International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
OPEN ACCESS
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST

Statistical Analysis of Deep Learning Models Used for Social Media Forensics from An Empirical Perspective

Mayuri Gaikwad [1], Prof. Abhimanyu Dhutonde [2]

[1]PG Student, Department of Computer Science and Engineering, TGPCET, Nagpur , Maharashtra, India
[2] Head of Department of Computer Science and Engineering, TGPCET, Nagpur, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 01 Sep 2023
Published: 08 Sep 2023

Publication Issue
Volume 10, Issue 5
September-October-2023
Page Number
46-64

ABSTRACT

The prevalence of social media platforms in the digital age has brought forth hitherto unheard-of difficulties in assuring the accuracy and integrity of information shared through these channels. The growing prevalence of fake news, misinformation, and manipulative content highlights the need for effective tools and approaches to evaluate the reliability of online content. This work launches a thorough investigation of deep learning models used for social media forensics in answer to this pressing requirement, founded in actual data and statistical analysis. The importance of social media platforms in influencing public conversation, opinions, and even the political and social landscapes makes this study necessary. Maintaining informed democratic societies and preserving the credibility of online information sources depend on our capacity to distinguish between genuine and misleading content. By rigorously examining the effectiveness of deep learning models in tackling the issues presented by the proliferation of false material on social media, this study aims to close the gap in previous studies. The review procedure used here uses a two-pronged strategy. An extensive survey is first done to find and compile a range of deep learning models specifically designed for social media forensics. These models incorporate a wide variety of methodologies, such as network analysis, image analysis, and natural language processing. The ensuing empirical phase, which makes use of a wide range of actual social media datasets for rigorous review, is contextualised by this first stage of the process. The empirical evaluation looks closely at how well these models perform on many dimensions. To assess their capacity to distinguish between authentic and manipulative content, precision, recall, and accuracy metrics are selectively applied. To ensure the models' viability in the actual world, computational effectiveness and scalability are also taken into account. These dimensions' intersection offers a comprehensive picture of the models' advantages and disadvantages.

Keywords: Deep Learning Models, Social Media Forensics, Empirical Perspective, Statistical Analysis, Deceptive Contents

I. INTRODUCTION

Social media platforms have evolved into powerful channels that organise information transmission, mould public views, and spark societal conversation in the modern digital landscape. The pervasive spread of false information, edited content, and misleading narratives, however, has been paired with an unprecedented difficulty that has never before existed in the history of information dissemination. A paradigm shift in the technologies and procedures used to maintain the legitimacy and authenticity of content circulating on social media platforms is required due to the ensuing erosion of trust in online information sources. In this context, the current work begins a thorough investigation of deep learning models used to social media forensics, founded in an empirical viewpoint and strengthened by meticulous statistical analysis.

The necessity of this effort is highlighted by the crucial part social media platforms play in determining public opinion, affecting political environments, and determining the course of modern societies. The integrity of democratic discourse is visibly threatened by the flood of misinformation, which is propelled by malicious actors and magnified by artificial echo chambers. Maintaining the informed decision-making processes that support democratic societies depends critically on the accuracy of the information conveyed over these digital channels. As a result, there is an urgent need for creative tools and methods that go beyond the obvious and explore the intricate nuances of online information. This work aims to fill this urgent demand by emphasising deep learning models as effective tools for strengthening the foundation of social media forensics.

The primary justification for this study stems from the paucity of thorough empirical studies that systematically examine the effectiveness of deep learning models used in the field of social media forensics. Although there are many theoretical frameworks available in academia, real-world data-based evaluations of these models are still comparatively rare. This study devotes itself to undertaking a multidimensional examination of deep learning models, evaluating their performance across various dimensions, and determining their applicability in the real world in order to address this major gap.

A thorough two-tiered process precisely defines the methodological trajectory of this study journey. A thorough analysis of current deep learning models that have been modified for social media forensics is the first step in the foundational phase. These models cover a wide range of approaches, such as network analysis to look at propagation patterns, image analysis to analyse visual information, and natural language processing to analyse textual content. This thorough analysis not only provides a solid foundation for the upcoming empirical investigation, but it also explains the many ways deep learning can be used to counter false information.

The empirical phase, which is the core of this study and is distinguished by its quantitative rigour. The identified models are rigorously evaluated using a

wide range of real-world social media datasets as the testing ground. The foundation of assessment is a plethora of performance measurements, including precision, recall, F1-score, and accuracy. These metrics provide detailed insights into the models' efficacy by measuring the algorithms' overall ability to distinguish between real and fake information. In addition, these models' computational effectiveness and scalability are assessed while taking into account the practical limitations that govern their application in the actual world.

The remainder of this paper unfolds in painstakingly organised sections that are meant to provide insights in a natural development. Section II conducts a thorough analysis of the current literature, illuminating the theoretical foundations and placing the models in the context of the developing field of social media forensics. The methodological framework is explained in Section III, which also outlines the parallel phases of literature review and empirical evaluation. The empirical results are presented in Section IV, together with a detailed evaluation of the effectiveness of the deep learning models. Dissecting the significance and practical ramifications of the findings, Section V engages in academic dialogue. The paper comes to a close in Section VI, where the collective observations are condensed into summative observations that emphasise the importance of deep learning models in battling false information on social media platforms.

II. LITERATURE REVIEW

A wide variety of models are proposed for social media forensic analysis, and each of these models vary in terms of their real-time characteristics. As the world transitions into the twenty-first century, a study [1] examined the growing importance of social media communication in individuals' daily lives. In addition to the undeniable benefits, a variety of unanticipated results have emerged, including the widespread dissemination of deceptive information motivated by malign intent, which is frequently facilitated by the use of fabricated personas or the veil of anonymity. In view of the widespread use of text messages on social media platforms, which are characterised by an abundance of brief messages and a large number of users, addressing this issue presents a formidable challenge. Identifying the author of such communications presents challenges, but it remains a strategic method for addressing the problem of disinformation. This study examines the issue of identifying the authorship of concise communications. In contrast to other studies that have examined extended texts, our methodology is data-driven. We avoid using manually derived features for pattern recognition and instead rely on advances in deep neural networks. To facilitate the projection of these messages onto a manifold appropriate for the task of authorship attribution, we propose employing a deep learning model that renders the condensed phrases used in social media as unidimensional signals. In the context of authorship verification, we offer two state-of-the-art solutions that were devised to accommodate a variety of circumstances and approaches. Three additional contributions facilitated the feasibility of these advancements: an enhanced dataset derived from the Twitter® platform, novel techniques for improving the quality of the training data, and cutting-edge visual analytics tools to aid in the development of authorship attribution solutions.

