, are utilized to address concerns in various evidence data types. These methods primarily strive to enhance the ease and accuracy of detecting audio/image tampering as well as performing language analysis. The inclusion of machine learning technologies in the Digital Forensic field aims to bolster the investigators' toolbox to properly defend against the ever-evolving complexity of threats and datasets.**

## I. INTRODUCTION

### *A. Digital Forensic Challenges*

The field of digital forensics encompasses all the computing processes and processing techniques used to analyze digital evidence in criminal investigations. These online pools of evidence have proliferated in the past three decades, resulting in oceans of data that investigators must parse through to produce justice [1]. In 2020, reports showed that 49.7% of the world's population is connected to the Internet, with a 936% growth rate. [2] Investigators must adapt a toolkit capable of matching this incredible growth of digital evidence. This paper aims to analyze how machine learning technology can efficiently identify and process this evidence in these overwhelming datasets.

### *B. E-Discovery*

The process in which this electronically stored information (ESI) is identified, collected, or produced is referred to as electronic discovery (e-Discovery). This phenomenon, while not initially heavily correlated to the IT field, is increasingly being tethered to computing as investigators find the need to discover evidence online [7]. E-Discovery is the realm where the computing processes meet the law procedures as a means to use the ESI in court as evidence. When in the e-Discovery process, investigators must adhere to the guidelines and regulations of standard sets such as Federal Rules of Civil Procedure (FRCP), Federal Rules of Evidence (FRE), and Federal Rules of Criminal Procedure (FRCrP). Once investigators navigate the challenges of discovering evidence in the vast and varied datasets of ESI, they must also overcome the challenge of successfully aligning this evidence to be used in court.

### *C. Machine Learning Approach*

Machine learning in the field of forensics is based on the idea of training algorithms for detecting and analyzing data to discover evidence and identify usable patterns. These algorithms can automatically analyze large online datasets, trained to handle the increasing variety of data types. This paper discusses their implementation with text log, image, and audio sample data types. The algorithms showcased follow both supervised and unsupervised learning methods. Supervised training allocates examples to a set of classifications, whereas unsupervised training does not know the labels from the start [8]. Unsupervised training is often referred to as a Clustering algorithm and lends itself to targeting similarities between different samples based on features and data types.

## II. METHODS

### *A. Mobile Forensics*

The global security index in 2017 reported that roughly 80% of adults worldwide would be using a smartphone by 2020. These devices serve as the communication platform for many daily activities, including work operations, social interactions, and entertainment. This constant online presence leads to a vast surface area for criminals to target and generates a massive online fingerprint for the user. Mobile forensics

looks to analyze the user's SMS messages, call records, images, etc., to develop a profile and describe a pattern of activity [3].

Many tools currently available in the mobile space are commercial. While these tools provide a robust array of utilities, they can be quite costly. This can be alleviated by some of the open-source tools on the Android and IOS markets [13]. Linux Memory Extractor (LiME), for example, can be used for memory data collection in Android phones, and iPhone Backup Manager helps with access to analyze IOS device backups. While these tools don't provide the full utility needed for an investigation, they can be valuable to the overall process.

*1. Emails*

K. Uma Maheswari and S. Nikkath Bushra [9] propose a clustering algorithm method in which they attempt to detect e-mail fraud. Once detected, the fraudulent components of the e-mail are sent to the algorithm for further training. Their three-step process includes the following:

- Forensic Data Acquisition/Preprocessing
- Adaptive Acquisition of Source of Attack
- Evidence Isolation/Presentation

Machine learning training used a dataset of 50,000 emails from the Enron Corporation with information collected on the sender, receiver, time, and date of the user. The information is stored in a cloud virtual machine for further analysis by the Enhanced Forensics Fuzzy C-Means (EFFCM) clustering algorithm. This model aims to identify and then group the data flagged as malicious. Once formed, the features of these clusters can start to help identify the source of the attack. The prototype then isolated the evidence in another VM to be analyzed without the risk of data breaches and to avoid service interruption. Law enforcement can then use snapshots from the VM as admissible evidence with a chain of custody in court.

