A Literature Review: Advanced Deepfake Detection using ResNeXt and LSTM for a Trusted Digital World

[1]Pranav M, [2]Dr Amith Shekar, [3]Karthik R, [4]Dandamraju Sri Harshith
[1]Student, [2]Associate Professor, [3]Student, [4]Student
[1]Computer Science and Engineering,
[1]BNM Institute of Technology, Bengaluru, India

Abstract- Deepfakes have increasingly generated very realistic manipulated visuals and audio through weaponized GANs and advanced deep learning techniques, albeit rather misused in committing identity theft, misinformation campaigns, and digital fraud. This paper introduces a novel deepfake detection framework based on advanced machine learning techniques to accurately detect tampered content. Such systems make use of CNN for the detection of faint inconsistencies at the frame level, while RNNs are used to study sequential patterns for anomalies in sequences. The proposed ensemble technique here adds credence to the system by taking the output from a set of models for improved detection. Scaling and flexible, the approach presented here adapts to the fast-evolving landscape of deepfake manipulation and combines visual and temporal features. This work therefore fights towards the protection of integrity for digital media and allows less room for misuse of synthetic content.

Keywords: Detection, ResNeXt, Deepfake, LSTM, Video and Image Manipulation

INTRODUCTION

The human face is among the most prominent traits of an individual, since facial features are quintessential in bodily interaction and have a major part in biometric security. Nevertheless, the latest developments in face synthesis technology have opened the doors to some serious security threats by providing tools that can create particularly realistic but altered content known as deepfakes. These are generated using deep learning techniques to superimpose one person's face onto another's without consent, leading to the creation of synthetic images, videos, and audio that are difficult to distinguish from authentic media.

Generative adversarial networks and other such deep learning models have mainly fueled the development of deepfake technology revolutionized content creation but also raised critical concerns. It has been used to spread falsehood, fake news, and fraudulent extorting money from people.

Deepfakes were being increasingly misused, so identification and counteraction of them were a global priority for governments, technology corporations, and private individuals.
The menace has been countered with deep fake d etection systems devised by computer vision, machine researchers. Learning, and forensic analysis.
Methods of such kinds include CNN and RNNs that perform analyses frame-level anomalies and temporal inconsistencies in tampered video. For instance, use a benchmark dataset from FaceForensics++ to train models such as Xception and MobileNet to identify the following deepfakes, created by different services: Deepfakes, Face2Face, and FaceSwap. Further, voting mechanisms that aggregate the results from multiple models have been proposed to increase accuracy and Stability.

Even with better methods of detection, problems persist. Through continuous evolution of deepfake algorithms, traditional methods become ever more less effective with time. Models must identify subtle visual and audio cues, often undetectable by humans. Therefore, new techniques such as frame-level feature extraction and time-sensitive analysis are currently being Formulated to overcome these barriers. For example, experimental configurations consisting of both CNNs and RNNs could reach up to 94% accuracy in identifying modified material.

The spread of propaganda, explicit content, and fake news has been fueled by the misuse of deepfake technology.
Apprehensions regarding its influence on society. Social media sites, such as Facebook and Instagram, have also implemented policies that

would regulate the spread of this content. Though content, effectiveness is highly dependent on the precision of a detection algorithm. Accordingly, pinpointing deepfakes with much accuracy is crucial for maintaining trust in virtual communication and balancing bad deeds.

This review explores state-of-the-art deepfake detection techniques, evaluating their effectiveness and Factors. It stresses the need for robust and dynamic solutions to meet the fast strides of deepfake technology and Maintain its authenticity of digital media. When paired with cutting-edge AI detection systems, this combination can provide a multi-layered defense against deepfakes, ensuring that fabricated content is identified swiftly and that genuine media remains protected. Such advancements could revolutionize the way digital content is managed, fostering greater trust in online interactions while mitigating the risks associated with deepfake misuse.

IMPORTANT KEY CONCEPTS

Deepfakes are synthetically created media using AI algorithms especially Generative Adversarial Networks (GANs), in mimicking the visual, auditory, or behavioral characteristics of real Spectators. They imply alteration or production of pictures, videos, or audio to create the impression that someone said or did an action they never actually performed. This means deepfakes can have creative applications in entertainment and education, but raises important ethical and security concerns. And among them are spreading misinformation, defamation, and assisting with frauds or identity theft. It has been increasingly challenging to distinguish reality from illusion as the technology advances in deepfakes content that underlines the importance of creating reliable detection tools and lobbying for increased digital literacy to mitigate this potential misuse.