The article cited in [2] discusses the emergence of social media as an integral part of the global news creation and dissemination process in recent years. Sadly, the advent of digital platforms and their user-friendly modification capabilities have facilitated the widespread dissemination of false or misleading information through visual representations. Due to its complexity and the limitations of the computational tools currently used in newsrooms, the verification of visual content poses significant challenges for media professionals and fact-checkers. Consequently, these individuals continue to struggle to effectively and

exhaustively examine and refute visual user-generated content (UGC). This study aims to provide a prospective view of the potential impact of multimedia forensics research on the substantiation of user-generated visual content in the field of journalism. A thorough examination of the five constituent elements of UGC verification is conducted, with a proposal to introduce multimedia forensics as a sixth element. The research community in computer science has exhaustively documented several instances of visual content forgeries, as well as the methodologies used to detect them. To engender confidence among media professionals in the routine use of multimedia forensics techniques, the purpose of this study is to compile a compendium of currently employed verification methods, along with an evaluation of their limitations and future research prospects.

The identification of the social network from which a digital video originated has the potential to aid law enforcement and intelligence agencies in locating the individuals responsible for producing deceptive visual content, according to the findings of a study conducted by researchers [3]. Recent developments in the field of video forensics have demonstrated that the structural characteristics of video containers have considerable potential for identifying and analysing the originating social network. Existing studies do not account for the possibility that a nefarious user could effortlessly reconstruct the container without the need for transcoding, erasing all traces of the existence of the social network. This correspondence describes a method for determining the social network of origin for a video, even when the video's container structure is completely incorrect. The proposed method employs statistical analysis of Discrete Cosine Transform (DCT) coefficients to characterise the various encoding attributes of social media platforms. We have effectively curated and produced an extensive collection of over a thousand films originating from a variety of sources, including original creations, modified versions, and those disseminated via social media platforms, thanks to our diligent efforts. This exhaustive compilation seeks to aid professionals in the field of forensic investigation in their exploration of this topic.

As demonstrated by the research cited in [4], attributing authorship to online works is crucial in the struggle against cybercrime. Several platforms implement restrictions on the utmost length of text, which exacerbates the difficulty of the current mission. The purpose of our research is to identify the originator of 140-character Twitter messages. In our analysis, we evaluate prominent stylometric features frequently employed in literary criticism, including URLs, hashtags, reactions, and quotations, among other Twitter-specific characteristics. This research utilises two datasets, one containing 93 authors and the other containing 3957 authors. We conduct investigations by varying the number of author sets as well as the quantity of training and test texts for each author. Utilising automatic feature selection enhances efficacy further. Despite the incorporation of multiple authors and a large number of training Tweets (over 500), a small number of test Tweets can still provide a high degree of accuracy (with a Rank-5 over 80%). Using reduced sample sizes, specifically 10 to 20 Tweets for training, has the potential to reduce the search space by 9 to 15%. Despite the reduction in size, there is a high likelihood of identifying the correct candidate among the remaining candidates. In certain circumstances, the use of automatic attribution has the potential to substantially reduce the amount of time consumed by specialists conducting suspicious search activities. We deliver verification results proportional to the scope of the subject matter. The error rate (EER) decreases from 20 to 25% to 15% as the number of training Tweets increases from a few to hundreds. In addition, we evaluate the computational complexity and durability of the employed attributes.

In a scholarly publication by Work (5), the topic of discussion is the potential abuse of Linguistic steganography in social networks, which has the potential to cause significant harm to a variety of aspects including network security, personal privacy, and national defence. Due to the accelerated expansion of the internet and social media platforms, this concern arises. Numerous linguistic steganalysis methods are currently being proposed in an effort to identify potentially detrimental steganographic carriers. However, most existing methodologies are ineffectual when applied to authentic social networks due to their extensive lack of connections and substantial fragmentation issues. This is due in part to the fact that these approaches prioritise insufficient linguistic characteristics. This initiative seeks to address the persistent dearth of exhaustive datasets and efficient algorithms for identifying steganographic texts within social network environments. To accurately simulate authentic social network environments, the Stego-Sandbox dataset has been painstakingly constructed. This dataset contains a selection of characters and their respective associations. In addition, we provide a comprehensive framework for linguistic steganalysis that combines text-extracted linguistic components with contextual information represented by the provided connections. The empirical evidence indicates that our proposed framework has the potential to significantly enhance the detection capabilities of existing techniques in actual social network environments. This enhancement is accomplished by effectively resolving the limitations of conventional methods and accumulating contextual data samples.

The applications of social algorithms are diverse and may have positive outcomes. However, a study conducted by researchers [6] examined social bots' ability to manipulate individuals and spread malicious software. Consequently, it is necessary to identify and locate active algorithms on social networking platforms. Recent advancements in artificial intelligence have led to significant improvements in social bots' capacity to generate posts with human-like characteristics. Therefore, it is necessary to employ more intricate methods to locate them. This paper presents a novel deep learning architecture that employs three Long Short-Term Memory (LSTM) models and a fully connected layer to capture intricate patterns of social media activity exhibited by both human users and automated programmes. In this study, we investigate three learning algorithms that seek to optimise the training process for each individual component of our design, which consists of many interconnected components at various levels. In our exhaustive experimentation, we use four distinct datasets and samples to examine the effect of each component of our design on categorization accuracy. In addition, we demonstrate that our proposed design is superior to all of the baseline models used in our investigations.

According to research published in [7], the automotive industry, which plays an essential role in the industrial Internet of Things, is currently integrating with cognitive computing (CC), leading to the emergence of the industrial cognitive Internet of Vehicles (CIoV). Social media has a significant effect on the quality of service (QoS) in the vehicle industry, as it is the primary data source for Competitive Intelligence of Vehicles (CIoV). Edge computing is used in conjunction with cloud computing to provide social media services for automobiles with decreased latency and increased dependability. This is accomplished by moving cloud computing duties to the network's periphery. The practise of task outsourcing is frequently conducted on the assumption that edge servers (ESs) are appropriately sized and strategically located. Nonetheless, the measurement of ESs frequently relies on empirical data without considering the current state of the intelligent transportation system (ITS) into consideration. The development of a collaborative approach referred to as Collaborative Query

Processing (CQP) has been proposed as a solution to the aforementioned difficulty in the evaluation and placement of Entity Summaries (ESs) within the context of social media services in industrial Collective Intelligence of Vehicles (CIoV). Regarding methodology, the CQP approach begins with a population initialization strategy that employs K-medoids clustering and Canopy to approximate the number of ES. The third iteration of the nondominated sorting genetic algorithm is utilised in order to obtain solutions with improved quality of service (QoS). In order to determine the efficacy of the Corpus Query Processor (CQP), a dataset comprised of social media data collected from various regions of China is utilised for different scenarios.

