An Intelligent System for Analysing and Detecting Deepfake Videos: A Deep Learning Approach

Ofualagba Mamuyovwi Helen[1], Asagba Prince Oghenekaro[2], Nathaniel Ojekudo[3]

[1, 2,3] Department of Computer Science, Ignatius Ajuru University of Education (IAUE) Port Harcourt, Nigeria

DOI: https://doi.org/10.51584/IJRIAS.2025.101100040

Received: 25 November 2025; Accepted: 02 December 2025; Published: 09 December 2025

ABSTRACT

The swift rise of Artificial Intelligence (AI) has brought about remarkable technological progress in numerous fields such as media, entertainment, and communication. Among the various outcomes of this advancement, deepfake technology stands out as a contentious issue; it involves using machine learning to artificially change video content. Although deepfakes have potential applications in creativity and education, they also pose significant ethical, legal, and social risks, such as spreading false information, impersonating others, and harming reputations. This increasing danger has underscored the urgency for effective and smart deepfake detection systems that can accurately and swiftly identify altered content. Despite ongoing research, many current deepfake detection models struggle with poor generalization and performance issues when faced with complex data sets. These limitations highlight a notable gap in research concerning the creation of resilient, flexible, and multimodal detection systems that can pinpoint inconsistencies in deepfake videos. This research aims to establish an intelligent model for both detecting and analyzing deepfake videos by utilizing cutting-edge deep learning methods. The study's primary goals are: (i) to create a deep learning framework that uses Long Short-Term Memory (LSTM) with attention mechanisms for analyzing temporal features, while also merging various features through Convolutional Neural Networks (CNN) and Graph Neural Networks (GNN) for feature extraction, (ii) to implement a software prototype in Python that can identify videos as either fake or genuine, and (iii) to assess and contrast the effectiveness of existing deepfake detection models with the new system. The research methodology employs agile and responsive software development strategies to facilitate adaptability and ongoing enhancement. Training, testing, and evaluation of the model occur on Google Colab, which allows for GPU acceleration to expedite processing. The dataset comprises multiple types of deepfake and genuine videos, which undergo thorough pre-processing, feature extraction, and fusion before classification. Various performance metrics, including accuracy, precision, recall, and F1-score, are used to assess the model's effectiveness. The main discoveries from this research indicate that the proposed intelligent model significantly boosts detection accuracy compared to current models. By incorporating attention mechanisms and multimodal fusion, the model can identify subtle discrepancies in both video frames and audio signals, thus improving its reliability and durability. The software developed achieved high classification accuracy, proving its applicability in real-life situations. In summary, we have successfully created a sophisticated system for detecting deepfakes that integrates deep learning techniques with contemporary programming resources.

Keywords: Deepfake detection, Attention Mechanism, CNN, LSTM, Video Forensics, Deep Learning

INTRODUCTION

Recently, quick progress in deep learning has resulted in the widespread application of advanced techniques for manipulating content, which raises important questions concerning the reliability of digital media. Deepfake technology represents a notable danger by generating highly realistic images, videos, or sounds, ultimately jeopardizing the trustworthiness of visual and auditory data (Rajalaxmi et al., 2023). Currently, the growing influence of deepfake technology poses significant issues for both individuals and companies. Deepfakes are created through manipulated images, videos, or audio by artificial intelligence (AI) systems (Conti et al., 2022). These misleading yet often realistic pieces of digital content can be used for various reasons, including spreading false information, influencing public perception, or engaging in deceitful practices. Consequently, there is a pressing need for robust methods to identify deepfakes and prevent these harmful fabrications from spreading (Agarwal et al., 2021; Agarwal et al., 2020a; Agarwal et al., 2020b).

A sophisticated detection model is currently being developed using advanced machine learning techniques to effectively identify deepfakes. These models scrutinize diverse visual and auditory signals in the content to ascertain whether it has been tampered with or altered (Trabelsi et al., 2022). Facial recognition technology is capable of detecting anomalies in facial expressions, eye movements, or skin texture that may signal a deepfake. Likewise, voice recognition systems can identify irregularities in speech patterns or audio artifacts that imply manipulation (Guo et al., 2023).

This advanced model for deepfake detection boasts the significant benefit of adapting to new challenges posed by deepfake technology. As advancements in this domain continue, traditional detection methods may struggle to keep up (Taeb & Chi, 2022). The adaptive nature of this model allows it to learn from fresh examples, thereby improving its accuracy over time. Training algorithms on a comprehensive dataset of both authentic and deepfake materials ensures that these systems can refine their skills consistently to remain ahead in this area.

The emergence of deepfake technology poses profound risks to the authenticity of digital content, highlighting the crucial necessity to devise effective detection approaches (Khodabakhsh et al., 2018; Khodabakhsh & Loiselle, 2020). With the increasing sophistication of machine learning tools, deepfakes can deceive and manipulate audiences, illustrating the critical need for strong strategies to recognize and combat these dangerous technologies (Costales et al., 2023). Deepfakes, generated through advanced deep neural networks and generative adversarial networks (GANs), can produce realistic audio and visual content by seamlessly integrating fake elements into genuine footage. This raises serious concerns, including the spread of misinformation, damage to individuals' reputations, and a decline in trust towards digital media. The growing availability and enhancement of deepfake technologies further stress the immediate need for effective countermeasures (Naik et al., 2022; Saxena et al., 2023).

Today's methods for detecting deepfakes are influenced by the interplay between improvements in deep learning models and the increasing complexity of deepfake creation techniques. The evolution of AI systems designed for deepfake detection faces many challenges and limitations, as highlighted by (Dagar & Vishwakarma, 2022).

The swift advancement of deepfake technology poses a major obstacle, moving faster than the progress of measures aimed at countering its impacts (Rani et al., 2022; Rebello et al., 2023). As this technology develops, it becomes essential for detection systems to enhance their capabilities to identify more convincing deepfakes. The variety of elements involved, including differing facial expressions, backgrounds, and audio variations, makes it difficult to create effective methods for spotting deepfakes (Chowdhary et al., 2021; Elpeltagy et al., 2023; Guo et al., 2023; Ismail et al., 2021, 2022). Additionally, the creation of algorithms for deepfake detection raises ethical and privacy concerns. Striking a balance between protecting individual privacy and preventing the harmful use of deepfake technology requires thorough examination and creative solutions (Agarwal et al., 2020b; Ismail et al., 2022). The effects of deepfakes go beyond privacy matters; they can manipulate political situations to influence public opinion and disrupt democratic systems. In light of the potential threats from deepfakes, governments and companies are putting resources into AI detection technologies as part of their cybersecurity efforts. Such technologies can aid in identifying and combating false information or disinformation campaigns that utilize deepfakes (Awotunde et al., 2023; Q. Li et al., 2023). Even with advancements in AI-driven detection, numerous issues remain. There exists an ongoing struggle between those who create deepfakes and those who work on detection solutions. As deepfake technology enhances, it becomes progressively more challenging for AI algorithms to differentiate between authentic information and altered content (Soleimani et al., 2023). Furthermore, ethical challenges arise from the use of deepfake detection technology due to possible infringements on individual rights. This research aims to fill significant gaps in current AI deepfake recognition systems. It aspires to make meaningful progress in the field by examining how deepfakes are created, exploring innovative deep learning models, and analyzing the ethical ramifications of detection technologies. The objective is to create robust, flexible, and ethically responsible AI deepfake detection tools that reduce societal risks linked to the misuse of this technology.

Problem Statement

The emergence of deepfake technology has resulted in a significant increase in the production and distribution of altered videos, which can pose substantial dangers to individuals, organizations, and society as a whole. As the algorithms behind deepfakes evolve quickly, they outstrip existing detection techniques. This leads to the propagation of misinformation, privacy violations, and threats to people's reputations and safety, even with efforts in place to combat these challenges. In addition, the absence of dependable and scalable automatic systems for identifying deepfake videos exacerbates the situation, complicating effective solutions and eroding trust in digital media. Consequently, there is a pressing need for reliable and efficient models capable of swiftly and accurately identifying altered content, thus protecting public trust, privacy, and the integrity of digital information. This research aims to create new algorithms and methodologies for the automatic detection of deepfake videos to offer viable solutions against the risks associated with deepfake manipulation.

Related Works

Saraswathi et al (2022) developed a deepfake detection method that merged temporal analysis and spatial feature learning using CNN and LSTM networks. For their feature extraction, they utilized a pre-trained ResNeXt-50 CNN to analyze twenty frames from each video. These features were then input into the LSTM model to determine whether the videos were deepfakes. The LSTM was provided with the same 2,048-dimensional feature vectors. In contrast to Jalui et al.'s research, these authors trained and validated their approach using videos sourced from multiple datasets, including the Deep Fake Detection Challenge (DFDC), FaceForensics++, and Celeb-DF datasets. Their method resulted in an accuracy of 90.37% on the test dataset derived from this set of sources.

Khedkar et al (2022) introduced a framework that combines CNN and LSTM to classify deepfake videos. They extracted features from forty frames using four CNN models that had been previously trained: VGG-19, ResNet-50 v2, Inception v3, and DenseNet-121. This was followed by the use of two LSTM layers for temporal analysis. A dense layer was then used to finalize the classification. Their framework was evaluated using the Face Forensics++ and DFDC datasets. The model achieved an area under the curve (AUC) score of 0.908 and an accuracy of 90.7%, particularly excelling when DenseNet-121 provided the spatial representation of frames, which was augmented by the two LSTM layers for temporal analysis. Similarly, Saif and associates (2022) proposed a deep temporal learning architecture using LSTM to detect face forgery in videos. They focused on contrastive frames to highlight cross-learning aspects. Additionally, they investigated several CNN architectures for extracting features from the frames. Among these, EfficientNet B3 achieved the best performance in feature extraction, recording a 97.3% accuracy on videos manipulated through deepfake methods and achieving 91.36%, 91.85%, and 88.15% accuracy for FaceSwap, Face2Face, and NeuralTexture alterations, respectively. Nevertheless, its overall performance on the FaceForensics++ dataset was not as strong as most baseline models. However, it performed exceptionally well on videos with low-quality compression, reaching an accuracy of 90.95%, and performed even better on videos with high-quality compression, achieving 98.7% accuracy.