ResNeXt is actually a deep learning architecture that progresses from the ResNet framework by Fig1. Introduces the concept of cardinality to enhance model performance and efficiency. Instead of merely increasing the depth or width of the network, ResNeXt focuses on splitting computations into multiple parallel paths or "cardinal groups" within each block. This grouped convolution design allows for more flexible and scalable feature learning without significantly increasing computational costs. By combining residual connections with grouped convolutions, ResNeXt achieves state-of-the-art performance across various tasks, including image classification and object detection, while maintaining a balance between accuracy and computational efficiency. Its modular design makes it versatile and easy to adapt to different machine learning problems.

Long Short-Term Memory (LSTM) is a type of recurrent neural network (RNN) designed to effectively capture and process sequential data while addressing the vanishing gradient problem common in traditional RNNs. LSTMs achieve this through a unique structure comprising memory cells and three key gates: input, forget, and output gates shown in Fig2. These gates control the flow of information, allowing the network to retain relevant data over long sequences and discard unnecessary details. This capability makes LSTMs particularly suited for tasks like natural language processing, time-series forecasting, and speech recognition, where understanding context over time is critical. Their robustness and adaptability have made LSTMs a cornerstone in deep learning for sequence-based applications.

The addition of pictures and videos in deepfake technology has enhanced its impacts significantly but with both negative and positive outcomes. These deepfake algorithms alter visual content and produce very realistic synthetic media. They include combinations and modifications of images and videos with a purpose of misrepresenting stories. It can change any faces in videos or even produce a completely artificial scene, which then is presented to be real. These advancements have transformational potential in entertainment, gaming, and education primarily by opening up novel forms of visual storytelling. But they simultaneously pose serious risks: the spreading of misinformation, violations of privacy, and the creation of fake evidence. Thus, ensuring the detection of manipulated images and videos becomes a matter of urgent need. Increasingly sophisticated deepfakes require equally sophisticated tools to counter them and detect such optical illusions. Researchers and technologists counter the increasing tendency of

deepfake videos by using various methodologies in the field aimed at detection, prevention, and mitigation.

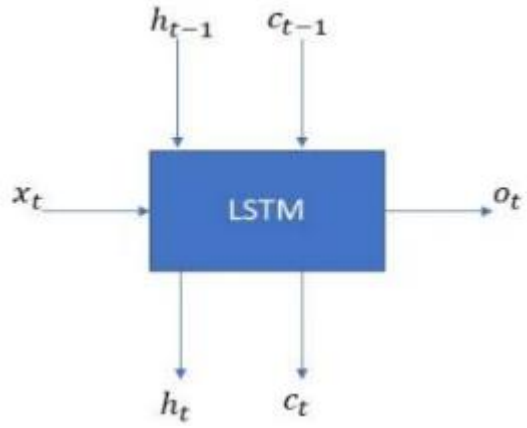

Fig 1. General Structure of ResNeXt

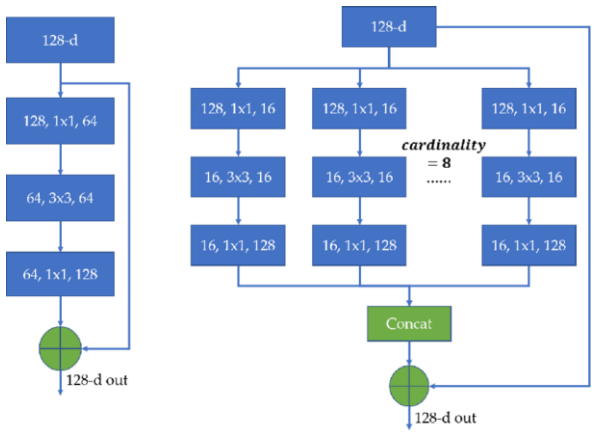

Fig 2. LSTM Architecture

The primary detection techniques rely on the deep architecture of CNN in order to identify small anomalies in the face, lighting, or pixel patterns that define deepfakes. Audio-visual synchronization-based approaches work by detecting inconsistency in what is spoken versus the movement of the lips.

Another recent approach is the blockchain-based authentication system for secured timestamping and cryptographic hashing in order to guarantee integrity in digital content. In addition to this, awareness campaigns and digital literacy programs are necessary for educating users to recognize manipulated media.