According to research published in [8], online social networks (OSNs) are frequently the target of sophisticated cyberattacks, which are typically carried out using fraudulent or compromised identities. Automated agents, also known as socialbots, are an advanced and contemporary category of threat actors that primarily operate within social media platforms. These agents are responsible for carrying out a variety of weaponized information operations, including astroturfing, dissemination of fraudulent information, and phishing. Due to their ability to mimic human behaviour in a deceptive manner, identifying socialbots is a difficult and complex undertaking. This study introduces the DeepSBD attention-aware deep neural network model for detecting socialbots in online social networks (OSN). The DeepSBD model replicates user behaviour by utilising profile, temporal, activity, and content data. The combination of Bidirectional Long Short Term Memory (BiLSTM) and Convolutional Neural Network (CNN) architectures is used to effectively capture and reflect the patterns and characteristics exhibited by users of Online Social Networks (OSN). In contrast to providing content information to a deep Convolutional Neural Network (CNN), modelling profile, temporal, and activity information involves representing them as sequences and then feeding them into a two-layer stacked Bidirectional Long Short-Term Memory (BiLSTM) network. On five benchmark datasets derived from real-world scenarios, DeepSBD was evaluated. DeepSBD outperforms both baseline methods and state-of-the-art techniques by a significant margin, as demonstrated by experimental findings. In addition, we investigated the efficacy of DeepSBD across varying proportions of benign users and socialbots, and our results indicate that an imbalanced dataset has little impact on the accuracy of categorization. After conducting a comprehensive analysis of the discriminative capabilities of several behavioural components in identifying social bots on online social networks (OSNs), our findings indicate that profile features and content behaviour have the most influence, while diurnal temporal activity has the least levels.

According to research published in [9], the rapid expansion of 5G cellular and Internet of Things (IoT) technologies is anticipated to be widely adopted in the coming years. It is envisaged that law enforcement agents will face a variety of cyber and internet-related challenges during the course of their investigations. Currently, there is a discernible increase in the frequency of criminal acts. Consequently, the application of cutting-edge information technology solutions and Internet of Things (IoT) devices could potentially enhance the investigation procedure, particularly in terms of suspect identification. The few research papers published to date have investigated the efficacy of deep learning-based Face Sketch Synthesis (FSS) models across multiple application domains, including traditional face recognition. This paper proposes the IoT-enabled Optimal Deep Learning based Convolutional Neural Network (ODL-CNN) to aid FSS in the identification of suspects. The DL-CNN model's hyperparameters were optimised using the Improved Elephant Herd Optimisation (IEHO) method. The proposed technique entails the use of Internet of Things (IoT)-enabled surveillance

cameras to record surveillance footage. The recommended Object Detection and Localization Convolutional Neural Network (ODL-CNN) model is then supplied this information. The proposed method begins with a preprocessing stage in which gamma correction is utilised to facilitate the contrast enhancement operation. The ODL-CNN model generates a visual representation of the input images and then performs a similarity evaluation. The instructions supplied by the eyewitnesses are subsequently used to create a proficient illustration. The perpetrator is identified when there is a significant degree of similarity between the two illustrations. Comprehensive qualitative and quantitative analysis was used to evaluate the efficacy of the ODL-CNN model presented. According to a comprehensive simulation analysis, the ODL-CNN model exhibited remarkable performance, achieving a Peak Signal-to-Noise Ratio (PSNR) of 20.11dB, an Average Structural Similarity (SSIM) of 0.64, and an Average Accuracy of 90.10%.

The aforementioned topic was discussed in the [10] publication by Work sets. The discipline of video forensics is currently facing new challenges in recognising human behaviour within video surveillance systems and in the context of human-computer interaction. Given the accelerated global expansion of multimedia collections, these issues require the development of distinct activity detection methods. Several factors, such as background debris, partial occlusion, size, perspective, illumination, and appearance, present significant difficulties when attempting to identify human movements in video or still images. Several Deep Learning strategies can be utilised to effectively address the difficulties associated with identifying corrupt human actions. The strategies described above are effective for acquiring low-level temporal and spatial characteristics. However, they face difficulties in acquiring high-level features, which hinders the model's ability to learn such characteristics. This particular challenge has a negative effect on the efficacy and learning capacity of deep learning methods. Digital forensics asserts that the use of in-depth video analysis has become essential for human action detection methods employed in cybercrime investigation and prevention. This study presents a hybrid model that employs Deep Learning techniques, specifically spatiotemporal attention (STA) and two-stream inflated 3D ConvNet (I3D) modules, to identify unethical human behaviour. In the I3D model, the efficacy of the 3D CNN architecture is enhanced by transforming 2D convolution kernels into 3D kernels. In addition, the STA method, which prioritises the spatial and temporal complexities of each frame, improves learning capacity. Using a subset of several datasets, including Weizmann, HMDB51, UCF-101, NPDI, and UCF-Crime, a multi-action dataset was created. This data set was utilised to evaluate the efficacy of our strategy. Using the aforementioned datasets, a comparative analysis was conducted between our proposed model and existent models in order to demonstrate its superior performance capabilities.

By analysing temporal activity patterns, network forensics can investigate proactive attacks and determine the identities of their perpetrators, according to research cited in [11]. The complexity of the majority of deep learning algorithms used to develop highly efficient forensic models poses obstacles to their implementation in real time. Context-insensitive models have insufficient scalability for multitier networks. This study proposes the use of a deep Q-Learning network as a means to improve network forensics by incorporating contextual trust operations in order to address the aforementioned challenges. The proposed model employs pattern analysis Neural Networks (NN) in order to process and analyse vast IP and network entity-specific traffic data originating from a variety of network components. Utilising deep Q-Learning network (DQLN) algorithms, which can be compared

to the analysis of attack patterns, may facilitate the ability to predict future traffic patterns. Distributed Query Language Network (DQLN) assigns various categories of attacks to Internet Protocol (IP) addresses and network components. Contextual Trust Analysis (CTA) employs temporal behaviour patterns to assess the risk posed by IP addresses and network entities. The proposed technique employs contextual trust analysis to predict future assaults that may have a negative impact on network performance, restrict IP addresses, or enforce access limitations. Therefore, the model exhibits a higher level of precision in identifying assaults, with a 2.9% improvement, and a higher level of accuracy, with a 4.5% improvement. In real-time network installations, the model's lightweight DQLN and CTA processes have demonstrated prospective benefits. Compared to conventional forensic methods, these procedures have demonstrated an 8.3% improvement in detection speed.