In 2021, Tu et al proposed a recurrent neural network approach to tackle the challenges of deepfake detection. Their strategy combined CNN and GRU layers to extract features and understand the temporal sequence of video frames. To ensure proper face alignment and define spatial parameters for affine transformation, they used a spatial transformer network alongside a landmark-based alignment method. Their approach, employing DenseNet CNN with face alignment and a GRU layer, significantly enhanced predictions on the FaceForensics++ dataset, especially for videos altered using Face2Face and FaceSwap techniques. However, integrating all three components only marginally increased the deepfake detection accuracy to 96.9%, compared to 96.7% from the DenseNet model with just face alignment, revealing the difficulties in predicting complex high-quality manipulations. Ultimately, the landmark-based alignment method outperformed the Spatial Transformer Network in terms of accuracy.

In 2020, Montserrat et al presented a novel method for detecting face forgery in videos through a weighting system focused on false face probabilities within frames, enhanced by a GRU layer for temporal learning of feature vectors. The EfficientNet model creates a feature map that provides both a weighted value and a logit value for every detected face within the video, showing the probability of being authentic or forged. By aggregating all weights and logits, they calculated the overall forgery probability, pw, for the video. Combining logit values, weights, and the final pw probability with the feature vectors allows the GRU layer to further classify them as either genuine or deepfake. This approach was named Automatic Face Weighting (AFW). The combination of AFW with GRU layers achieved the highest accuracy of 91.88% .

In their study, Hao et al. (2022) investigated how to detect deepfake videos by using a technique that analyzes both the visual and audio components of the footage. They applied an EfficientNet-b5 CNN to classify the visuals, examining each frame to discern if the face is genuine or manipulated, which indicates forgery. By assigning labels to every video frame, they later assess the overall probability of manipulation throughout the video. These labeled frame probabilities and combined feature vectors are then input into a GRU layer to capture spatiotemporal characteristics, allowing for the classification of the video as either real or fake. Furthermore, the authors proposed a straightforward method for audio classification, utilizing adapted CNN architecture to analyze spectrograms of audio signals in order to gauge their authenticity. By merging visual and auditory information, they aimed to enhance the classification effectiveness for deepfakes. Emotional features derived from both visual and audio components are integrated into a latent feature space to determine whether a video is real or altered. However, the authors did not include any quantitative analysis or results from their multimodal method.

Jaiswal (2021) introduced a hybrid model that integrates LSTM and GRU layers for the classification of deepfake video frames, capitalizing on the advantages of each recurrent model type. The author described a deep learning structure aimed at binary classification, featuring two layers of both recurrent models topped with a single dense layer. To capture temporal features from each video frame before entering the hybrid recurrent layers, a specially designed CNN architecture was included. The best accuracy was achieved through a sequence of GRU layers followed by two LSTM layers compared to using only one recurrent model type. In the Deep Fake Detection Challenge Dataset, they found an accuracy of 0.8165 with the GRU-LSTM setup.

Tu et al. (2021) employed a Convolutional GRU (ConvGRU) framework in their research to analyze feature maps generated by a pre-trained ResNet50 CNN over ten video frames for deepfake detection. They chose to use ConvGRU due to its simplicity and reduced parameter count in comparison to Convolutional LSTM. Their method attained a remarkable accuracy of 94.56% and 89.3% AUC on the celeb-DF(v2) dataset. However, one significant limitation is the omission of critical architectural details, such as the dimensions of the feature maps, resulting from the combination of both ResNet50 and ConvGRU.

In their study, Ismail et al. (2022) introduced a novel technique combining gradient directions acquired through the Histogram of Oriented Gradients (HOG) method with image characteristics from a modified Xception Net framework to detect face forgery in videos. Their approach utilized a tailored Convolutional Neural Network (CNN) architecture that takes input images with HOG-generated gradient orientations, leading to a fixed-size feature vector output. To improve feature vector extraction from video frames, the authors advanced the Xception Net model. They integrated the feature vectors from both CNN models and processed them through multiple GRU layers for deeper analysis of the video's authenticity. To address differences caused by processing individual frames, eight sequences of GRU layers captured the temporal characteristics of the video frames. These features were subsequently input into a fully connected layer that concluded whether the final video was authentic or manipulated. When assessed against standard CNNs, their method performed exceptionally well, achieving a 95.56% accuracy and a 95.53% Area Under the Receiver Operating Characteristic (AUROC) score on the Celeb-DF and FaceForensics++ datasets, respectively.

To address the challenge of deepfake detection in datasets exhibiting class imbalance, Pu et al. (2022) proposed a novel loss function along with a temporal learning method. They distinguished real from fake faces in videos by combining feature maps from 300 video frames with temporal learning conducted by GRU layers, using both video-level and frame-level classification techniques. Features for each frame were derived using ResNet50. Moreover, they proposed a loss function that combines binary cross entropy with area under the curve (AUC) to effectively tackle the imbalanced class distribution issue in video and frame classification. Their experimental research involved the FaceForensics++ and Celeb-DF datasets. To simulate an imbalanced data distribution, samples from the DFDC dataset with different proportions of positive and negative examples were utilized. Notably, no data augmentation was implemented in this research. The proposed technique demonstrated excellent classification capabilities at both video and frame levels, even under imbalanced conditions with an excess of real face samples. It achieved a 98.9% AUC and a 96.5% accuracy on the imbalanced samples from the Celeb-DF dataset. Additionally, the combined loss function enhanced the model's performance.

In the work conducted by Elpeltagy et al. (2023), a multimodal feature-level strategy was examined for classifying deepfakes in videos. This technique relies on two distinct feature types extracted from both audio and visual frames of the input videos. Each component, visual and audio, is processed by its own CNN architecture to generate two separate feature vector representations. When combined, a GRU network evaluates the video’s temporal features. Finally, a fully connected layer uses these temporal features from the GRU model to ascertain whether a video is real or fake. Tests on the FakeAVCeleb dataset showed that this approach performed remarkably well.

Sun et al. (2023) offered a novel viewpoint on identifying deepfakes, suggesting that the task can be redefined as recognizing anomalies within multivariable time series data. This methodology attempts to spot both spatial and temporal inconsistencies caused by facial changes. The authors introduce a method called virtual anchor-based region displacement trajectory extraction, which aims to capture the spatial and temporal features of various parts of the face. Moreover, they developed a dual-stream spatial-temporal graph attention technique for tracking altered trajectories. Consequently, identifying deepfakes becomes a binary classification problem for multivariable time series, utilizing a gated recurrent unit backend for implementation. To validate this method, samples from the Face-Forensics++ database were applied.

He et al. (2021) proposed a method combining a video transformer with a face UV Texture Map for detecting deepfakes. Their technique outperformed current leading models based on analyses of five publicly available datasets. The segment embedding they introduced helps the network extract more relevant features, resulting in better accuracy in detection. Extensive evaluations showed that this model not only excelled with unseen datasets but also proved effective with previously tested datasets.

In their research, Messina et al. (2022) investigated various strategies that integrate convolutional neural networks, particularly emphasizing EfficientNet-B0, with different Vision Transformers. They compare their findings with the best available technologies. To merge two visual transformer frameworks utilizing multi-scaled feature maps derived from pre-trained EfficientNet-B0 CNNs, they proposed a solution. This method allows the model to learn deepfake features through multi-scale representations using the transformer approach. Despite ongoing advancements, video deepfake detection continues to seek improvements in generalization for more accurate and dependable results. To facilitate this, an EfficientNet-based patch extractor was employed, showcasing high efficiency, even with the smallest model in its category. This approach outperformed a conventional convolutional network that was trained from scratch, achieving an impressive AUC of 0.951 from the cross-visual transformer. Additionally, this strategy exhibited the highest average accuracy against four face manipulation techniques present in the FaceForensics++ dataset, outperforming all other existing alternatives.

Heo et al. (2023) introduced a fresh method for detecting DeepFakes using a Vision Transformer Model. This model combines CNN with patch-embedding features at the input stage, achieving commendable results in recent image classification tasks. It surpassed the traditional EfficientNet model, a two-dimensional CNN network. The latest state-of-the-art model secured an AUC of 0.972, while the new model achieved 0.978 in identical conditions without utilizing an ensemble technique. The proposed method attained an F1 score of 0.919, in contrast to the existing model’s F1 score of 0.906 at the same threshold of 0.55. Additionally, the authors recorded an AUC improvement of up to 0.17 compared to a more recent method. When applying the ensemble strategy, the new model reached an AUC of 0.982, whereas the top model managed only 0.981.

In their 2022 research, Xue et al proposed a method based on transformers aimed at identifying deepfakes by focusing on facial attributes. They noted that detecting deepfake content, particularly with intricate expressions and subtle changes in facial details or distorted images, has gained considerable attention from researchers. The authors mentioned that existing techniques, which analyze the full face, often miss critical details because they are affected by significant changes in image size. To tackle these challenges, they devised a specialized detection strategy that hones in on specific facial features with a transformer model, thereby minimizing the focus on damaged or unclear sections. They also developed a dataset named the Facial Organ Forgery Detection Test Dataset (FOFDTD), capturing facial features in different scenarios like being unmasked, masked, or wearing sunglasses. Experimental results demonstrated the new method's effectiveness, reflected in AUC scores of 92.43% for FaceForensics++ and 75.93% for DFD.