REVIEW OF LITERATURE

Authors Raghava M S, Tejashwini S P, Kavya Sree, Sneha A, Naveen R [1] has done a study which focuses on CRISP-DM, a structured methodology for data analytics that ensures projects follow a systematic workflow from business understanding to deployment. It starts from Business Understanding: business objectives define and align them with the data mining goals. Data understanding is about gathering and assessing the quality of data, while data preparation focuses on cleaning and transforming data for analysis. It involves making appropriate techniques and generating models, further optimizing these models' performance. In Evaluation, models are reviewed for efficiency and consistency with objectives, and the Deployment phase. It implements and oversees the structure for maintenance. Additionally, transfer learning is highlighted as a technique leveraging pre-trained models to accelerate new activities. This very effectively applies to applications such as computer vision and natural language processing, the reduction the demand for basic training and efficiency enhancement in analytical procedures.

Authors Preeti, Manoj Kumar, Hitesh Kumar Sharma [2] suggested the implementation of Deepfakes utilizes GAN-based techniques, particularly Deep Convolutional GAN (DCGAN), to generate realistic swapped images and videos. Using the celebA dataset, DCGAN learns from real images to produce synthetic ones, improving through training. Over 10 iterations, results showed decreasing generator loss and improving discriminator accuracy. Graphs highlight the discriminator's enhanced performance and convergence, achieving better accuracy by the 10th iteration. Evaluation metrics like Inception Score and Fréchet Inception Distance assessed image quality. A low FID score indicated realistic image distributions, while a high IS showed diversity in outputs. Tables compared model metrics, validating DCGAN's effectiveness. The discriminator’s ability to classify authenticity in batches further improved generated image quality.

Authors MA Shohel rana, Mohammad nur nobi, Beddhu Murali, Andrew H.sung,[3] suggested a systematic literature review (SLR) examines 112 studies on Deepfake detection methods from 2018 to 2020, presenting and analyzing state-of-the-art

techniques. Key findings include: Literature paper review Deep Learning Dominance: Deep learning methods, particularly convolutional neural networks (CNNs), are widely used and represent a large portion of the models applied in Deepfake detection. Dataset Prevalence: The FaceForensics++ (FF++) dataset is the most commonly used in these experiments. Key Metric: Detection accuracy is the primary performance metric across studies. Performance Insights: Experimental results consistently show that deep learning models outperform non-deep learning approaches in detecting Deepfakes effectively. The review notes that despite progress in multimedia technology and detection tools, challenges remain. This SLR aims to aid the research community in developing more robust detection methods and countermeasures against Deepfake technology.

Authors Prof. Aparna Bagde, Sakshi Fand, Kanchan Varma, Aditya Gawali [4] has done a study which focuses on the pre-processing module for deepfake detection converts video content into single image frames suitable for deep learning models. Using OpenCV, videos are split into individual frames for frame-by-frame analysis, avoiding inter-frame dependencies. OpenCV's Haarcascade frontal facial classifier detects faces in each frame, retaining only the largest detected face to ensure accuracy. Detected faces are saved as new images and resized to meet the input requirements of the deep learning model. This organized preparation ensures effective analysis for deepfake detection. By analyzing visual, auditory, and contextual cues, models trained on large datasets identify inconsistencies in digital media. This process improves detection accuracy and helps differentiate authentic content from deepfakes, ensuring reliable digital media analysis.

Authors Aryaf Al-Adwan, Hadeel Alazzam, Noor Al-Anbaki and Eman Alduweib [5] has done a study which focuses on the survey evaluates deep learning models for deepfake detection using datasets like Celeb-DF and Face Forensics++, which provide reliable benchmarks. Models utilizing temporal features achieved the highest accuracy, highlighting the importance of temporal data in detection. While most models showed high performance, models and stood out, with model achieving 99.95% accuracy. Conversely, model, which combined biological and temporal features, had the lowest performance, suggesting challenges in blending feature types. AUC scores were consistently high, with four out of five models scoring at least 99.5%. The survey underscores the effectiveness of CNNs and deep learning methods in detecting deepfakes, emphasizing their reliability for combating digital media manipulation.