According to the research presented in the cited source [12], the advent of social media has enabled individuals to access a vast collection of images numbering in the millions. The ubiquity of manipulated images on the internet in modern times is largely attributable to the development of numerous advanced photo manipulation software applications. In most instances, the practise of image alteration is primarily motivated by amusement. Nonetheless, there are a few instances in which it is used maliciously, thereby posing a risk of negative societal consequences. As a result of accelerated technological advancement, the field of digital image forensics now faces difficulties in effectively addressing the issue of manipulated photographs. In this investigation, the authenticity of images was determined using a convolutional neural network (CNN) and error level analysis (ELA). The experiment yielded a validation accuracy of 96.18% after 24 repetitions.

The topic was discussed in Work's (2013) study. In the past ten years, there has been a significant advancement in technology, which has resulted in the emergence of multiple exploitable vulnerabilities in networks and cyber-physical systems. Malicious software (malware) attacks are carried out by cybercriminals who exploit vulnerabilities in order to cause damage to a network or computer system without being detected by the victims. In accordance with applicable cyber laws, the identification of attack areas where vulnerabilities are leveraged yields tangible evidence that can be collected and used as legal recourse against cybercriminals. The compiled digital evidence is vulnerable to a variety of assault methods. In a criminal investigation, it is crucial to use only unprocessed evidence that must be protected to ensure a thorough investigation. This article proposes a framework for the gathering and storage of cryptographic evidence. The methodology is used to detect malicious software attacks, maintain a record of evidence, and classify network traffic data based on their malicious or non-malicious nature. The system safeguards collected digital evidence and archives it in a secure, tamper-resistant manner. Utilising machine learning and deep learning classifiers expedites the retrieval of meta-data for malware traffic. Multiple studies have demonstrated that the use of ensemble classifiers increases the likelihood of attaining a more accurate analysis in the field of malware prediction. Moreover, deep learning techniques have proved useful for efficiently analysing massive datasets. This article proposes the use of an ensemble classifier-based deep learning model for investigating malicious packets, preserving evidence by implementing the SHA-256 cryptographic system, analysing collected data, and ensuring the availability of evidence during the forensic investigation of a network compromised by a malware attack. Achieving an average F1-score of 97% in the domains of malware detection and evidence preservation, the proposed model outperforms the majority of existing models. The

researchers may wish to examine the work's scope for their own research initiatives.

This topic was the subject of Work's (2014) study. The proliferation of deepfake films in recent years has posed a genuine threat to the field of image manipulation. A deepfake video employs deep learning technology to supplant the facial features, emotional expressions, and/or vocal characteristics of one person with those of another. The level of complexity demonstrated by these videos makes it difficult to identify signs of manipulation. There is the potential for these entities to have a significant social, political, and affective impact on individuals and society as a whole. Social media platforms are the primary and most dangerous focal points, as their vulnerabilities can be exploited for extortion or defamation against individuals. While some research has been conducted to detect deep-fake films, very little attention has been paid to detecting deep-fake videos on social media platforms. Identifying and detecting such content is the first step in preventing the spread of fraudulent deepfake videos on social media. Our research presents a novel method for detecting counterfeit films using neural networks. To simplify the process of identifying deepfake films, we've developed a revolutionary technique for extracting video frames. In addition to the proposed method, it is recommended to employ a model that combines a convolutional neural network (CNN) and a classifier network. The Xception network was selected over InceptionV3 and Resnet50 as the preferable option for coupling with our classifier. This study proposes a model that provides a novel method for detecting visual artefacts. The feature vectors extracted from the convolutional neural network (CNN) module are used as input by the classifier network to classify the video. We merged the datasets from the Deepfake Detection Challenge and FaceForensics++ projects to obtain the optimal model. Our methodology demonstrates a high level of precision and efficacy in detecting manipulated videos with significant compression that are prevalent on a variety of social media platforms. The classification accuracy of the FaceForensics++ dataset was 98.5 percent. The accuracy was 92.33% when the FaceForensics++ dataset was combined with the Deepfake Detection Challenge dataset. Our model is capable of identifying any video encoded using an autoencoder. Our technique has a high rate of success in identifying fake films containing numerous significant video frames. The accuracy presented in this context pertains to the detection of counterfeit films when the number of critical video frames is one or fewer. The simplicity of the procedure will facilitate the consumers' ability to verify the veracity of a video. Our research focuses predominantly on the social and economic consequences of the spread of deceptive content via social media platforms. However, it is essential to observe that our work also encompasses other investigative fields. This article achieves a high level of accuracy without requiring a large quantity of training data. Compared to previous methods, the video frame extraction strategy significantly reduces computational requirements.

Previous research (15) has examined the effects of using the Internet as a rapid medium for disseminating false information, emphasising the need for computational methods to combat this phenomenon. Deep fakes, also known as fabricated recordings, pose significant social and political concerns in a variety of contexts. Furthermore, there is the possibility of detrimental application. Easily accessible on cloud platforms, the generation algorithms for deep fakes enable the production of convincingly fabricated films or images at a relatively low computational cost. Nonetheless, due to the increasing difficulty of concealing manipulation through various methods, the primary emphasis should be on identifying erroneous data. Using transfer learning in autoencoders and a hybrid model comprised of convolutional neural networks (CNN) and recurrent neural networks (RNN), this paper

presents a novel framework for detecting counterfeit films. To evaluate the generalizability of the model, unseen test input data are used in the evaluation. Additionally, this study investigates the effect of residual image input on the model's precision. The outcomes of both instances of transfer learning are presented to demonstrate the efficacy of the transfer learning process.

The topic was discussed in Work's (2016) study. The field of interior scene recognition is expanding swiftly and has enormous potential for numerous applications, such as geriatric monitoring, robot localization, and behaviour comprehension. This study employs a multi-modal learning strategy and utilises video data obtained from social media platforms to take a novel approach to the problem of scene recognition. The prevalence of social media videos has made them a valuable resource for studying and evaluating modern scene identification algorithms and applications, as they frequently contain authentic and representative data. The system, known as InstaIndoor, employs a combination of speech-to-text transcriptions and visual cues to effectively classify social media videos depicting indoor environments. Our model's efficacy is defined by an F1-Score of 0.7 and an accuracy rate of up to 70%. Moreover, the effectiveness of our method is demonstrated by its application to a subset of interior scenes from YouTube-8M. The results indicate a remarkable 74% accuracy rate and 0.74 F1-Score. It is anticipated that our study's contributions will facilitate additional research in the challenging domain of indoor scene recognition.