K. Debnath and N. Kar's [19] work addresses email spam detection with the use of deep learning techniques (LSTM, Bidirectional LSTM, and Bidirectional Encoder Representations from Transformers (BERT)). Data is processed using NLP and word embedding methods for smooth analysis by deep learning algorithms. The word embedding methods used in this research are count vectorizer (converts text into a vector based on the amount of usage of a word) and TF-IDF Vectorizer, which uses term frequency and inverse document frequency for vectorization.

This work compares its results to those of similar studies using machine learning algorithms, showing a slight increase in consistency of accuracy. The overall accuracy of both approaches is relatively high (above 83%), but the deep learning methods of this work show an impressive >97% accuracy for all three algorithms used.

*2. Text Data/SMS*

A. Aydogen and N. Sashidhar [7] developed a method attempting to detect malicious words and sentences in online learning environments. The crux of this method focuses on using Natural Language Processing (NLP) to sanitize the text data for efficient processing through Logistic Regression, Support Vector Machine (SVM), and k-nearest neighbors (KNN) algorithms.

The work utilized several methods of normalizing the data using NLP, including:

a. Tokenization: Breaking down sentences into individual words and, in some cases, further into word parts. This process breaks the data into digestible tokens for the algorithms to process.
b. Stemming: Algorithms to remove word affixes that could confuse the data processing and decrease accuracy.
c. Lemmatization: Similar to stemming but with the added intelligence to produce the word's main state/root meaning. In some cases, this process can result in using a general synonym.

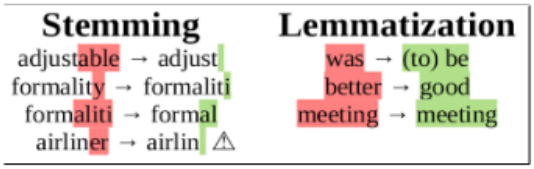


Figure 1: Differences Between Stemming and Lemmatization. Adapted from [7]

d. Stop-Words: Eliminating words deemed unnecessary to meaning, such as prepositions or post-positions.
e. Punctuation/Spell Checking: Eliminating punctuation, letter capitalization, and general spell checking.

Once sanitized, the researchers compared this data with several trained datasets of flagged violent words and behavioral training. Two strategies we attempted focused on detecting violent words and violent sentences. The aim here was to determine if the algorithms could successfully detect malicious intent in a single word or if the added context of other words in the sentence would better frame the intent of the target word.

L. Peng et al. [3] proposed a method of detecting spam SMS messages in smartphones to help investigators filter out illegitimate communications between users. Their strategy utilized a Naïve Bayes algorithm to classify the data as spam or legitimate. Then, they used a

partitional clustering algorithm (K- means) to further segregate the evidence into groupings for deeper analysis.

This usage of machine learning allows investigators to minimize the amount of data that is needed to be analyzed by identifying and removing useless input, then categorizing the valuable data as evidence for proper analysis and usage in court.

*3. Method Comparison*

All methodologies of analyzing text data began with a preprocessing step focused on sanitizing the data for smooth analysis through machine learning algorithms. When training for processing this type of data, it seems necessary to break down the terms into the most digestible form using NLP and/or word embedding techniques to reduce errors and increase processing speed.

Whether concerned with detecting spam messages or human emotion/intent, the machine learning algorithms must be trained using a robust array of datasets to capture the nuance of the written language (English, in this case). The ability to properly detect legitimate meaning from the text data appears to rely heavily on the size and variety of the datasets used for training.

In many of the studies, efficiency was significantly increased by the usage of clustering algorithms in the later steps to further categorize the evidence into more specific groupings for analysis. This step goes beyond simple binary detection and provides investigators with deeper insight to filter evidence in more applicable means.

For performance, the results of the methods used were all relatively successful (Ranging from 83% to 98%), but the deep learning algorithms showed a slight edge in consistency (All above 97%). When it comes to language analysis, the ability of a deep learning algorithm to attempt to mimic human thinking may closer resemble the patterns involved in word meaning/choice than the machine learning alternatives.