Zhang et al (2022) introduced TransDFD, a transformer model designed to detect deepfakes. This network learns both broad and particular manipulation patterns effectively. To improve its performance, a spatial attention scaling module has been added, which highlights essential features while reducing the influence of less critical ones. The model examines both local and global features with a focus on detailed intra-patch relationships while also recognizing enhanced inter-patch relationships in facial images. Testing against various publicly available datasets indicates that TransDFD offers unmatched efficiency and durability compared to current leading methods.

In a 2022 study, Khan and Dang-Nguyen presented a hybrid transformer network that employs a feature fusion approach for deepfake video detection. Their model combines XceptionNet and EfficientNet-B4 as feature extractors, fully integrated with a transformer structure, tested on FaceForensics++ and DFDC benchmarks. They also proposed two augmentation methods: face cut-out and random cut-out. This model not only matches the performance of advanced techniques but also benefits from improved detection capabilities and reduced overfitting through the use of these augmentation strategies.

The DFDT framework, introduced by Khormali and Yuan in 2022, employs end-to-end Transformers for detecting deepfakes. This framework is unique because it uses a re-attention mechanism rather than traditional multi-head self-attention layers. It consists of four main components: a multi-scale classifier, a multi-stream transformer block, attention-based patch selection, and patch extraction followed by embedding. These components aid the model in recognizing subtle manipulation signs in local image features and the global interactions of pixels at various levels of forgery. The effectiveness of this method was evaluated using multiple deepfake forensics benchmarks, achieving detection rates of 99.41% for FaceForensics++, 99.31% for Celeb-DF (V2), and 81.35% for WildDeepfake.

Coccomini et al. (2022b) explored whether it is possible to separate the detection of deepfakes from the training sample generation processes. They used the ForgeryNet dataset formatted for cross-forgery and compared two models: Vision Transformer and EfficientNetV2 (He et al., 2021). Their results suggest that EfficientNetV2 often specializes more, leading to improved performance during training. Conversely, Vision Transformers demonstrate impressive generalization skills, functioning well even with images produced by novel techniques.

Wang et al. (2022) presented the Multi-modal Multi-scale TRansformer (M2TR), which aims to identify subtle image manipulation artifacts at various scales through a transformer-based approach. This model detects local inconsistencies in images by examining regions of different sizes across multiple spatial levels. Additionally, it can locate forgery artifacts in the frequency domain and combines this information with RGB data using a cross-modality fusion block. Testing on a new, large dataset called Swapping and Reenactment DeepFake (SR-DF) showed that this method significantly outperforms current deepfake detection strategies.

A recent research effort by Wang et al. (2023) introduced a deep convolutional transformer model designed to merge crucial local and global features from images. This model employs techniques such as convolutional pooling and re-attention to improve both the features extracted and the important keyframes of images. Its aim is to enhance deepfake detection while clearly illustrating how video compression affects feature quantity between keyframes and regular image frames. Testing on various deepfake benchmark datasets indicated that this model outperforms many leading techniques regarding performance both within and across datasets.

Raza et al. (2023) developed a vision transformer model for classifying deepfakes, which integrates features from videos at three levels: spatiotemporal, temporal, and spatial-temporal. To extract spatial features, 2D convolutional layers are applied to individual video frames, while 3D convolutions analyze sequences of images to capture temporal differences between frames. Subsequently, facial spatiotemporal features are obtained through 3D convolutions applied to the video frames. This approach merges transformer representations from all three feature maps into one feature vector, which is then processed by a fully connected layer. It can detect potential manipulations across various feature domains, including spatial and temporal aspects. The AUC scores attained for the DFDC, Celeb-DF, and FaceForensics++ datasets were 0.926, 0.9624, and 0.9415, respectively. Notably, this method achieved the highest accuracy for videos from the Neural Texture subset of the FaceForensics++ dataset.

Feinland et al. (2022) presented a novel method that integrates two visual transformer frameworks to create multi-scaled feature maps by using two pre-trained EfficientNet-B0 CNNs. Their approach effectively merges feature representations through an attention mechanism, allowing it to extract important details at various scales from facial images. Furthermore, they devised a prediction strategy based on a majority vote for each detected face in a video, declaring the entire video as fraudulent if a single face is identified as fake. By combining this voting classification with the cross-visual transformer and leveraging EfficientNet-B0 for feature extraction, they achieved an AUC of 0.951. When compared to other leading methods, their technique secured the highest mean accuracy among the four face manipulation methods evaluated on the FaceForensics++ dataset.

To tackle the challenge posed by deepfake videos, Lin et al. (2023) unveiled a dual-subnet network with a transitional architecture, designed to learn and aggregate multi-scale insights and crucial facial features. This methodology identifies inherent traits that could indicate potential modifications in various regions of the target face by utilizing information across different scales. Concurrently, depth-wise convolutions are applied to high-dimensional features captured through an EfficientNet-B4 convolutional module. After these multi-scale and high-dimensional features are merged, they undergo processing via a vision transformer module, helping to reveal deeper contextual connections among the image features, eventually classifying the video as either real or fake. This method achieved outstanding performance across all tested datasets and ablation studies, boasting impressive accuracy rates, including 99.80% on the Celeb-DF dataset. However, it performed less effectively on the WildDeepfake dataset, earning a score of 82.63%.

In a separate study, Zhang et al. (2022) used a vision transformer architecture to carry out a temporal analysis of random facial areas, focusing on spatiotemporal inconsistencies that might indicate video manipulation. The spatial-temporal dropout technique eliminates random sections of each frame and facial segments based on a uniform distribution defined by dropout rates. From these chosen facial regions, multiple patches are generated and fed into the vision transformer architecture for inconsistency detection across frames. Using the output from the transformer, a fully connected layer assesses whether the video is real or fake. Since counterfeit artifacts tend to be concentrated in specific areas of the face, the model can capture distinctive characteristics that reveal localized spatial inconsistencies. Compared to twenty-five advanced methods, the results displayed the highest AUC scores across all deepfake datasets, averaging 99.8%, 99.1%, and 97.2% for the FaceForensics++, DFDC, and Celeb-DF datasets, respectively. Furthermore, the model adeptly managed all four facial manipulations within the FaceForensics++ dataset, achieving exceptional performance with scores exceeding 90% across all deepfake generation subsets.

Khalid et al. (2023) created the Swin Y-Net Transformers architecture to extract information effectively. The encoder, comprising a Swin transformer, segments the entire image into patches, while the decoder, built on U-Net, produces a segmentation mask for future classification. The experimental assessments conducted on the Celeb-DF and FF++ datasets demonstrated the capability of the proposed model to generalize well and accurately classify videos produced by DeepFakes, FaceSwap, Face2Face, FaceShifter, and NeuralTextures algorithms.

Zhou et al. (2017) put forth a two-stream network design aimed at detecting facial manipulations. They created a patch-based triplet network as an auxiliary stream to capture local noise residuals and camera characteristics, while GoogLeNet was trained to identify anomalies in face classification. Additionally, they utilized two separate online face-swapping applications to produce a new dataset with 2010 modified images, each featuring a manipulated face. The proposed two-stream network was evaluated using this newly collected dataset. The experimental findings confirmed the effectiveness of their method, achieving an area under the curve of 85.1%. This advanced two-stream network is complex to train compared to the results it delivers. However, in the Celeb-DF evaluation, it underperformed with an AUC of just 53.8%.

Afchar et al. (2018) introduced an automatic method for detecting facial tampering in videos at a mesoscopic level. Their research mainly targeted two recent techniques, DeepFake and Face2Face, which create hyper-realistic false videos. Traditional image forensics techniques often face challenges in analyzing videos due to compression that compromises the data. This study implemented a deep learning approach focused on the mesoscopic scale, featuring two networks with fewer layers to highlight image properties at this level. One network, called "MesoInception-4," is a modified version of the "Meso-4" inspired by the "Inception module" mentioned in reference [17]. Their method was tested using a private dataset, achieving an impressive accuracy of 98% for optimal outcomes. However, when evaluated against unseen datasets in [18], it showed resilience in certain cases, such as with "FaceForensics++," but faced difficulties detecting anomalies in specific Deepfake videos, as illustrated by an AUC of 84.3% for the UADFV dataset.

Tsai et al. (2020) presented a real-time surveillance application that incorporates a deep learning system designed for recognizing actions among multiple people. The authors addressed the challenges of recognizing simultaneous actions of various individuals and proposed enhancements such as a "zoom-in" feature and nonmaximum suppression (NMS) to boost accuracy. Their system allows for real-time recognition of multiple individuals' actions, making it suitable for environments like long-term care facilities.

Goswami et al. (2014) introduced MDLFace, an innovative face recognition algorithm for videos that utilizes memorable frames and deep learning techniques to achieve outstanding performance while reducing false accept rates. Their crucial findings include the development of a deep learning-driven frame selection algorithm that leverages memorability to extract and match facial features, along with achieving top-tier performance with minimal false accept incidents. The study conducted by Korshunov and Marcel (2019) investigates several important aspects regarding Deepfake videos. It discusses how easy it is to create these videos, how vulnerable face recognition technologies are to them, the importance of establishing effective detection methods, the release of a public database featuring Deepfake videos, and the pressing need for stronger detection solutions in the future. Current detection techniques and face recognition systems find it challenging to detect deepfake videos produced with GANs because of the poor quality of the videos. Moreover, advancements in face-swapping technology are likely to heighten this issue.

Uddin et al. (2017) introduced a robust facial expression recognition system that leverages depth cameras and deep learning, enhanced by cloud computing for faster processing, and achieves a mean recognition accuracy of 96.25%. The paper emphasizes the critical role of reliable features in achieving accurate facial expression recognition, suggesting a method that incorporates deep learning and cloud resources, which outperforms traditional techniques with an average accuracy rate of 96.25%.