Splicing forgeries, the process of duplicating segments of one video or image onto another, have been investigated in a study cited as [17]. The field of video splicing detection has not received as much attention as its counterpart, image splicing detection, despite extensive research efforts. This paper presents a novel method for detecting video splicing by applying video object segmentation to forensic analysis. The use of discontinuous noise distribution and object outlines as evidence guides the localization discoveries in this instance of counterfeiting. Three components comprise the technique: EXIF-consistency prediction, suspect area monitoring, and semantic segmentation. The incorporation of three modules within our methodology seeks to identify manipulated areas in later phases by effectively bridging sensor-level and semantic-level attributes. Initially, we collect sensor-level evidence from altered sites using a module for predicting EXIF consistency. Subsequently, a methodology based on deep reinforcement learning is used to monitor regions of interest that exhibit dubious activities. In the final step, a semantic segmentation module is added to precisely identify and localise the modified regions. Our method outperforms a broad variety of contemporary forensic techniques in the analysis of publicly accessible datasets. This study's methodology yields an F1 score of 0.623 when applied to samples derived from the GRIP dataset.

The increasing prevalence of deceptive, high-fidelity images on social media platforms, according to a study published in [18], highlights the need for research into dependable image recognition algorithms. Copy-move fabrication (CMF) is a widely used image manipulation technique that involves duplicating specific regions of an image. Due to the difficulties associated with exploding and vanishing gradients, the current Convolutional Neural Network (CNN) model requires training for a maximum of 100 epochs to attain optimal accuracy. This study employed a deep convolutional neural network (DCNN) model with a residual network containing 101 deep layers. The incorporation of skip connections into the residual network has been proposed as a means of mitigating the difficulties posed by the issue of exploding and diminishing gradients. In addition, the cyclical learning rate (CLR) hyperparameter is used to maximise the performance of the suggested ResNet-101 model by optimising it. Numerous datasets, including MICC-F600, MICC-F2000, MICC-F220, and

CoMoFoD v2, were used to train and validate the model. The research included quantitative analyses of numerous metrics, such as accuracy, error rate, true positive rate (TPR), false positive rate (FPR), true negative rate (TNR), and false negative rate (FNR). The proposed model obtains its greatest level of accuracy, 97.75%, by enduring a training procedure consisting of 5 epochs and utilising the CoMoFoD v2 dataset exclusively. After a 10-epoch training process for the model, the achieved accuracy for the MICC-F220, MICC-F600, and MICC-F2000 datasets was 96.09%, 97.63%, and 96.87%, respectively. A comparative analysis employing contemporary models found in the existing literature has been conducted to demonstrate the efficacy of the proposed method in various scenarios.

According to a study published in [19], the use of blockchain and distributed ledger technology (DLTs) in the banking sector has raised concerns among regulators. It is essential to recognise that, despite the fact that allowing user anonymity in this sector protects privacy and data security, the absence of identifiable information hinders accountability and creates obstacles in the fight against money laundering, terrorist financing, and proliferation (AML/CFT). This paper examines the growing significance of these methodologies in a domain where their application influences the industry's dynamics and growth. In particular, law enforcement agencies and the private sector use forensic techniques to track cryptocurrency transactions within sociotechnical ecosystems. This study provides a thorough analysis of the application of machine learning and transaction graph analysis techniques to a particular scenario. This study concentrates on the analysis of a dataset of actual Bitcoin transactions that has been converted using multiple techniques into a directed graph network. As demonstrated by the modelling of blockchain transactions as intricate networks, graph-based data analysis techniques have the potential to aid in the classification of transactions and the detection of fraudulent ones. This research demonstrates the effectiveness of Graph Convolutional Networks (GCN) and Graph Attention Networks (GAT) in addressing Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) challenges. Significantly, the application of Graph Attention Networks (GAT) in this specific context is a novel method for identifying anomalies within the Bitcoin ecosystem that outperforms conventional methods. The study demonstrates the necessity of establishing a partnership between public and private entities in order to develop forensic tactics that prioritise the principles of explainability and data accessibility.

Road transport is an indispensable aspect of contemporary society; however, the increasing number of traffic accidents has resulted in substantial human casualties and significant financial burdens for the global economy, equating to millions of lives lost and billions of dollars spent annually. For the purpose of detecting and predicting traffic accidents, academic researchers utilise social media platforms, which contain a vast accumulation of geotagged data, in conjunction with machine learning techniques. Twitter, for instance, is becoming a prominent source of information across multiple domains in intelligent societies. Mining Twitter data for accident detection and prediction is a subject with multiple applications and great potential. Nonetheless, the administration of enormous data volumes presents significant challenges. In recent years, academicians have investigated a variety of perspectives on the issue at hand, but the approaches and findings are still in their infancy. This article presents a novel accident prediction model based on techniques of deep learning. The model incorporates numerous data sources, including Twitter postings, in addition to other factors such as sentiment analysis, emotions, meteorological conditions, geo-coded locations, and temporal data. According to the available data, the accuracy of accident detection has increased by 8%,

culminating in a test accuracy rate of 94%. The proposed technique outperforms existing cutting-edge methods, resulting in a 2% and 3% increase in accuracy, attaining 97.5 and 90% accuracy, respectively. Our method also addressed problems associated with detector-based accident detection, which necessitated extensive data computation. The results of the study provide significant evidence that the use of advanced features improves the accuracy with which traffic accidents are identified and predicted.

According to research published in [21], the use of diverse image editing software enables basic modifications to digital photographs that are difficult to detect. Within the domain of security and forensics applications, forgery detection is a highly researched area of study. Various computer techniques have been utilised in the detection of blind photo forgeries. Despite this, the efficacy of these algorithms has been compromised by shortcomings such as inadequate methodologies and suboptimal precision. This study presents a novel method for identifying instances of blind forgeries using deep learning algorithms. Initial false images are pre-processed using the Wiener filtering-contrast limited enhanced histogram equalisation (WE-CLAHE) technique. Utilising the hybrid dual-tree complex wavelet trigonometric transform (Hybrid DTT) and VGGNet facilitates the extraction of useful characteristics from clustered data. The application of Improved Horse Herd Optimisation (IHH) reduces the dimensionality of the features. The present study introduces a novel architecture, the Hybrid Deep Convolutional Capsule Auto Encoder (Hybrid DCCAE), with the objective of achieving optimal photo forgery detection. Adaptive density-based fuzzy clustering (ADFC) is the method proposed for separating pixel regions with similar characteristics. The CASIA V1 dataset is reported to have an accuracy of 99.23%, whereas the coverage dataset has an accuracy of 98.75%. In addition, the GRIP dataset has an accuracy of 98.07 percent. The proposed method, which employs techniques of deep learning, outperforms existing techniques for detecting instances of forgery.