*B. Audio Forensics*

Audio clips are vital in some criminal cases to help authenticate the voice of suspects or victims. This data is easily manipulated with the array of open-source tools on the market. Audio forensics aims to detect tampering techniques such as splicing, deletion, or copy-move [4]. These acts, or even the verification of data purity, help investigators authenticate the data for use in court. A primary challenge investigators face with this data type is overcoming environmental data that could skew the target audio data. Researchers are starting to both deafen and, in some cases, utilize this environmental noise to better craft the desired evidence [20]. Studies suggest that usage of this data can better contextualize the full picture of the scene in which the targeted audio exists.

*1. Speech Recognition*

L. Peng and X. Zhu [10] focused their research on using machine learning techniques to detect Chinese dialects to geolocate criminals in China. They suggest that the incredibly large population, with 56 nationalities using various dialects, has easy access to open-source voice communication tools, such as QQ and WeChat, allowing for a broad data pool investigators must navigate. They note that many criminal gangs in the country utilize these software apps and tend to use distinct dialects and colloquial language. The method centers around Long Short-Term Memory (LSTM) neural networks for detecting these dialects in the audio data.

Speech recognition techniques often use pattern recognition and probability statistics to recognize a specific human voice accurately. This work suggests such models as Baum-Welch, Good-Turning, Maximum Likelihood Evaluation, and Minimum Phone Error models are effective tools in this effort.

The neural networks in their methodology follow a four-step process to analyze the voice audio data, including preprocessing, feature extraction, speech recognition algorithm (neural network model), and recognition results. A recurrent neural network (RNN) was tested for the best effect; however, the algorithm suffers from a vanishing gradient issue. To alleviate this problem, the LSTM method was proposed. In tandem with the traditional RNN, this method aims to detect Chinese dialects in the data efficiently.

F. Zhang et al. [17] also attempted to use machine learning for speech recognition to detect different Chinese dialects. They use an end-to-end neural network, using an attention mechanism to reduce the character error rate (CER) in discerning characters in spoken Chinese dialects. This method removes the RNN component, simply relying on the attention mechanism, which they claim improves its ability for speech recognition. Their results show a 12% improvement in CER from the baseline using their methodology.

D. Bharti and P. Kukana [18] address machine learning's ability for emotion detection in speech recognition. Their proposed methodology is composed of seven steps:

- The speech signal is initialized, checking the load and input, focusing on duration and frequency.
- Elimination of noise interference for better clarity of the signal. High Pass Filter (HPS) is

used in this effort.

- The Gateway Feedback Congestion Control (GFCC) algorithm is used for feature extraction.
- The Ant Lion Optimizer (ALO) algorithm is used to select features based on pitch, entropy, and energy.
- The Multi-Class SVM algorithm is used to train the speech data and input samples.
- MSVM model is used again to verify the speech samples, process data, and training.
- The output is compared to the training features to determine if there is a match, detecting a specific emotion in the speech data.

*2. Audio Tampering*

Audio authentication is a crucial process in digital forensics as researchers attempt to detect the tampering of audio data in investigations. V. Rahinj et al. [4] propose a method to detect audio tampering based on supervised learning and active learning techniques.

For the supervised learning approach, only labeled data was used for training, marked tampered or untampered. They used the Free-Spoken Digit Dataset (FSDD), containing spoken digits (0-9) at 8kHz in ".wav" format. Fifty recordings per each of the six speakers provided a dataset of 3,000 recordings for use. This data was tampered with using copy and move, splicing, and insertion/deletion. This work focuses on copy and move tampering, where a portion of one audio sample is copied and pasted into another. The PRAAT software generates this tampering, resulting in a total of 6,000 audio samples, half of which are tampered with and half untampered.