Miao et al. (2019) present a CNN-based system capable of identifying real-time facial expressions through joint supervision and transfer learning. This system shows remarkable accuracy on well-established datasets such as JAFFE and CK+, highlighting the potential diverse uses of automatic facial expression analysis. For facial expression recognition, the CNN-based system achieved top-tier accuracy on JAFFE and CK+, completing classification tasks significantly faster than traditional classifiers and outperforming similar CNN-based systems in both speed and precision.

Dong et al. (2020) introduce a video-focused cascaded intelligent face detection algorithm grounded in deep learning principles. This algorithm exhibits resilience against rotating faces, maintains real-time processing capabilities, and shows outstanding detection effectiveness for both single and multiple faces. With advancements in face recognition and technology for security monitoring, intelligent video retrieval is becoming increasingly crucial for video surveillance systems. The proposed face detection algorithm delivers strong outcomes for both single and multi-face images while effectively addressing the requirement for real-time detection.

Hu et al. (2022) introduce FInfer, a detection framework based on frame inference, designed to address the challenges of recognizing high-quality Deepfake videos. By incorporating information theory analyses, FInfer demonstrates promising results in terms of efficiency and detection performance. The capability of the FInfer framework to identify visually high-quality Deepfake videos is supported by information theory insights and extensive experimental data.

In a recent paper, Ismail et al. (2021) unveil a new deepfake detection technique named YOLO-CNN-XGBoost, showcasing impressive accuracy and performance on the CelebDF-FaceForencics++ dataset, exceeding that of existing leading methods. The proposed method achieves an area under the receiver operating characteristic curve of 90.62% on the merged CelebDF-FaceForencics++ dataset, illustrating the high effectiveness of YOLO-CNN-XGBoost, which surpasses existing techniques in deepfake detection.

The paper by Yin et al. (2021) introduces a two-stream network structure designed to effectively handle the challenges presented by low-quality data. This architecture achieves state-of-the-art results when tested on the FaceForensics++ dataset. In this model, one stream employs learnable SRM filters to capture noise features for Deepfake detection in videos, while the second stream leverages semantic inconsistencies found in RGB data. The results from the experiments highlight the FaceForensics++ dataset's superior performance.

El-Gayar et al. (2024) proposes an enhanced technique for identifying deepfake videos. This method combines graph neural networks (GNN) with a four-block CNN stream that includes convolution, batch normalization, activation functions, and a flattening step. The detection is conducted in two stages, which are then integrated through three different fusion methodologies: additive fusion (FuNet-A), element-wise multiplicative fusion (FuNet-M), and concatenation fusion (FuNet-C). This innovative approach overcomes the shortcomings of conventional deepfake detection methods, which often lag behind the advanced technologies used to create deepfakes. The presented model shows remarkable effectiveness, achieving a training and validation accuracy of 99.3% after 30 epochs, while being tested across various datasets. Below are the strengths, key contributions, and limitations identified in the work of El-Gayar et al. (2024).

METHODOLOGY

This project embraced the Agile methodology for software development, a framework recognized for its efficiency in managing projects. Agile emphasizes iterative progress, enabling the requirements and solutions to grow through collaboration between diverse, self-organizing teams and their users (Tyagi, 2021). In general, Agile methods advocate for a well-organized project management process that allows for ongoing evaluation and adjustments. They encourage a leadership approach that nurtures collaboration, independence, and responsibility. Furthermore, Agile includes a series of best practices in engineering that strive to produce high-quality software promptly, while also considering how development aligns with customer expectations and business goals.

Agile development encompasses any processes that adhere to the principles outlined in the Agile Manifesto. Created by fourteen prominent figures in the software field, this Manifesto captures their thoughts on what works well and what doesn’t in software development. For this particular project, the Dynamic Software Development Method (DSDM) was the chosen methodology.

Dynamic Software Development Methodology

The Dynamic Software Development Methodology (DSDM) is a Rapid Application Development (RAD) technique that incorporates incremental prototyping to address common software development issues like missed deadlines, budget overruns, and insufficient user engagement. As part of Agile methodology, DSDM aims to deliver projects on schedule and within budget while remaining adaptable to changing requirements. This flexibility makes DSDM ideal for projects with unclear or evolving demands throughout the development stages (Babatunde, 2016).

The Dynamic Systems Development Method employs an iterative approach with incremental prototyping, following the 80 percent rule to guide the next iteration. This approach provides stakeholders with a clear and detailed project description during development. Furthermore, it cultivates a collaborative environment where the project team works together throughout the software development lifecycle (Fahad et al., 2017).

Justification for the Choice of DSDM Methodology

By adopting the Dynamic Software Development Method (DSDM), teams can create a timeline for ongoing project deliveries, implement incremental solutions, adapt based on feedback, and meet expected benefits. DSDM serves as an Agile model that can significantly aid organizations accustomed to project changes, enhancing their ability to deliver value and shorten time to market. Anwer et al. (2017) highlight that a major advantage of the Dynamic Systems Development Method is its facilitation of cooperation and collaboration among all stakeholders involved in a project, leading to successful project completion. Additionally, DSDM is well-suited for highly iterative program designs, such as large-scale machine learning models. Benefits of dynamic software development, as identified by Cohen et al. (2004), include:

1. It facilitates the quick development of applications while embracing agile practices.
2. This framework is flexible enough to integrate the best techniques from various methods.
3. It supplies clear guidelines for different aspects of projects, including management, risk control, and development strategies.

Data Collection Method

The dataset utilized for training and testing the intended system was sourced from the Kaggle machine learning library. This deepfake collection includes both audio and visual deepfake datasets. It features a mix of altered images and genuine photographs. The modified images are those whose faces have been edited in various ways. A thorough analysis of this dataset was conducted to maximize information extraction from the images and video streams. Each image is a 256 x 256 jpeg depiction of a human face, whether real or fake. The visual deepfake dataset can be found at: https://www.kaggle.com/datasets/abdallamohamed312/in-the-wild-audio-deepfake, while the audio part is available at: https://www.kaggle.com/datasets/abdallamohamed312/i

Dataset Upload and Model Training

To begin using the dataset within the model, we first downloaded it and reduced its size from 18GB to 1.28GB, which included both the training and testing datasets. After that, we zipped the dataset into a folder and uploaded it to the Google Colab file menu during runtime, where it was then unzipped and made ready for the model. This reduction was necessary because the original dataset was too large for a direct upload, so we compressed it to a more manageable size for easier access when training and testing the model. We successfully uploaded the deepfake video datasets to the Colab Python Jupyter notebook in around 60 seconds.

Analysis of the Existing System

The system previously designed by El-Gayar et al. (2024) integrates two deep learning classification models:

convolutional neural networks and graph neural networks. Its primary function is to differentiate between deepfake films and genuine videos by spotting visual inconsistencies. By merging features from CNNs and mini GNNs into a trainable network from end to end, the model was developed to improve deepfake video detection outcomes. The CNN effectively captures visual characteristics from each frame, aiding the model in managing various deepfake detections, while the GNN leverages spatial-temporal data from the video stream.

The training and evaluation of this system used three datasets: FaceForensics++, DFDC, and Celeb-DF. The FaceForensics dataset contains over 1000 authentic YouTube videos showcasing diverse faces, lighting conditions, and angles. Upon evaluation, the model achieved a validation accuracy of 99.3% in detecting deepfake videos after 30 training epochs.

Description of the Existing System Architecture

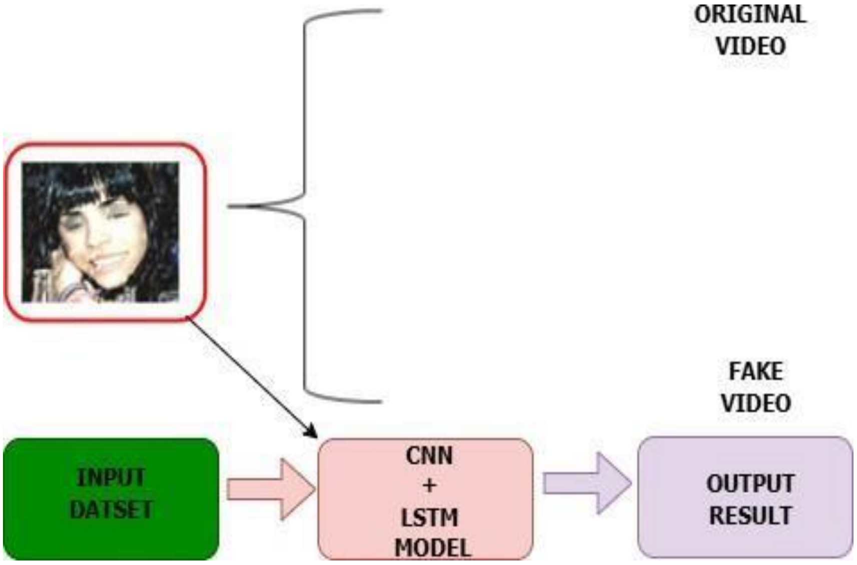
The current system utilizes a layered structure that leverages multiple scales of image features while decreasing the spatial dimensions as it goes deeper. This design enables the model to more efficiently recognize distinct features and characteristics. By using a hierarchical approach, accuracy is improved through a reduction in parameters, leading to stronger models. Such architectures are particularly well-suited for image datasets as they can efficiently capture specific attributes of samples while keeping complexity low. The mini GNN transforms image patches into graphs. The model is comprised of concatenated and compressed segments. Each segment includes a Feedforward Network sub-block and a GraphNet sub-block. The GraphNet includes two convolutional layers, a graph convolution layer, along with two convolutional layers that utilize batch normalization and ReLU activation. Linear layers enhance diversity and integrate node features pre- and post-graph convolution. ReLU activation helps reduce interference across layers following graph convolution.