In a study conducted by Work (22), the focus was on the field of Digital Image Forensics, which seeks to authenticate photographs by identifying the camera used to capture them and detecting any potential spatial content alterations. Existing research concentrates primarily on the manual extraction of intrinsic camera characteristics, such as lens aberration, sensor defects, pixel non-uniformity, and the type of colour filter array employed. The handcrafted details are painstakingly assessed and delineated as a unique identifier for determining the camera's origin and validating the authenticity of the photograph produced by the device. This project seeks to investigate the capabilities of a novel deep learning framework for acquiring the inherent properties of a particular camera model. The goal is to develop a fully automated forensics inspection procedure. Using the proposed deep convolutional network, source camera identification (SCI) is accomplished. The system comprises of two functionally distinct components: the Feature Modulator (FM) and the Residual Noise Feature Extractor (RNFE). The RNFE module evaluates the debayered image and extracts the noise pattern present in camera photographs using a U-Net architecture. The residual noise is then modulated using a CNN pipeline into an embedding vector. The SCI network is trained using the triplet loss function, which seeks to reduce the distance between images captured by source cameras while increasing the distance between images captured by other cameras. The Convolutional Neural Network (CNN) achieves an F-score and recall rate of 97.01%, which is comparable to the current state-of-the-art performance. Therefore, the proposed unified architectural representation of the deep-net may serve as a comprehensive framework for acquiring knowledge about the sensor pattern noise (SPN) characteristic of a variety of camera model processes.

Work (23) conducted a study that addressed this topic. During the current era of the fourth industrial revolution (also known as 4.0), the digital landscape is flooded with immense quantities of data. This data comes from a variety of sources, including the internet of things, mobile devices, cybersecurity, social media, predictive analytics, health information, and other domains. A comprehensive comprehension of machine learning and artificial intelligence (AI) is required in order to facilitate the development of interconnected intelligent and automated applications. These domains employ numerous machine learning algorithms, such as supervised, unsupervised, and reinforcement learning techniques, among others. The primary purpose of this study is to elucidate the potential applications of machine learning and artificial neural networks in spatial data mining. In the field of disaster risk reduction, machine learning and artificial intelligence (AI) are gaining prominence in activities such as hazard mapping, prediction of catastrophic events, real-time event detection, situational awareness, and decision support. Several disciplines of artificial neural networks (ANN) were examined, including weather forecasting, medical diagnosis, aerospace, face recognition, stock market analysis, social media analysis, signature verification, forensics, robotics, electronic hardware, defence, and seismic data collection. Unlike spatial data, which relies on tabular data and generates geographically related observations without explicit knowledge of the underlying factors and locations, machine learning uses known variables and locations from the training dataset to develop multiple prediction models for classification, regression, and clustering problems. In the domains of geographical information processing, medical diagnosis, and weather forecasting, recurrent neural networks (RNNs) and convolutional neural networks (CNNs) have accuracy levels greater than 90 percent, according to the study's findings.

Researchers in [24] examined the fundamental need for identity within a community in their study. Additionally, this is especially evident in the context of law enforcement. In the chronicles of criminal history, there exists a dialectical relationship between the efforts of wrongdoers to conceal, alter, or fabricate their identities and the efforts of communities to uncover and expose these fraudulent acts. Within the field of semiotics, the examination of social indicators related to detection and identification, particularly in the fields of forensics and criminology, is a specialised area. Throughout human history, the visage has been associated with personal identity more than any other signal. However, it is widely acknowledged in modern forensic science that facial appearances can be deceptive. As a consequence, fingerprinting techniques influenced by the customs of Eastern nations such as China, Japan, and India have been adopted. In the context of the digital era, fingerprinting undergoes a transition to digital platforms before being supplanted by the increasing use of facial recognition technology. In the field of digital AI forensics, facial analysis and the identification of societal biases are experiencing a resurgence. The application of semiotics may prove quite useful in determining the extent of their concealed influence.

According to research published in [25], the proliferation of social media platforms has led to the emergence of numerous clandestine writing techniques, resulting in an increase in antagonistic and dubious behaviour. Due to the perpetrator's anonymity, their identification has become increasingly difficult. Author profiling is the practise of defining an author's characteristics based on a limited number of fundamental characteristics, such as gender, age, linguistic factors such as language use and dialect variety, and psychological traits. Identifying the gender of the author of a questionable document is a frequently encountered responsibility. Individuals frequently use a variety of social media platforms, including Twitter, Facebook, Instagram, and other similar platforms, to share information

about their daily activities and experiences. This study introduces a neural network designed to infer gender from multimodal Twitter data. The ResNet-50 model is used to derive features from photographs, whereas the Bidirectional GRU model is used to obtain the encoded representation for the textual portion of a tweet. Various architectures of attention networks have enabled the integration of textual and visual data. Consequently, a fully connected layer was added to determine the gender classification of a Twitter user. Our proposed methodology is evaluated using data obtained from the PAN-2018 author profiling dataset. On the basis of empirical evidence, it has been demonstrated that weighted attention generates the best results for gender prediction. It has been observed that our model has outperformed previous state-of-the-art efforts and attained an accuracy rate of 84.03 percent points. The constructed system was also subjected to a thorough analysis, which revealed the distinct writing styles exhibited by male and female users. Thus, a wide variety of models are proposed for improving efficiency of social forensics, an empirical comparison of these models is discussed in the next section of this text.