This approach looks at six different features for extraction, which in combination help to determine accuracy. These features include:

- Mel-Frequency Cepstral Coefficients (MFCC) – To determine these features, a signal is run through a triangle filter pool on a non-linear Mel-Frequency scale. Using discrete cosine transformation (DCT), the final features are determined after being logarithmically compressed.
- Zero Crossing Rate (ZCR) – This feature targets the rate at which the audio signal changes from positive to negative or vice versa. It helps in both voice recognition and the detection of percussive sounds.
- Root-Mean-Square Energy (RMSE) – Evaluates the volume of an audio signal by analyzing the magnitude and energy of the signal.
- Spectral Centroid – A measurement that defines the spectral center of mass of a spectrum of the audio signal.
- Spectral Bandwidth – The calculation of the difference between lower and upper frequencies on a continuous grouping of frequencies.
- Short-Time Fourier Transform (STFT) – These calculations are used to analyze several aspects of the audio signal, such as noise reduction and pitch detection/shifting.

With the class labels of each file known, the combination of tampered and untampered files, combined with these calculated features, is processed through training and testing data at a ratio of 70:30. For training purposes, this model uses the Random Forest, AdaBoost, XGBoost, KNN, and SVM machine learning algorithms. The model is then tested on the dataset to determine the accuracy of each of the mentioned algorithms.

This work also compares this method to an active learning approach, using labeled and unlabeled data. They suggest the benefit of this approach is the usage of large amounts of easy-to-access unlabeled data. The smaller portion of labeled data is used to train the model so that it can be used to predict the labels of the unlabeled data. The predictions are then used to compare the observations to their predefined criteria. These predictions are combined with the labeled data and compared for accuracy using the different classifier algorithms.

*3. Method Comparison*

Similar to the sanitization of the written text in the mobile forensic section, audio forensic methods tend to have an initial step in purifying the targeted audio sample. Most saw the environmental background noise as interference and thus irrelevant data that simply slowed down the analysis process or increased errors. The studies that were concerned with speech detection wanted to isolate the targeted user's speech to increase clarity, but the studies looking for audio tampering treated the entire audio sample as valuable. In some cases, tampering detection was identified primarily by noticing manipulation of the environmental audio.

Both studies attempting to identify Chinese dialects had successful results with similar methodologies using an RNN as a foundation and modifying for efficiency. [10] proposes classifiers to discern between the dialects found in the samples, followed by using an LSTM neural network to automatically detect specific dialects. [17] suggests deviating from the neural network approach, leveraging Connectionist Temporal Classification (CTC), and using an Attention Structure.

There is some added nuance for speech detection

when analyzing the methods concerned with detecting Chinese dialects and identifying emotional intent. The studies on Chinese dialects note the language's use of a character system. This system lends itself to a relatively straightforward approach of matching these characters to a dataset developed in training. To accurately detect emotion in audio data, training needs an additional layer concerned with interpreting emotional meaning from the data.

### C. Image Forensics

Similarly to its audio counterpart, image data suffers from the broad access to editing tools available to users online. Tampered images are being used to negatively impact the reputation of organizations by falsifying events or actions [5]. Researchers extract data on features such as shape, color, and texture to help determine if there are any irregularities in the image [6].

Image data faces an array of difficult-to-detect image forgery techniques that investigators must overcome. The "copy move" method consists of copying one portion of the image and pasting it to another to hide or highlight a desired area. Retouching is used to lessen or enhance the quality of an image, sometimes requiring it to be enlarged, shrunk, or rotated. Splicing is similar to copy move but uses more images than just the original. Multiple images can be spliced into the original, creating a new depiction altogether [15].

#### 1. Image Manipulation

Investigators must be able to properly authenticate image data and detect any tampering with the data. S. Kumar et al. [6] attempt to accomplish this goal by analyzing the illumination inconsistency principle provided by Illuminant Maps (IM). Two algorithms (Generalized Grayworld Estimates (GGE) and Inverse Intensity Chromaticity (IIC)) are applied to detect image splicing, using feature extraction data on color, shape, and texture. For feature extraction, the algorithms tested are SVM, KNN, and GLCM, while the proposed methodology uses GLCM and Speed Up Robust Feature (SURF).