Different neural networks can provide unique representations from this data. CNNs focus on both spatial and spectral features, while GCNs analyze relationships between samples. However, no individual model can capture all necessary information. To enhance discrimination power, the current system effectively integrates CNNs and GCNs. MiniGCNs are progressively trained and subsequently integrated with CNNs. The end-to-end fusion model, FuNet, merges the advantages of both architectures.

Design of the Proposed System

The new system employs an attention mechanism to boost the accuracy of detection and classification, reducing issues like noise, misclassification, and false positives. Using a recurrent neural network (RNN) long short-term memory (LSTM) model, the attention mechanism allows the system to effectively analyze multimodal datasets, identifying deepfake streams as either authentic or counterfeit. It operates as an encoder-decoder LSTM, where the encoder processes the full input sequence and encodes it into a context vector representing the last hidden state of the LSTM, ensuring a robust memory of the input data. Meanwhile, the decoder LSTM generates the dataset sequentially. The three-layer deep LSTM model helps decompose the input data, identifying key components by assessing their significance based on how they align with the training dataset. It judges how much focus should be applied to each data piece, whether it is a frame, sound, or text input. Ultimately, it combines all data elements, weighting the crucial parts more heavily, before passing the results to the CNN/GNN component that performs the final deepfake detection and classification based on visual, audio, and textual inputs.

Fig 1: Design of the Proposed DeepFake Smart Model System



LSTM Attention Mechanism

The LSTM, or Long Short-Term Memory network, belongs to the family of recurrent neural networks (RNNs) that excel with sequential data. This mechanism is employed to explore the sequential links present in image data.

Input Sequence (X1, X2, ..., Xn): This component denotes pixel or patch data organized in sequences.

Hidden States (h1, h2, ..., hn): These represent the LSTM's internal states, which store critical sequential details derived from the input.

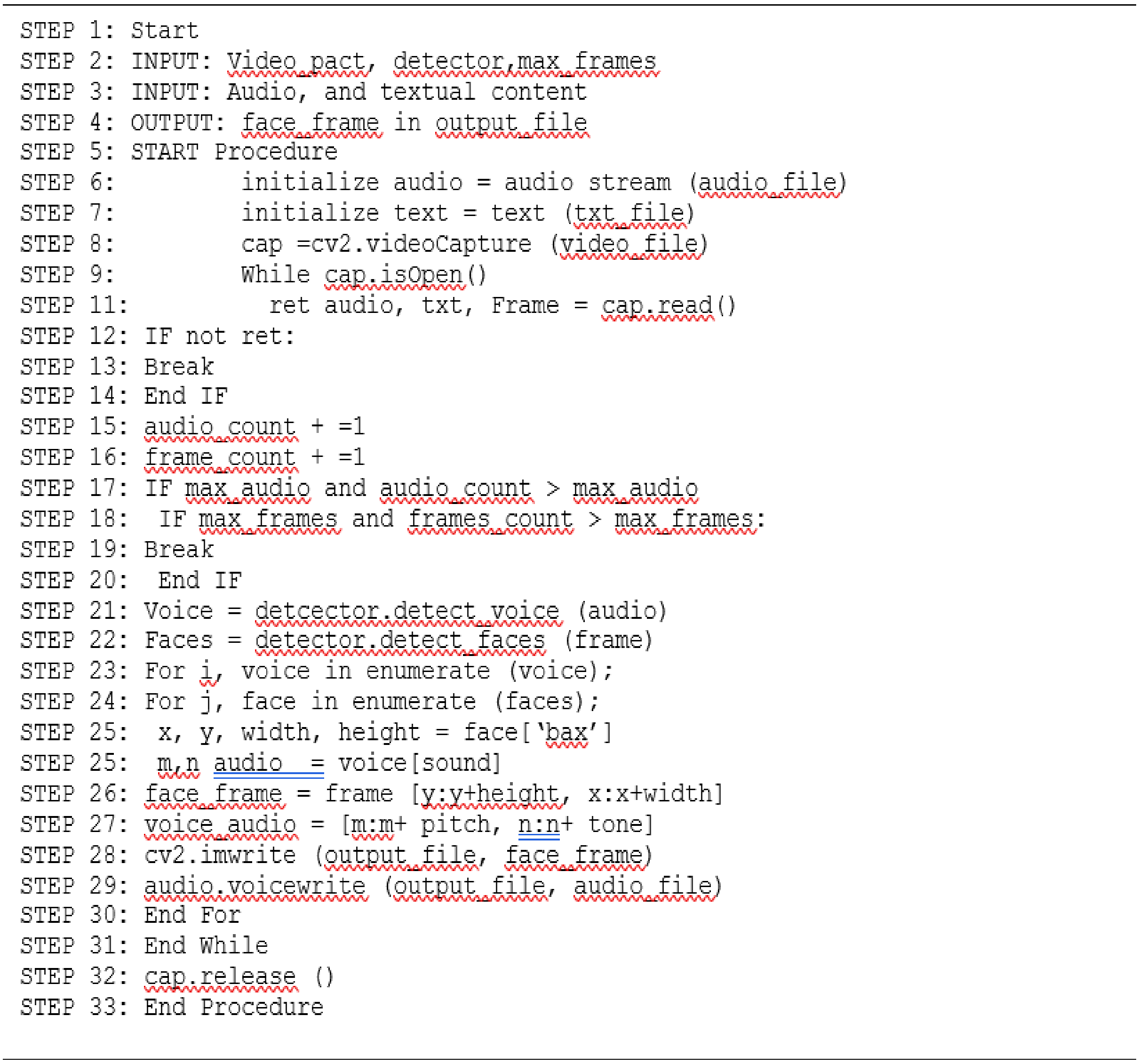
Bidirectional Arrows: These indicate the application of a bidirectional LSTM that analyzes sequences in both directions, enhancing the system's comprehension of contextual relationships within the data.

Attention Mechanism: This part zeroes in on the most significant sections of the sequence to aid in predictions. It boosts effectiveness by highlighting crucial features while disregarding less essential information.

GCN (Graph Convolutional Network)

The output from the LSTM feeds into a Graph Convolutional Network (GCN), which models the connections between pixels or image patches. GCNs are particularly adept at processing non-grid structured data, such as feature relationships.

Purpose: This captures complex dependencies and interactions among the image features.



```
STEP 1: Start
STEP 2: INPUT: Video pact, detector,max frames
STEP 3: INPUT: Audio, and textual content
STEP 4: OUTPUT: face frame in output file
STEP 5: START Procedure
STEP 6:         initialize audio = audio stream (audio file)
STEP 7:         initialize text = text (txt file)
STEP 8:         cap =cv2.videoCapture (video file)
STEP 9:         While cap.isOpen()
STEP 11:          ret audio, txt, Frame = cap.read()
STEP 12: IF not ret:
STEP 13: Break
STEP 14: End IF
STEP 15: audio count + =1
STEP 16: frame count + =1
STEP 17: IF max audio and audio count > max audio
STEP 18:  IF max frames and frames count > max frames:
STEP 19: Break
STEP 20:  End IF
STEP 21: Voice = detcector.detect voice (audio)
STEP 22: Faces = detector.detect faces (frame)
STEP 23: For i, voice in enumerate (voice);
STEP 24: For j, face in enumerate (faces);
STEP 25:  x, y, width, height = face['bax']
STEP 25:  m,n audio  = voice[sound]
STEP 26: face frame = frame [y:y+height, x:x+width]
STEP 27: voice audio = [m:m+ pitch, n:n+ tone]
STEP 28: cv2.imwrite (output file, face frame)
STEP 29: audio.voicewrite (output file, audio file)
STEP 30: End For
STEP 31: End While
STEP 32: cap.release ()
STEP 33: End Procedure
```

Algorithm of the Proposed System

Implementation

Every intelligent system that is created and used aims to offer solutions within a specific area, which helps decrease the potential for mistakes and risks that could arise from direct human involvement in the process. The innovative model developed for detecting fake audio and video streams utilizes elements of computer vision (CV) to identify and categorize fake video content. This helps to address impersonation and other malicious activities that may arise from altered video streams, as well as the associated security and social issues. This timely response is crucial for tackling theft, criminal actions, and disturbances to public order.

The process of implementation involves using the system to carry out the tasks it was designed for. Essentially, this means operating the system according to its intended requirements and guidelines. This is a series of organized actions aimed at ensuring that the system is effectively delivered and utilized to meet its intended objectives and goals.

Cloud Services

In this research, cloud-based deep learning services such as Google Collaboratory, commonly referred to as Google Colab, and Kaggle are employed for convenient access to a wide variety of datasets. Utilizing cloud services for developing and deploying deep learning models has also cut down on the costs associated with purchasing high-end and complex graphic processing units (GPUs) and allows for faster processing. The extensive dataset options available through Kaggle make it easy for data scientists and developers of deep learning models to find, prepare, and manage different kinds of datasets. Meanwhile, Google Colab, which was introduced by Google in 2015, offers free GPU access, a Python interpreter, TensorFlow, Jupyter notebooks, and other essential libraries and resources necessary for building and applying deep learning models. Its free nature makes it user-friendly and cost-effective for model development, training, and evaluation.

Choice of Programming Language

The proposed system will be implemented using Python as the programming language. Python boasts a vast array of libraries and frameworks that streamline coding and enhance development efficiency. This open-source language is user-friendly and comes with abundant resources and excellent documentation. Its platform-independent nature, flexibility, and readability, along with a broad ecosystem, make it ideal for visualization purposes. Recently, Python has become one of the leading programming languages for developing artificial intelligence (AI) and machine learning models due to its numerous features and resources that support the creation of AI, machine learning, and deep learning applications.