Authors Jacob Mallet, Dr. Rushit Dave, Dr. Naeem Seliya, Dr. Mounika Vanamala [6] has done a study which focuses on Deepfake videos pose a serious threat by spreading disinformation and eroding trust in visual media. This study proposes a hybrid deepfake detection model combining CNN and RNN, optimized using Particle Swarm Optimization (PSO) for hyperparameter tuning. Tested on Celeb-DF and DFDC datasets, the model achieved 97.26% and 94.2% accuracy, respectively. The RNN captured temporal dependencies, improving detection, while PSO enhanced sensitivity, specificity, and F1 scores. Compared to models like CNN-XGBoost and CNN-only approaches, the hybrid model outperformed in most metrics, especially on DFDC. Future work includes incorporating attention mechanisms, expanding datasets to handle diverse conditions, and developing real-time detection for practical applications, making it a robust tool against deepfakes.

Authors Anuj Badale, Lionel Castelino, Chaitanya Darekar, and Joanne Gomes [7] proposed a deepfake detection system utilizing Dense and Convolutional Neural Networks (CNNs) to identify manipulated videos by analyzing pixel-level anomalies. They took that dataset of 900 deepfakes, went frame by frame and labeled each as real or fake in making the training set balanced. Some pre-processing steps in frame resizing to some standard resolution and pixel values normalization for similar to the CNN architecture. It employs 13 convolution layers to learn the feature and 5 pooling layers to reduce the dimensionality without loss of critical spatial information. Classifications were done with effective use of ReLU activation function and Adam optimizer on the dense layers.

Reaching 91% in accuracy, this model uses categorical cross-entropy loss. The system showed good performance, and some metrics from it-accuracy and reduction in loss-do justify its effectiveness efficiency. Further, tuning hyperparameters optimized learning rates, batch sizes, and model configurations that improved detection certainty. This indicates CNNs

sensitivity at detecting subtle deepfake manipulations to try to reduce growing concern regarding the inappropriate application of that technology. This opened the possibility of using analogous neural network-driven systems for resistance to the proliferation of media manipulation should be protected for the integrity of digital content in applied contexts.

The Authors Yogesh Rai, Aditya Shinde, Pranav Patil, and Prof. Preeti Komati [8] proposes a deepfake detection system utilizing Convolutional Neural Networks (CNNs) to identify common deepfake techniques such as face swapping and reenactment. It was trained on Deepfake Detection Challenge Data and separated the fake from the real media. Preprocessing included face detection and alignment to select frames for capturing different
Lighting angles and conditions resized, normalized to feed these frames into the CNN that used convolutional and pooling denser layers at the end which perform final binary classification, feature extraction, and dimensionality-reducing layers. Thus, through a sigmoid activation function challenges for the authors include identifying truly realistic deepfakes as advancements are made considering continual advances in manipulation technique. I have done some hyperparameter tuning to hyper-optimize the model for better accuracy. The system demonstrated strong performance in detecting subtle manipulations that might otherwise elude human Detection. The potential applications range from content moderation on social media to forensic analysis for law enforcement, and
Real-time detection tools for the media organisation The authors also discussed the ethical considerations of misuse and privacy, suggesting future improvements by incorporating multimodal data, such as audio and text analysis, to strengthen the system's detection capabilities

The authors Trupti Kularkar, Tanvi Jikar, Vansh Rewaskar, Krupali Dhawale, Achamma Thomas, and Mangala Madankar [9] present a sophisticated approach to deepfake detection by integrating ResNeXt Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) networks. Their research addresses manipulations in digital media by leveraging ResNeXt for spatial feature extraction and LSTM for temporal pattern recognition across video frames. The preprocessing pipeline includes video segmentation, face detection, cropping, and frame normalization to ensure the model operates with consistent and relevant data. By utilizing datasets like FaceForensics++, Celeb-DF, and DFDC, the system achieves a robust classification accuracy of 94.1%, distinguishing between real and manipulated content with high reliability.
The study acknowledges the rapid advancements in deepfake technology and highlights the importance of adaptive solutions. The authors propose future enhancements, such as multimodal analysis incorporating audio, metadata, and semantic context, to further strengthen detection capabilities. Potential applications include real-time monitoring for social media platforms, digital forensic tools, and public awareness campaigns to mitigate misinformation. The research emphasizes the ethical challenges posed by deepfakes and underscores the need for continuous innovation and global cooperation to safeguard the authenticity and integrity of digital media.