Once fake regions of the images are identified, they are processed through the IM to analyze the features. This approach obtains two types of image intensities: diffuse and specular reflectance. Similar to light scattering principles and light reflection, respectively. The forgery is then classified using SVM, KNN, Naïve Bayes, and Decision Tree algorithms.

S. Thepade et al. [14] also addressed the concern of image splicing, using Thepade's Sorted Block Truncation BTC algorithm (TSTBTC) for feature extraction on R/G/B color indicators of the image. Once extracted, these features are used to train several classifiers for an ensemble, majority voting method of detecting image splicing. Their results show a range between 49% to 64% accuracy, with LMT, Simple Logistic, and Logistic classifier algorithms providing the strongest outcomes.

#### 2. Image Source/Time Identification

H. -T. Wang and P. -C. Su [11] proposes a method of detecting image manipulation focused on camera model identification. They suggest the wide variety of image tampering techniques makes collecting tampered image data for supervised training difficult. They aim to avoid this issue by examining data from original images. Firstly, a neural network is trained to obtain features that accurately locate camera models. They then use a Siamese network to analyze the consistency between block pairings to determine if the image has any manipulated sections.

The neural network is convolutional and is trained for feature extraction. The training process uses different camera models than this step to better develop the capability of determining unknown models. The parallel networks in the Siamese model allow for the features in each block (one block from the pair in each network) to identify similarities in them. Once added together and combined with the convolutions of the neural network, the blocks are evaluated to determine consistency.

F. Ahmed et al. [16] attempt to use deep learning to estimate the acquisition date of image data. The so-called temporal forensic analysis aims to determine the time between two pieces of image evidence. With open-source editing tools, perpetrators can easily alter image time stamps, and it is crucial that investigators can compare for validity. The methodology uses CNNs (AlexNet and GooLeNet) for feature extraction and k-NN/SVM classifiers.

They claim that in previous studies, CNN networks look at the contents of people of settings in the images (hair, clothing, accessories, etc.) or historical events to be able to identify year ranges. Others developed a method using a single reference image of comparison to determine if the target image was older or newer. This research aims to be the first to detect image date through classification using their own Northumbria Temporal Image Forensics (NTIF) database.

This database features ten different digital cameras recording natural scenes at up to 71 different timeslots with a timespan of 1-2 weeks in each timeslot. The set of 41,684 images of indoor and outdoor scenery can be used for image authentication, camera model identification,

and image date verification.

### 3. *Method Comparison*

As seen with audio tampering, when concerned with image tampering, all methods include some type of feature extraction and analysis. Researchers are able to isolate these characteristics of each data sample to train their algorithms to filter and compare based on more specified criteria. [6] utilized features connected to light behavior (illumination consistency and light scattering) and the image's shape, color, and texture. [17] only extracted R/G/B pixel values. The former compared several machine learning algorithms for classification, producing a range of successful detections between 76% and 83%. The latter chose to implement an ensemble, majority voting method using deep learning techniques across three different datasets, only resulting in a 62% best success rate. When comparing the two methods, it is difficult to determine if the resulting discrepancy is caused by the difference in the number of features extracted or the algorithm approach itself.

The methods examined for camera model and time detection both heavily rely on training a neural network. [16]'s work seems to almost be an extension of [11]'s, where the framework is functionally the same. However, the former extracts more features and attempts to identify the type of camera used to capture the image and verify the relative date it was taken.

Both frames of focus demonstrate the addition and increase of variety in features extracted can lead to both an increase in accuracy and the amount of information the evidence can provide.

## III. Findings

When processing data to run through a machine or deep learning algorithm, there seems to be a strong increase in efficiency by a preprocessing stage that sanitizes the data to ensure the accuracy of data interpretation. NLP/word embedding in text analysis and noise suppression/isolation in audio analysis allow the algorithm to process only the necessary information. This effect is shown at a macro level when attempting to filter out legitimate text or fraud messages while processing text data.