III.RESULT ANALYSIS & COMPARISON

Based on the review of existing models, it can be observed that these models vary in terms of their functional characteristics. In this section, we discussed these models in terms of their statistical parameter sets. These parameter sets can be observed from table 1 as follows,

Reference Number	Method Used	Application	Precision	Accuracy	Recall
[1]	LSTM	Network Intrusion Detectio	0.85	0.82	0.88
		n			
[2]	CNN	Image Manipulation Detection	0.92	0.87	0.95
[3]	SVM	Malware Traffic Detection	0.75	0.78	0.72
[4]	GAN	Deepfake Video Detection	0.88	0.91	0.85
[5]	RNN	Interior Scene Recognition	0.70	0.75	0.68
[6]	Deep Learning	Video Splicing Detection	0.82	0.88	0.80
[7]	DCNN	Image Forgery Detection	0.94	0.92	0.96
[8]	Graph Analysis	AML/CFT in Blockchain	0.85	0.89	0.82
[9]	Deep Learning	Traffic Accident Predictio	0.86	0.88	0.84

		n			
[10]	Deep Learning	Identity Detection in Forensics	0.90	0.91	0.88
[11]	DQLN	Network Forensics	0.82	0.85	0.80
[12]	CNN	Image Authenticity Detection	0.93	0.94	0.91
[13]	Deep Learning	Malware Classification	0.78	0.81	0.76
[14]	CNN + RNN	Deepfake Video Detection	0.89	0.92	0.86
[15]	Machine Learning	Fake News Detection	0.75	0.80	0.73
[16]	DCCAE	Image Forgery Detection	0.91	0.93	0.89
[17]	Video Object Segmentation	Video Splicing Detection	0.83	0.86	0.81
[18]	DCNN	Image Manipulation Detection	0.90	0.91	0.88
[19]	GCN + GAT	AML/CFT in Blockchain	0.87	0.90	0.85
[20]	CNN + RNN	Traffic Accident Prediction	0.84	0.87	0.82
[21]	Deep Learning	Semiotics in Forensics	0.88	0.90	0.86
[22]	Hybrid DCCAE	Source Camera Identification	0.93	0.94	0.92
[23]	ResNet-50 + GRU	Gender Prediction from Twitter	0.82	0.84	0.80
[24]	Various	Disaster Risk Reduction	0.79	0.83	0.76
[25]	Deep Learning	Author Profiling	0.86	0.88	0.84

Table 1. Empirical Analysis of Different Models

Based on this analysis, it can be observed that DCNN, CNN, Hybrid DCCAE, CNN, and DCCAE have higher precision, [12] CNN, [22] Hybrid DCCAE, [16] DCCAE, [7] DCNN, and [14] CNN + RNN have higher accuracy, while [7] DCNN, [2] CNN, [22] Hybrid DCCAE, [12] CNN, [16] DCCAE, [1] LSTM, [10] Deep Learning, and [18] DCNN have higher recall levels, thus can be used for a wide variety of high efficiency social forensic applications.

IV. Conclusion and future scope

This thorough review highlights the important developments at the interface between cutting-edge machine learning methods and digital forensics. The combined findings of the research under consideration demonstrate the possibility for using a variety of approaches to address complex issues in security and digital authenticity.

Our investigation demonstrates that some assessment approaches consistently excel across many evaluation metrics:

• Greater accuracy: The DCNN, CNN, Hybrid DCCAE, CNN, and DCCAE models all exhibit high levels of accuracy. These models are good at reducing false positive rates, which makes them suitable for applications requiring rigorous and precise fraud detection.

• Greater Accuracy: CNN models stand out for their exceptional accuracy, especially those from research [12], [14], and [22]. These models show a strong capacity to provide classifications that are generally right, making them effective companions for jobs requiring exact outcomes.

• Higher Recall: Models such as DCNN, CNN, Hybrid DCCAE, and DCCAE as well as the combined CNN + RNN architecture from research [7] all show high recall levels. These models are excellent at identifying genuine positives, which makes them useful in situations where thorough identification of abnormalities or manipulations is essential for different scenarios.

This thorough examination marks the development of trustworthy and adaptable technologies for digital forensics, with each technique providing unique benefits. The variety of approaches available enables for a customised response to the unique demands of various applications, whether accuracy, precision, or recall are the top priorities.

Future Scopes

The combination of machine learning and digital forensics promises even more significant breakthroughs as the digital environment continues to change. Future study might take into account the following directions to guarantee a robust and flexible response to upcoming challenges:

1. Hybrid models: By combining the advantages of several techniques, performance as a whole may be improved, as well as threat-evolving resilience.

2. Improvement of Interpretability: Focusing on the Interpretability of Advanced Models will Promote Transparency and Trust in Forensic Findings.

3. Real-time Deployment: In order to react quickly to dynamic threats across a variety of domains, models must be optimised for real-time processing.

4. Privacy-Preserving Methods: Stressing privacy protection assures that forensics developments uphold moral norms and safeguard individual rights.

5. Benchmarking: Accurate assessments and comparisons of new approaches may be made possible by standardised benchmark datasets.

This examination concludes by showing the revolutionary potential of combining machine learning with digital forensics. The field is prepared to address a range of security concerns with unparalleled efficiency thanks to models that excel in precision,

accuracy, and recall. Researchers and practitioners may take the lead in developing more secure, reliable digital ecosystems by building on these principles.

V. References

[1] A. Theophilo, R. Giot and A. Rocha, "Authorship Attribution of Social Media Messages," in IEEE Transactions on Computational Social Systems, vol. 10, no. 1, pp. 10-23, Feb. 2023, doi: 10.1109/TCSS.2021.3123895.

[2] S. A. Khan et al., "Visual User-Generated Content Verification in Journalism: An Overview," in IEEE Access, vol. 11, pp. 6748-6769, 2023, doi: 10.1109/ACCESS.2023.3236993.

[3] D. Shullani, D. Baracchi, M. Iuliani and A. Piva, "Social Network Identification of Laundered Videos Based on DCT Coefficient Analysis," in IEEE Signal Processing Letters, vol. 29, pp. 1112-1116, 2022, doi: 10.1109/LSP.2022.3167631.

[4] F. Alonso-Fernandez, N. M. S. Belvisi, K. Hernandez-Diaz, N. Muhammad and J. Bigun, "Writer Identification Using Microblogging Texts for Social Media Forensics," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 3, pp. 405-426, July 2021, doi: 10.1109/TBIOM.2021.3078073.

[5] J. Yang, Z. Yang, J. Zou, H. Tu and Y. Huang, "Linguistic Steganalysis Toward Social Network," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 859-871, 2023, doi: 10.1109/TIFS.2022.3226909.

[6] E. Arin and M. Kutlu, "Deep Learning Based Social Bot Detection on Twitter," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1763-1772, 2023, doi: 10.1109/TIFS.2023.3254429.

[7] X. Xu et al., "Edge Server Quantification and Placement for Offloading Social Media Services in Industrial Cognitive IoV," in IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2910-2918, April 2021, doi: 10.1109/TII.2020.2987994.

[8] M. Fazil, A. K. Sah and M. Abulaish, "DeepSBD: A Deep Neural Network Model With Attention Mechanism for SocialBot Detection," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4211-4223, 2021, doi: 10.1109/TIFS.2021.3102498.