The authors B. Manish, C. Manish, and B. Sai Kiran Reddy[10] propose a robust approach to deepfake detection leveraging cutting-edge deep learning models. Their research emphasizes using Convolutional Neural Networks (CNN) combined with architectures like Xception and MobileNet to identify manipulated media. The preprocessing pipeline includes data collection from Kaggle datasets, followed by image normalization, enhancement, and feature extraction. The models are fine-tuned on tasks like detecting facial distortions, temporal inconsistencies in videos, and feature deviations in fake images. By leveraging advanced techniques and ensemble methods, their system achieved high accuracy, with Xception recording an impressive 99.3%.
The study acknowledges the rapid evolution of deepfake technologies and stresses the importance of public awareness and ethical practices. The authors highlight future directions, such as integrating audio and metadata analysis to improve detection accuracy and robustness. Potential applications include content moderation for social media, tools for combating misinformation, and forensic investigations. This work offers a comprehensive and proactive strategy to mitigate the misuse of deepfake technology and preserve the authenticity of digital media.

The authors Shanjita Akter Prome, Neethiahnanthan Ari Ragavan, Md Rafiqul Islam, David Asirvatham, and Anasuya Jegathevi Jegathesan[11] propose a systematic review of deception detection techniques, focusing on the application of machine learning (ML) and deep learning (DL). Their work highlights various approaches, including facial micro-expression analysis, speech pattern recognition, and

physiological data interpretation. Techniques like Support Vector Machines (SVM), Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs) are discussed for their ability to identify verbal and nonverbal cues of deception. The study also delves into the importance of multimodal detection methods that analyze visual, audio, and physiological signals to improve accuracy. They recommend future research to integrate more advanced DL techniques and explore multimodal systems for improved robustness. This work provides a foundation for developing innovative and interdisciplinary approaches to deception detection.

The authors Aya Ismail, Marwa Elpeltagy, Mervat S. Zaki, and Kamal Eldahshan[12] introduce a novel deepfake detection methodology combining the YOLO face detector, InceptionResNetV2 CNN, and XGBoost classifier. The system, referred to as YOLO-InceptionResNetV2-XGBoost (YIX), detects and analyzes facial regions from video frames to identify inconsistencies. The model uses the Celeb-DF and FaceForensics++ (c23) datasets for training and testing, achieving an AUC score of 90.62% and an accuracy of 90.73%, outperforming several state-of-the-art models. The research underscores the significance of addressing deepfake threats to ensure media authenticity and public trust. The authors highlight future directions, including the use of advanced face detection techniques and adaptations to evolving deepfake technologies.

This work presents a robust and scalable approach to mitigating the risks of deepfake manipulation, with applications in security, forensic investigations, and content moderation

Table 1: LITERATURE REVIEW SUMMARY

TITLE	YEAR	TECHNIQUE	DESCRIPTION	ADVANTAGE	LIMITATION
AI deep fake detection research paper	2023	Cross-Industry Standard Process for Data Mining	A machine learning technique that uses a pre-trained model for a new, related task, particularly useful in deep learning for fields like computer vision and natural language processing.	The methodology covers essential phases, from understanding the business context to implementing the models in a real-world setting, ensuring that the data analytics process iswell-executed and aligned with the business goals.	CRISP-DM's linear structure limits flexibility for iterative or exploratory workflows in modern data analytics.
A GAN-Based Model of Deepfake Detection in Social Media	2023	Generative Adversarial Network	The implementation of Deepfakes leverages various GAN-based techniques, with advancements in GANs making it possible to generate realistic swapped images, videos, and even synthetic, non-existent faces.	DCGAN effectively generates realistic and diverse synthetic images, with high accuracy and improved discriminator performance over iterations.	The increasing realism of generated images poses challenges in distinguishing between authentic and fake content, raising ethical concerns.