Some of these methods seem to be extensions or evolutions of others in the review. Machine learning technology has the nature of growth and the ability to increase the system's capabilities. Some studies aim to simply detect valuable evidence in a sea of meaningless communication data, some pursue further by classifying the detected evidence, and some even make decisions based on those classifications. The power of a machine-learning-based solution is directly tied to the training that can be given to the system. Once the foundation of these systems has been built and tested, they have the increased opportunity to become more efficient and capable.

With concern to security, a machine algorithm approach to digital forensics would be an extremely efficient use of resource allocation, lead to quicker detection of data tampering, and prevent users from interacting with potentially malicious attack attempts. The modern datasets forensic teams must parse are becoming unfeasible for analysts to navigate without the use of automation. With proper training, machine learning provides this automation and can produce similar accuracy to a human with much more speed. In conjunction with other detection tools, such as IDS or Firewalls, machine learning techniques can be trained to detect any desired information type quickly. Investigators could use an audio recording device to alert them of a wanted suspect's voice after it's trained, or programs could be built to prevent adware by filtering out all illegitimate messages. This filtering can alleviate the overwhelming issue of user mistakes by removing the option to even interact with spam or phishing attempts.

Not only is a machine learning approach to digital forensics an inevitable necessity to compete with the evolution of modern electronic datasets, but it is also an opportunity to expand our security capabilities to be more efficient than ever.

## IV. Conclusions

With every passing day, the size and variety of electronically stored information proliferate towards an environment where investigators will be unable to efficiently attain evidence. The current toolset available in digital forensics does not have the capability to compete with the challenges these enormous datasets pose. The time and money loss of using traditional, non-automated means of data parsing and collection could exceed the loss of not finding the evidence at all. Digital forensic investigators must develop an appropriate set of tools to match this growth in data.

Machine learning technology, as a solution to this issue, provides automation of the process with both speed and accuracy. These algorithms can be trained to differentiate between these diverse data types for proper categorization and identify desired evidence based on given criteria.

However, machine learning is weak in being susceptible to zero-day attacks or any new methods of tampering. Training for these algorithms usually requires known methodology or signatures for it to make decisions successfully. This shortcoming may lead to false

positives/negatives in the system, but the speed and relative accuracy of the technology more than compensates for it [12]. As these novel methods enter the dataspace, the algorithms can be swiftly trained to handle the threats they present.

Future work for this research will focus on how machine learning techniques can benefit other areas in digital forensics and address the idea of aggregating the functionalities mentioned into a singular tool for increased efficiency when navigating entire datasets rather than segmented, partial ones. The work so far has developed a solid foundation for investigators to leverage machine learning in their efforts. I believe the future of this tool is its development as the primary means of data analysis and collection for all types and sizes of datasets.

## V. REFERENCES


[1] A. M. Qadir and A. Varol, "The Role of Machine Learning in Digital Forensics," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beruit, Lebanon, 2020, pp. 1-1, doi: 10.1109/ISDFS49300.2020.9116298

[2] Ibrahim Goni, Jerome Mishion Gumpy, Timothy Umar Maigari, Murtala Muhammad, Abdulrahman Saidu. "Cybersecurity and Cyber Forensics: Machine Learning Approach", Machine Learning Research. Volume 5, Issue 4, December 2020, pp. 46-50. doi: 10.11648/j.mlr.20200504.11

[3] L. Peng, X. Zhu and P. Zhang, "An Efficient Model for Smartphone Forensics Using SMS Spam Filtering," 2020 3rd International Conference on Hot Information-Centric Networking (HotICN), Hefei, China, 2020, pp. 166-169, doi: 10.1109/HotICN50779.2020.9350843.

[4] V. Rahinj, R. Patole and S. Metkar, "Active Learning Based Audio Tampering Detection," 2022 International Conference on Connected Systems & Intelligence (CSI), Trivandrum, India, 2022, pp. 1-5, doi: 10.1109/CSI54720.2022.9923997.

[5] R. Shao and E. J. Delp, "Forensic Scanner Identification Using Machine Learning," 2020 IEEE Southwest Symposium on Image Analysis and Interpretation (SSIAI), Albuquerque, NM, USA, 2020, pp. 1-4, doi: 10.1109/SSIAI49293.2020.9094618.