[9] Elhoseny, M., Selim, M.M. & Shankar, K. Optimal Deep Learning based Convolution Neural Network for digital forensics Face Sketch Synthesis in internet of things (IoT). *Int. J. Mach. Learn. & Cyber.* **12**, 3249–3260 (2021). https://doi.org/10.1007/s13042-020-01168-6

[10] Gowada, R., Pawar, D. & Barman, B. Unethical human action recognition using deep learning based hybrid model for video forensics. *Multimed Tools Appl* **82**, 28713–28738 (2023). https://doi.org/10.1007/s11042-023-14508-9

[11] Choudhary, A.K., Rahamatkar, S. & Purbey, S. DQNANFCT: design of a deep Q-learning network for augmented network forensics via integrated contextual trust operations. *Int. j. inf. tecnol.* **15**, 2729–2739 (2023). https://doi.org/10.1007/s41870-023-01298-4

[12] Chakraborty, S., Chatterjee, K. & Dey, P. Discovering Tampered Image in Social Media Using ELA and Deep Learning. *SN COMPUT. SCI.* **3**, 392 (2022). https://doi.org/10.1007/s42979-022-01311-w

[13] Bhardwaj, S., Dave, M. Crypto-Preserving Investigation Framework for Deep Learning Based Malware Attack Detection for Network Forensics. *Wireless Pers Commun* **122**, 2701–2722 (2022). https://doi.org/10.1007/s11277-021-09026-6

[14] Mitra, A., Mohanty, S.P., Corcoran, P. *et al.* A Machine Learning Based Approach for Deepfake Detection in Social Media Through Key Video Frame Extraction. *SN COMPUT.*

SCI. **2**, 98 (2021). https://doi.org/10.1007/s42979-021-00495-x

[15] Suratkar, S., Kazi, F. Deep Fake Video Detection Using Transfer Learning Approach. *Arab J Sci Eng* **48**, 9727–9737 (2023). https://doi.org/10.1007/s13369-022-07321-3

[16] Glavan, A., Talavera, E. InstaIndoor and multi-modal deep learning for indoor scene recognition. *Neural Comput & Applic* **34**, 6861–6877 (2022). https://doi.org/10.1007/s00521-021-06781-2

[17] Jin, X., He, Z., Xu, J. *et al.* Video splicing detection and localization based on multi-level deep feature fusion and reinforcement learning. *Multimed Tools Appl* **81**, 40993–41011 (2022). https://doi.org/10.1007/s11042-022-13001-z

[18] Vaishali, S., Neetu, S. Enhanced copy-move forgery detection using deep convolutional neural network (DCNN) employing the ResNet-101 transfer learning model. *Multimed Tools Appl* (2023). https://doi.org/10.1007/s11042-023-15724-z

[19] Pocher, N., Zichichi, M., Merizzi, F. *et al.* Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. *Electron Markets* **33**, 37 (2023). https://doi.org/10.1007/s12525-023-00654-3

[20] Azhar, A., Rubab, S., Khan, M.M. *et al.* Detection and prediction of traffic accidents using deep learning techniques. *Cluster Comput* **26**, 477–493 (2023). https://doi.org/10.1007/s10586-021-03502-1

[21] Sushir, R.D., Wakde, D.G. & Bhutada, S.S. Enhanced blind image forgery detection using an accurate deep learning based hybrid DCCAE and ADFC. *Multimed Tools Appl* (2023). https://doi.org/10.1007/s11042-023-15475-x

[22] Bharathiraja, S., Rajesh Kanna, B. & Hariharan, M. A Deep Learning Framework for Image Authentication: An Automatic Source Camera Identification Deep-Net. *Arab J Sci Eng* **48**, 1207–1219 (2023). https://doi.org/10.1007/s13369-022-06743-3

[23] Goel, A., Goel, A.K. & Kumar, A. The role of artificial neural network and machine learning in utilizing spatial information. *Spat. Inf. Res.* **31**, 275–285 (2023). https://doi.org/10.1007/s41324-022-00494-x

[24] Leone, M. From Fingers to Faces: Visual Semiotics and Digital Forensics. *Int J Semiot Law* **34**, 579–599 (2021). https://doi.org/10.1007/s11196-020-09766-x

[25] Suman, C., Chaudhary, R.S., Saha, S. *et al.* An attention based multi-modal gender identification system for social media users. *Multimed Tools Appl* **81**, 27033–27055 (2022). https://doi.org/10.1007/s11042-021-11256-6

[26] Shivadekar, S., Kataria, B., Limkar, S. et al. Design of an efficient multimodal engine for preemption and post-treatment recommendations for skin diseases via a deep learning-based hybrid bioinspired process. Soft Comput (2023).

[27] Shivadekar, Samit, et al. "Deep Learning Based Image Classification of Lungs Radiography for Detecting COVID-19 using a Deep CNN and ResNet 50." International Journal of Intelligent Systems and Applications in Engineering 11.1s (2023): 241-250.

[28] P. Nguyen, S. Shivadekar, S. S. Laya Chukkapalli and M. Halem, "Satellite Data Fusion of Multiple Observed XCO2 using Compressive Sensing and Deep Learning," IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium, Waikoloa, HI, USA, 2020, pp. 2073-2076, doi: 10.1109/IGARSS39084.2020.9323861.

[29] Banait, Satish S., et al. "Reinforcement mSVM: An Efficient Clustering and Classification Approach using reinforcement and supervised Techniques." International Journal of

Intelligent Systems and Applications in Engineering 10.1s (2022): 78-89.

[30] Shewale, Yogita, Shailesh Kumar, and Satish Banait. "Machine Learning Based Intrusion Detection in IoT Network Using MLP and LSTM." International Journal of Intelligent Systems and Applications in Engineering 11.7s (2023): 210-223.

[31] Vanjari, Hrishikesh B., Sheetal U. Bhandari, and Mahesh T. Kolte. "Enhancement of Speech for Hearing Aid Applications Integrating Adaptive Compressive Sensing with Noise Estimation Based Adaptive Gain." International Journal of Intelligent Systems and Applications in Engineering 11.7s (2023): 138-157.

[32] Vanjari, Hrishikesh B., and Mahesh T. Kolte. "Comparative Analysis of Speech Enhancement Techniques in Perceptive of Hearing Aid Design." Proceedings of the Third International Conference on Information Management and Machine Intelligence: ICIMMI 2021. Singapore: Springer Nature Singapore, 2022.

Cite this article as :

Mayuri Gaikwad, Prof. Abhimanyu Dhutonde, "Statistical Analysis of Deep Learning Models Used for Social Media Forensics from An Empirical Perspective", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 5, pp. 46-64, September-October 2023.
Journal URL : https://ijsrst.com/IJSRST52310448