Deepfake Detection: A Systematic Literature Review	2022	Convolutional neural networks	This SLR reviews 112 studies on Deepfake detection methods from 2018 to 2020, highlighting the dominance of deep learning approaches like CNNs and the prevalent use of datasets such as FaceForensics++.	Deep learning models consistently achieve high detection accuracy, outperforming traditional methods.	Despite advancements, challenges like evolving Deepfake techniques and limited generalizability of detection models persist.
Deep fake Detection using Deep Learning	2023	OpenCV's Haarcascade frontal facial classifier	The pre-processing module for deepfake detection converts videos into individual frames using OpenCV, detects faces with Haarcascade, and prepares high-quality, resized images for deep learning analysis.	This method ensures efficient and accurate preparation of input data, enhancing the model's detection performance.	It relies on predefined classifiers, which may fail to detect faces under challenging conditions like low resolution or poor lighting.
Using Deep Learning to Detecting Deepfakes	2020	CNNs and related deep learning algorithms	This survey evaluates deep learning models for deepfake detection, emphasizing the superior accuracy of temporal feature-based models on datasets like Celeb-DF and FaceForensics++.	Temporal features enhance detection accuracy, achieving results as high as 99.95%.	Combining biological and temporal features poses challenges, reducing performance in some models
Detection of Deepfake Media Using a Hybrid CNN–RNN Model and Particle Swarm Optimization (PSO) Algorithm	2024	Hybrid CNN–RNN Model and Particle Swarm Optimization	This study proposes a hybrid deepfake detection model combining CNN, RNN, and Particle Swarm Optimization, achieving high accuracy on Celeb-DF and DFDC datasets.	The model captures temporal dependencies effectively and outperforms many state-of-the-art techniques.	Accuracy slightly lags behind CNN-only models on some datasets, and real-time implementation remains a challenge.

Deep Fake Detection using Neural Networks	2021	CNNs and related deep learning architectures	This study proposes a deepfake detection model using CNN to analyze facial features and identify pixel-level inconsistencies caused by deepfake generation techniques. The model was trained and tested on datasets containing both real and manipulated media, achieving significant accuracy in differentiating between authentic and fake content.	The model offers high accuracy in detecting pixel-level artifacts, scalability for large datasets, and adaptability to new deepfake techniques with retraining.	The model's performance depends on the quality and diversity of training data, requires significant computational resources for training and deployment, and may struggle with advanced or unseen deepfake techniques.
Deepfake Detection System	2024	Convolutional Neural Networks (CNN) with Support Vector Machines (SVM) to detect deepfake images and videos	This study develops a hybrid deepfake detection system that integrates CNN for feature extraction and SVM for classification, effectively distinguishing real content from manipulated media across various datasets.	The system provides high detection accuracy by combining the feature extraction power of CNN with the classification efficiency of SVM, ensuring robustness across different datasets and deepfake techniques.	The system’s performance is limited by the quality of the training data, requires substantial computational resources for model training, and may not generalize well to highly sophisticated deepfake methods
Deepfake Detection Using LSTM and ResNext	2023	Long Short-Term Memory (LSTM) networks with ResNext architecture to detect manipulations in videos and images.	This study develops a deepfake detection model that integrates LSTM for sequential learning of temporal patterns and ResNext for extracting spatial features,	The hybrid model leverages the temporal learning capabilities of LSTM and the powerful feature extraction of ResNext, improving detection	The model’s effectiveness depends on the quality of the training data, requires high computational resources for training and processing, and may struggle with highly

			effectively identifying deepfake content in both video and image datasets	accuracy and robustness across dynamic video and image manipulations.	advanced deepfake techniques that bypass conventional feature detection methods.
Deepfake Detection on face images & videos using deep learning	2024	CNN and Recurrent Neural Networks (RNN), to detect deepfakes in both face images and videos	This paper proposes a deepfake detection model combining CNN for feature extraction from face images and RNN for analyzing temporal patterns in videos, effectively identifying fake content in both static and dynamic media.	The model enhances detection accuracy by utilizing CNN for spatial feature extraction and RNN for temporal pattern recognition, making it effective for both face images and videos.	The model's performance is highly dependent on the quality of the dataset, demands considerable computational resources for training, and may face challenges in detecting very advanced or subtle deepfake manipulations.
Deception Detection Using Machine Learning (ML) and Deep Learning (DL) Techniques: A Systematic Review	2024	Machine Learning and Deep Learning Techniques	The authors propose future directions for research, including the integration of advanced DL techniques, exploration of multimodal deception detection systems, and addressing ethical considerations.	Comprehensive review of ML/DL techniques for deception detection. Emphasis on multimodal detection and interdisciplinary research.	Lack of practical implementation or specific experimental results.Focused more on review than proposing a novel methodology.
A New Deep Learning-Based Methodology for Video Deepfake Detection Using XGBoost	2021	XGBoost and InceptionResNetV2 convolutional neural network (CNN)	This paper presents a novel framework for detecting deepfake videos. Deepfakes, which involve AI-generated realistic fake videos, pose significant risks to privacy, security, and public trust.	High performance metrics compared to existing models. Combines robust CNN feature extraction with the efficiency of XGBoost classification.	Model performance relies heavily on specific datasets, which may limit applicability to unseen data.