RESULTS AND DISCUSSION

Evaluation Metrics

Table 1: Evaluation metrics of the Existing Systems

SN	EVALUATION METRICS	RESULTS (%)
1	VALIDATION ACCURACY	99.3
2	ACCURACY	91.05
3	PRECISION	
4	RECALL	
5	F1-SCORE	
6	AUC-ROC	91.0

Figure 2 Evaluation Metrics for the Existing System

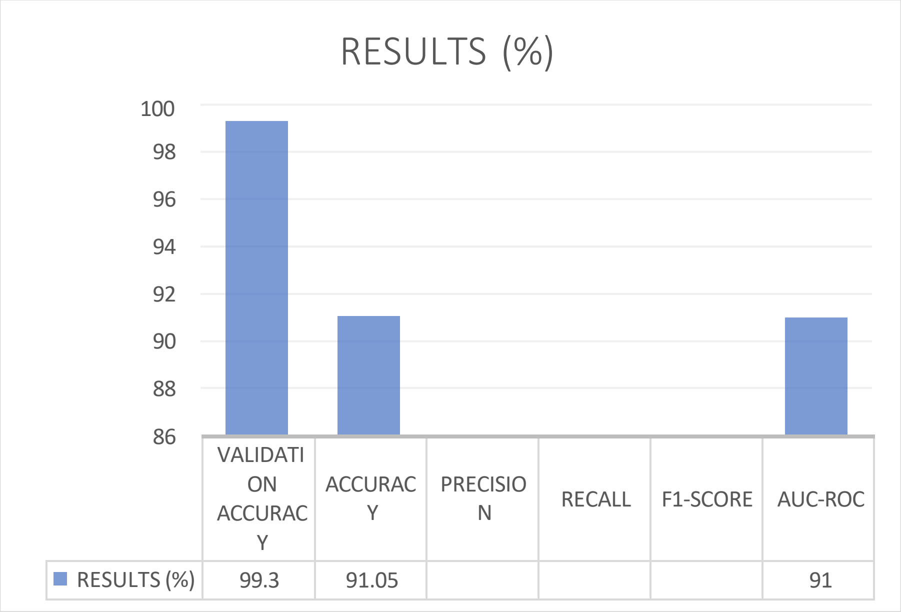


Table 2 Evaluation Metrics of New System

SN	EVALUATION METRICS	RESULTS (%)
1	ACCURACY	98.1
2	PRECISION	81.4
3	RECALL	86.8
4	F1-SCORE	84.3
5	AUC-ROC	81.8

Figure 3 Evaluation Metrics Chart of the New System

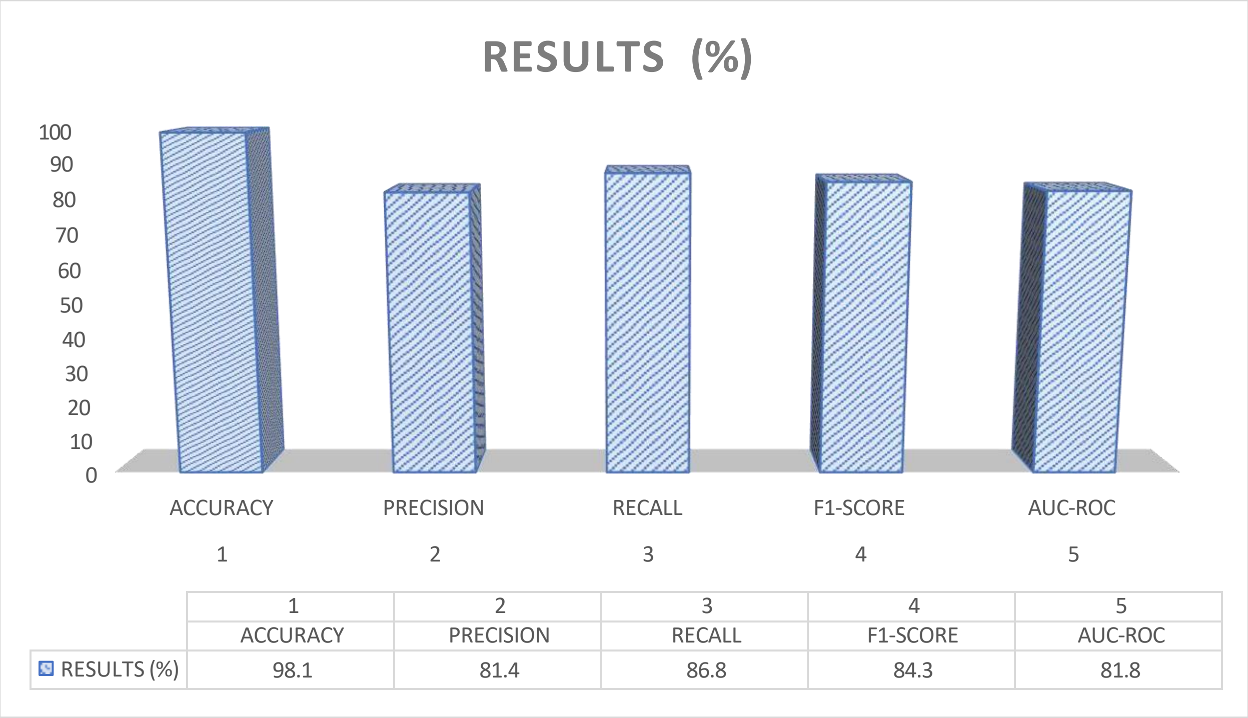
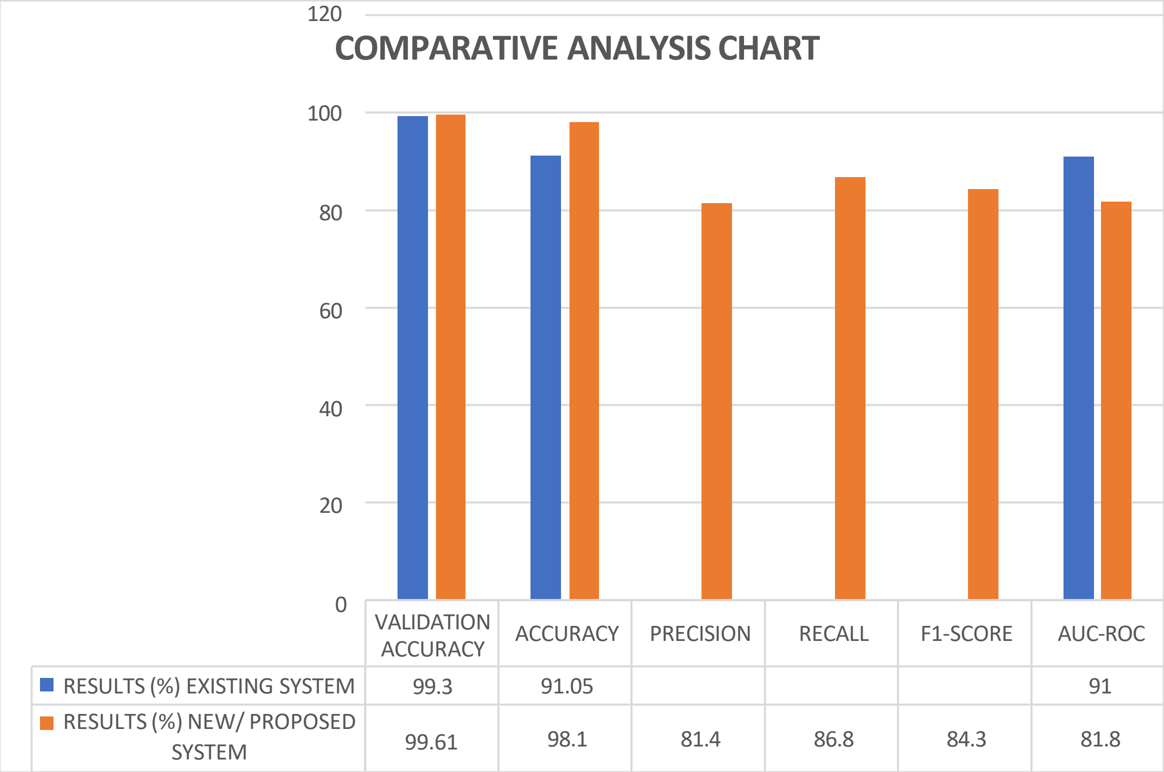


Table 3 Result of the Existing and New System

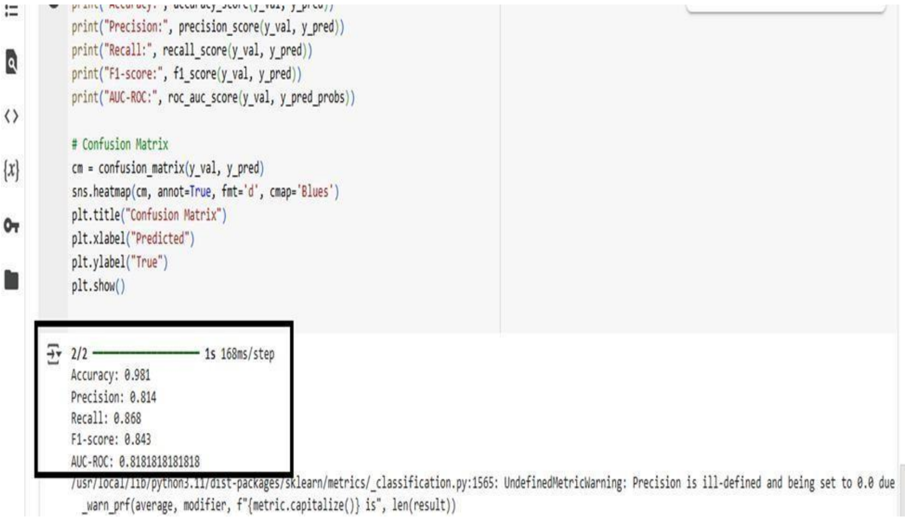
SN	EVALUATION METRICS	RESULTS (%)	
		EXISTING SYSTEM	NEW/ PROPOSED SYSTEM
	VALIDATION ACCURACY	99.3	99.61
1	ACCURACY	91.05	98.1
2	PRECISION		81.4
3	RECALL		86.8
4	F1-SCORE		84.3
5	AUC-ROC	91.0	81.8