[6] S. K. N, K. M and V. S P, "Image Splice Detection based on Illumination Inconsistency Principle and Machine learning Algorithms for Forensic Applications," 2021 Smart Technologies, Communication and Robotics (STCR), Sathyamangalam, India, 2021, pp. 1-4, doi: 10.1109/STCR51658.2021.9587928.

[7] A. F. Aydogan and N. Shashidhar, "Prevention Pre-Violence in E-Labs with Machine Learning: PVE," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, pp. 1-5, doi: 10.1109/ISDFS52919.2021.9486349.

[8] L. Peng, X. Zhu and P. Zhang, "A Machine Learning-Based Framework for Mobile Forensics," 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 2020, pp. 1551-1555, doi: 10.1109/ICCT50939.2020.9295714.

[9] K. U. Maheswari and S. N. Bushra, "Machine learning forensics to gauge the likelihood of fraud in emails," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1567-1572, doi: 10.1109/ICCES51350.2021.9489015.

[10] L. Peng, X. Zhu and P. Zhang, "Machine Learning-Based Speech Recognition of Chinese Dialects Method for Mobile Forensics," 2021 13th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, 2021, pp. 332-336, doi: 10.1109/ICCSN52437.2021.9463649.

[11] H. -T. Wang and P. -C. Su, "Deep-Learning-Based Block Similarity Evaluation for Image Forensics," 2020 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan), Taoyuan, Taiwan, 2020, pp. 1-2, doi: 10.1109/ICCE-Taiwan49838.2020.9258247.

[12] S. Qadir and B. Noor, "Applications of Machine Learning in Digital Forensics," 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2), Islamabad, Pakistan, 2021, pp. 1-8, doi: 10.1109/ICoDT252288.2021.9441543.

[13] V. Fernando, "Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges," 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 2021, pp. 1-7, doi: 10.1109/NTMS49979.2021.9432641.

[14] S. D. Thepade, D. M. Bakshani, T. Bhingurde, S. Burghate and S. Deshmankar, "Performance Appraise of Machine Learning Classifiers in Image Splicing Detection using Thepade's Sorted Block Truncation Coding," 2020 IEEE Bombay Section Signature Conference (IBSSC), Mumbai, India, 2020, pp. 16-20, doi: 10.1109/IBSSC51096.2020.9332167.

[15] M. S. Khazaal, M. Kherallah and F. Charfi, "An Overview on Detecting Digital Image Splicing," 2022 International Arab Conference on Information Technology (ACIT), Abu Dhabi, United Arab Emirates, 2022, pp. 1-4, doi: 10.1109/ACIT57182.2022.9994194.

[16] F. Ahmed, F. Khelifi, A. Lawgaly and A. Bouridane, "Temporal Image Forensic Analysis for Picture Dating with Deep Learning," 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 2020, pp. 109-114, doi: 10.1109/iCCECE49321.2020.9231160.

[17] F. Zhang, X. Xie and X. Quan, "Chinese Dialect Speech Recognition Based on End-to-end Machine Learning," 2022 International Conference on Machine Learning, Control, and Robotics (MLCR), Suzhou, China, 2022, pp. 14-18, doi: 10.1109/MLCR57210.2022.00012.

[18] D. Bharti and P. Kukana, "A Hybrid Machine Learning Model for Emotion Recognition From Speech Signals," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 491-496, doi: 10.1109/ICOSEC49089.2020.9215376.

[19] K. Debnath and N. Kar, "Email Spam Detection using Deep Learning Approach," 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), Faridabad, India, 2022, pp. 37-41, doi: 10.1109/COM-IT-CON54601.2022.9850588.

[20] S. Chandrakala and S. L. Jayalakshmi, "Generative Model Driven Representation Learning in a Hybrid Framework for Environmental Audio Scene and Sound Event Recognition," in IEEE Transactions on Multimedia, vol. 22, no. 1, pp. 3-14, Jan. 2020, doi: 10.1109/TMM.2019.2925956.