CONCLUSION

The evolution of deepfake technology presents both transformative opportunities and significant challenges in digital media. This review highlights the urgency of developing reliable detection mechanisms to counteract the misuse of such technology. By leveraging advanced deep learning frameworks like ResNeXt and LSTM, researchers have achieved promising results in detecting subtle inconsistencies within manipulated content, demonstrating up to 99% accuracy in some studies. However, the rapid advancements in deepfake algorithms necessitate continuous innovation to keep detection techniques robust and adaptive. The hybridization of spatial and temporal analysis, combined with ensemble methods, proves effective in addressing these challenges, offering a scalable and precise solution to safeguard digital authenticity. Future work should focus on incorporating multimodal data analysis and real-time detection capabilities to stay ahead of the growing sophistication of deepfake technologies, ensuring a secure and trustworthy digital ecosystem.

REFERENCES

[1] Raghava M S, Tejashwini S P, Kavya Sree, Sneha A, Naveen R, "AI deep fake detection research paper", (2023), International Journal of Novel Research and Development, https://www.ijnrd.org/papers/IJNRD2310407.pdf

[2] Preeti, Manoj Kumar, Hitesh Kumar Sharma, "A GAN-Based Model of Deepfake Detection in Social Media", (2023), International Conference on Machine Learning and Data Engineering, https://www.sciencedirect.com/science/article/pii/S1877050923001916?ref=pdf_download&fr=RR-2&rr=8e372cda8fdb3c01

[3] MA Shohel rana, Mohammad nur nobi, Beddhu Murali, Andrew H.sung, "Deepfake Detection: A Systematic Literature Review", (2022), Institute of Electrical and Electronics Engineers (IEEE), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9721302

[4] Prof. Aparna Bagde, Sakshi Fand, Kanchan Varma, Aditya Gawali, "Deep fake Detection using Deep Learning", (2023), International Journal of Science, Engineering and Technology, https://www.ijset.in/wp-content/uploads/IJSET_V11_issue6_571.pdf

[5] Aryaf Al-Adwan, Hadeel Alazzam, Noor Al-Anbaki and Eman Alduweib, "Using Deep Learning to Detecting Deepfakes", (2020), Institute of Electrical and Electronics Engineers (IEEE)

[6] Jacob Mallet, Dr. Rushit Dave, Dr. Naeem Seliya, Dr. Mounika Vanamala, "Detection of Deepfake Media Using a Hybrid CNN–RNN Model and Particle Swarm Optimization (PSO) Algorithm", (2024), Multidisciplinary Digital Publishing Institute

[7] Anuj Badale, Lionel Castelino, Chaitanya Darekar, and Joanne Gomes, "Deep Fake Detection using Neural Networks",(2021), International Journal of Engineering Research & Technology (IJERT)

[8] Yogesh Rai, Aditya Shinde, Pranav Patil, and Prof. Preeti Komati,"Deepfake Detection System",(2024), International Journal for Research in Applied Science & Engineering Technology (IJRASET)

[9] Trupti Kularkar, Tanvi Jikar, Vansh Rewaskar, Krupali Dhawale, Achamma Thomas, and Mangala Madankar," Deepfake Detection Using LSTM and ResNext",(2023), International Journal for Research in Applied Science & Engineering Technology (IJRASET)

[10] B. Manish, C. Manish, and B. Sai Kiran Reddy," DEEPFAKE DETECTION

ON FACE IMAGES & VIDEOS USING DEEP LEARNING",(2024), International Journal for Research in Applied Science & Engineering Technology (IJRASET)

[11] Shanjita Akter Prome, Neethiahnanthan Ari Ragavan, Md Rafiqul Islam, David Asirvatham, and Anasuya Jegathevi Jegathesan, "Deception Detection Using Machine Learning (ML) and Deep Learning (DL) Techniques: A Systematic Review", (2024), International Journal for Research in Applied Science & Engineering Technology (IJRASET)

[12] Aya Ismail, Marwa Elpeltagy, Mervat S. Zaki, and Kamal Eldahshan, "A New Deep Learning-Based Methodology for Video Deepfake Detection Using XGBoost", (2021), Sensors