Figure 4 Evaluation of Metrics of the Existing and New System



	VALIDATION ACCURACY	ACCURACY	PRECISION	RECALL	F1-SCORE	AUC-ROC
■ RESULTS (%) EXISTING SYSTEM	99.3	91.05				91
■ RESULTS (%) NEW/ PROPOSED SYSTEM	99.61	98.1	81.4	86.8	84.3	81.8

Figure 5 Model Predicted Results/ Output



```
print("Accuracy:", accuracy_score(y_val, y_pred))
print("Precision:", precision_score(y_val, y_pred))
print("Recall:", recall_score(y_val, y_pred))
print("F1-score:", f1_score(y_val, y_pred))
print("AUC-ROC:", roc_auc_score(y_val, y_pred_probs))

# Confusion Matrix
cm = confusion_matrix(y_val, y_pred)
sns.heatmap(cm, annot=True, fmt='d', cmap='Blues')
plt.title("Confusion Matrix")
plt.xlabel("Predicted")
plt.ylabel("True")
plt.show()
```

```
2/2 ━━━━━━━━━━━━━━━━━━━━ 1s 168ms/step
Accuracy: 0.981
Precision: 0.814
Recall: 0.868
F1-score: 0.843
AUC-ROC: 0.8181818181818
/usr/local/lib/python3.11/dist-packages/sklearn/metrics/_classification.py:1565: UndefinedMetricWarning: Precision is ill-defined and being set to 0.0 due
  _warn_prf(average, modifier, f"{metric.capitalize()} is", len(result))
```

CONCLUSION

The importance of a more effective deepfake detection and classification model is critical, as the use of deepfake media to create deceptive videos and audio continues to rise worldwide, leading to serious consequences. The advancement of deep learning has opened new avenues for developing improved and hybrid models aimed at reducing the potential damage caused by misleading deepfake content, especially online, which can distort information and foster discord among individuals, groups, and organizations, resulting in significant economic harm. The newly developed model has shown a lower incidence of falsehoods, successfully differentiating between authentic and fabricated content in video and audio streams.

This model achieved a detection and prediction accuracy of 0.981 (98.1%), precision of 0.814 (81.4%), recall of 0.868 (86.8%), F1-Score of 0.843 (84.3%), and an AUC-ROC of 0.818 (81.8%). These results represent a notable improvement compared to the existing system by El Gayer et al. (2024), which has validation accuracy at 99%, prediction accuracy of 91.5%, and an AUC-ROC of 91.0%, surpassing the previous system's validation and prediction accuracies by 0.31% and 7.05%. Additionally, this model demonstrated high predictive accuracy combined with low rates of false positives. This innovation could assist in identifying the erratic use of deepfake content by malicious internet users, helping to alleviate the negative impact of misinformation and related issues affecting individuals, groups, and organizations.

REFERENCES

1. Aduwala, S. A., Arigala, M., Desai, S., Quan, H. J., & Eirinaki, M. (2021). Deepfake detection using GAN discriminators. Proceedings of the IEEE 7th International Conference on Big Data Computing Service and Applications (BigDataService 2021). https://doi.org/10.1109/BigDataService52369.2021.00014
2. Afchar, D., Nozick, V., Yamagishi, J., & Echizen, I. (2018). MesoNet: A compact facial video forgery detection network. 2018 10th IEEE International Workshop on Information Forensics and Security (WIFS).
3. Agarwal, A., Agarwal, A., Sinha, S., Vatsa, M., & Singh, R. (2021). MD-CSDNetwork: Multi-domain cross stitched network for deepfake detection. 2021 16th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2021), 1–8.
4. Agarwal, S., El-Gaaly, T., Farid, H., & Lim, S.-N. (2020a). Detecting deep-fake videos from appearance and behavior. 2020 IEEE International Workshop on Information Forensics and Security (WIFS), 1–6.
5. Agarwal, S., El-Gaaly, T., Farid, H., & Lim, S.-N. (2020b). Detecting deep-fake videos from appearance and behavior. 2020 IEEE International Workshop on Information Forensics and Security (WIFS), 1–6.
6. Agarwal, S., Farid, H., Fried, O., & Agrawala, M. (2020a). Detecting deep-fake videos from phoneme-viseme mismatches. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2814–2822.
7. Agarwal, S., Farid, H., Fried, O., & Agrawala, M. (2020b). Detecting deep-fake videos from phoneme-viseme mismatches. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2814–2822.
8. Akgün, E., & Demir, M. (2018). Modeling course achievements of elementary education teacher candidates with artificial neural networks. International Journal of Assessment Tools in Education, 5(3).
9. Al-Dhabi, Y., & Zhang, S. (2021). Deepfake video detection by combining convolutional neural network (CNN) and recurrent neural network (RNN). 2021 IEEE International Conference on Computer Science, Artificial Intelligence and Electronic Engineering (CSAIEE 2021).
10. Alkinani, H., Al-Hameedi, A. T., Dunn-Norman, S., Flori, R., Alsaba, M., & Amer, A. (2019, November). Applications of artificial neural networks in the petroleum industry: A review. Society of Petroleum Engineers. https://doi.org/10.2118/195072-MS
11. Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q. E. U., Saleem, K., & Faheem, M. H. (2023). A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN. Electronics (Switzerland), 12(1).
12. Amerini, I., Galteri, L., Caldelli, R., & Del Bimbo, A. (2019). Deepfake video detection through optical flow based CNN. 2019 International Conference on Computer Vision Workshop (ICCVW). https://doi.org/10.1109/ICCVW.2019.00152

13. Anas Raza, M., Mahmood Malik, K., & Ul Haq, I. (2023). HolisticDFD: Infusing spatiotemporal transformer embeddings for deepfake detection. Information Sciences, 645. https://doi.org/10.1016/j.ins.2023.119352
14. Anjum, U. (2021). Artificial intelligence, machine learning and deep learning in healthcare. Bioscience Biotechnology Research Communications, 14(7). https://doi.org/10.21786/bbrc/14.7.36
15. Awotunde, J. B., Jimoh, R. G., Imoize, A. L., Abdulrazaq, A. T., Li, C. T., & Lee, C. C. (2023). An enhanced deep learning-based deepfake video detection and classification system. Electronics (Switzerland), 12(1). https://doi.org/10.3390/electronics12010087
16. Babu, M. R., & Veena, K. N. (2021). A survey on attack detection methods for IoT using machine learning and deep learning. 2021 3rd International Conference on Signal Processing and Communication (ICSPC). https://doi.org/10.1109/ICSPC51351.2021.9451740
17. Chang, W.-J., Chen, L.-B., & Su, K.-Y. (2019). DeepCrash: A deep learning-based Internet of Vehicles system for head-on and single-vehicle accident detection with emergency notification. IEEE Access, 7, 148163–148175.
18. Cheng, B., & Titterington, D. M. (1994). Neural networks: A review from a statistical perspective. Statistical Science, 9(1).
19. Chintha, A., Thai, B., Sohrawardi, S. J., Bhatt, K., Hickerson, A., Wright, M., & Ptucha, R. (2020). Recurrent convolutional structures for audio spoof and video deepfake detection. IEEE Journal of Selected Topics in Signal Processing, 14, 1024–1037.
20. Cho, K., Van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., & Bengio, Y. (2014a). Learning phrase representations using RNN encoder-decoder for statistical machine translation. Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP), 1724–1734.
21. Cho, K., Van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., & Bengio, Y. (2014b). Learning phrase representations using RNN encoder-decoder for statistical machine translation. EMNLP 2014 - 2014 Conference on Empirical Methods in Natural Language Processing, Proceedings of the Conference.
22. Choi, R. Y., Coyner, A. S., Kalpathy-Cramer, J., Chiang, M. F., & Campbell, J. P. (2020). Introduction to machine learning, neural networks, and deep learning. Translational Vision Science and Technology, 9(2).
23. Chowdhary, C. L., Alazab, M., Chaudhary, A., Hakak, S., & Gadekallu, T. R. (2021). Computer vision and recognition systems using machine and deep learning approaches: Fundamentals, technologies and applications.
24. Chowdhury, M. I., Zhao, Q., Su, K., & Liu, Y. (2021). CMNN: Coupled modular neural network. IEEE Access, 9.
25. Ciftci, U., Demir, I., & Yin, L. (2020a). How do the hearts of deep fakes beat? Deep fake source detection via interpreting residuals with biological signals. 2020 IEEE International Joint Conference on Biometrics (IJCB), 1–10.
26. Ciftci, U., Demir, I., & Yin, L. (2020b). How do the hearts of deep fakes beat? Deep fake source detection via interpreting residuals with biological signals. 2020 IEEE International Joint Conference on Biometrics (IJCB), 1–10.
27. Coccomini, D. A., Caldelli, R., Falchi, F., Gennaro, C., & Amato, G. (2022). Cross-forgery analysis of Vision Transformers and CNNs for deepfake image detection. MAD 2022 - Proceedings of the 1st International Workshop on Multimedia AI Against Disinformation. https://doi.org/10.1145/3512732.3533582
28. Coccomini, D. A., Messina, N., Gennaro, C., & Falchi, F. (2022). Combining EfficientNet and Vision Transformers for video deepfake detection. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13233 LNCS. https://doi.org/10.1007/978-3-031-06433-3_19
29. Conti, E., Salvi, D., Borrelli, C., Hosler, B., Bestagini, P., Antonacci, F., Sarti, A., Stamm, M. C., & Tubaro, S. (2022). Deepfake speech detection through emotion recognition: A semantic approach. ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, 2022-May. https://doi.org/10.1109/ICASSP43922.2022.9747186

30. Costales, J. A., Shiromani, S., & Devaraj, M. (2023). The impact of blockchain technology to protect image and video integrity from identity theft using deepfake analyzer. International Conference on Innovative Data Communication Technologies and Application (ICIDCA 2023) - Proceedings. https://doi.org/10.1109/ICIDCA56705.2023.10099668
31. Dagar, D., & Vishwakarma, D. K. (2022). A literature review and perspectives in deepfakes: Generation, detection, and applications. International Journal of Multimedia Information Retrieval, 11(3).
32. Dami, L. (2019). Deepfake Salvador Dalí takes selfies with museum visitors. The Verge. https://www.theverge.com/2019/6/19/18691125/deepfake-salvador-dali-museum-visitor-experience-ai.
33. Das, A., & Sebastian, L. (2023). A comparative analysis and study of a fast parallel CNN based deepfake video detection model with feature selection (FPC-DFM). Proceedings of the ACCTHPA 2023 - Conference on Advanced Computing and Communication Technologies for High Performance Applications.
34. Delgado, S., Moran, F., Jose, J. C. S., & Burgos, D. (2021). Analysis of students' behavior through user clustering in online learning settings, based on self organizing maps neural networks. IEEE Access, 9, 134244–134258. https://doi.org/10.1109/ACCESS.2021.3115024
35. Dharmaraj, D. (2022). Convolutional neural networks (CNN) — Architecture explained. Medium.
36. Dong, Z., Wei, J., Chen, X., & Zheng, P. (2020). Face detection in security monitoring based on artificial intelligence video retrieval technology. IEEE Access, 8, 54166–54173.
37. Du, M., Pentyala, S., Li, Y., & Hu, X. (2020). Towards generalizable deepfake detection with locality-aware autoencoder. Proceedings of the 29th ACM International Conference on Information and Knowledge Management (CIKM '20).
38. Durall, R., Keuper, M., Pfreundt, F., & Keuper, J. (2019). Unmasking deepfakes with simple features. arXiv. https://arxiv.org/abs/1911.00686
39. El-Gayar, M. M., Abouhawwash, M., Askar, S. S., & Sweidan, S. (2024). A novel approach for detecting deep fake videos using graph neural network. Journal of Big Data, 11(1), 1–17.
40. Elpeltagy, M., Ismail, A., Zaki, M. S., & Eldahshan, K. (2023). A novel smart deepfake video detection system. International Journal of Advanced Computer Science and Applications, 14(1), 115–122.
41. Feinland, J., Barkovitch, J., Lee, D., Kaforey, A., & Ciftci, U. A. (2022). Poker bluff detection dataset based on facial analysis. In F. Falchi, A. Messina, G. Amato, & N. Vadicamo (Eds.), Lecture notes in computer science (13233, pp. 466–476).
42. Frank, J., Eisenhofer, T., Schönherr, L., Fischer, A., Kolossa, D., & Holz, T. (2020). Leveraging frequency analysis for deep fake image recognition. Proceedings of the 37th International Conference on Machine Learning (ICML 2020).
43. Fukushima, K. (1987a). Neural network model for selective attention. Unpublished manuscript.
44. Fukushima, K. (1987b). Neural network model for selective attention in visual pattern recognition and associative recall. Applied Optics, 26(23), 4985–4992.
45. Fukushima, K. (1989). Modeling visual systems for visual pattern recognition. Journal of the Japan Society for Precision Engineering, 55(4), 638–644.
46. Giudice, O., Guarnera, L., & Battiato, S. (2021). Fighting deepfakes by detecting GAN DCT anomalies. Journal of Imaging, 7(8), 128.
47. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial networks. In Advances in Neural Information Processing Systems (NeurIPS 2014). https://doi.org/10.1145/3422622
48. Goswami, G., Bhardwaj, R., Singh, R., & Vatsa, M. (2014). MDLFace: Memorability augmented deep learning for video face recognition. IJCB 2014 - 2014 IEEE/IAPR International Joint Conference on Biometrics. https://doi.org/10.1109/BTAS.2014.6996299
49. Guarnera, L., Giudice, O., & Battiato, S. (2020). Deepfake detection by analyzing convolutional traces. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2841–2850. https://doi.org/10.1109/CVPRW50498.2020.00341
50. Guera, D., & Delp, E. J. (2018). Deepfake video detection using recurrent neural networks. Proceedings of AVSS 2018 - 2018 15th IEEE International Conference on Advanced Video and Signal-Based Surveillance. https://doi.org/10.1109/AVSS.2018.8639163

51. Guo, J., Zhao, Y., & Wang, H. (2023). Generalized spoof detection and incremental algorithm recognition for voice spoofing. Applied Sciences (Switzerland), 13(13), 7773. https://doi.org/10.3390/app13137773
52. Gurucharan, M. (2020). Basic CNN architecture: Explaining 5 layers of convolutional neural network. UpGrad Knowledge Base.
53. Gurucharan, M. K. (2022). Basic CNN architecture: Explaining 5 layers of convolutional neural network. UpGrad Blog. https://www.upgrad.com/blog/basic-cnn-architecture/
54. Han, W., Zheng, C., Zhang, R., Guo, J., Yang, Q., & Shao, J. (2021). Modular neural network via exploring category hierarchy. Information Sciences, 569 204–215. https://doi.org/10.1016/j.ins.2021.05.032
55. Hao, H., Bartusiak, E. R., Güera, D., Mas Montserrat, D., Baireddy, S., Xiang, Z., Yarlagadda, S. K., Shao, R., Horváth, J., Yang, J., Zhu, F., & Delp, E. J. (2022). Deepfake detection using multiple data modalities. In Advances in Computer Vision and Pattern Recognition (pp. 205–220). https://doi.org/10.1007/978-3-030-87664-7_11
56. He, M., Meng, Q., & Zhang, S. (2019). Collaborative additional variational autoencoder for top-N recommender systems. IEEE Access, 7, 117100–117110. https://doi.org/10.1109/ACCESS.2018.2890293
57. He, Y., Gan, B., Chen, S., Zhou, Y., Yin, G., Song, L., Sheng, L., Shao, J., & Liu, Z. (2021). ForgeryNet: A versatile benchmark for comprehensive forgery analysis. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2021), 7665–7674.
58. Heo, Y. J., Yeo, W. H., & Kim, B. G. (2023). Deepfake detection algorithm based on improved vision transformer. Applied Intelligence, 53(7), 8391–8406.
59. Hidasi, B., Karatzoglou, A., Baltrunas, L., & Tikk, D. (2016). Session-based recommendations with recurrent neural networks. 4th International Conference on Learning Representations (ICLR 2016) - Conference Track Proceedings.
60. Hsu, C. C., Lee, C. Y., & Zhuang, Y. X. (2018). Learning to detect fake face images in the wild. Proceedings - 2018 International Symposium on Computer, Consumer and Control (IS3C 2018), 388–391.
61. Hu, J., Liao, X., Liang, J., Zhou, W., & Qin, Z. (2022). FInfer: Frame inference-based deepfake detection for high-visual-quality videos. Proceedings of the AAAI Conference on Artificial Intelligence, 36(1), 1333–1341.
62. Huang, L., Xu, S., Liu, K., Yang, R., & Wu, L. (2021). A fuzzy radial basis adaptive inference network and its application to time-varying signal classification. Computational Intelligence and Neuroscience, 2021, Article 5528291. https://doi.org/10.1155/2021/5528291
63. Ilbeigipour, S., Albadvi, A., & Akhondzadeh Noughabi, E. (2022). Cluster-based analysis of COVID-19 cases using self-organizing map neural network and K-means methods to improve medical decision-making. Informatics in Medicine Unlocked, 32, Article 101005. https://doi.org/10.1016/j.imu.2022.101005
64. Ilyas, H., Irtaza, A., Javed, A., & Malik, K. M. (2022). Deepfakes examiner: An end-to-end deep learning model for deepfakes videos detection. 2022 16th International Conference on Open-Source Systems and Technologies (ICOSST 2022) - Proceedings, 1–6. https://doi.org/10.1109/ICOSST57195.2022.10016871
65. Ismail, A., Elpeltagy, M., Zaki, M. S., & Eldahshan, K. (2021). A new deep learning-based methodology for video deepfake detection using XGBoost. Sensors, 21(16), Article 5413. https://doi.org/10.3390/s21165413
66. Ismail, A., Elpeltagy, M., Zaki, M. S., & Eldahshan, K. (2022). An integrated spatiotemporal-based methodology for deepfake detection. Neural Computing and Applications, 34(24), 21269–21284. https://doi.org/10.1007/s00521-022-07633-3
67. Ivanov, N. S., Arzhskov, A. V., & Ivanenko, V. G. (2020). Combining deep learning and super-resolution algorithms for deep fake detection. 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 53–57. https://doi.org/10.1109/EIConRus49466.2020.9039498.
68. Jaiswal, G. (2021). Hybrid recurrent deep learning model for deepfake video detection. 2021 IEEE 8th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON 2021), 1–6. https:// doi.org/10.1109/UPCON 52273.2021. .9667632

69. Jalui, K., Jagtap, A., Sharma, S., Mary, G., Fernandes, R., & Kolhekar, M. (2022). Synthetic content detection in deepfake video using deep learning. 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), 1–6.
70. Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. Electronic Markets, 31(3), 685–695. https://doi.org/10.1007/s12525-021-00475-2
71. Jeong, Y., Kim, D., Ro, Y., & Choi, J. (2022). FrePGAN: Robust deepfake detection using frequency-level perturbations. Proceedings of the AAAI Conference on Artificial Intelligence, 36(1), 1233–1241. https://doi.org/10.1609/aaai.v36i1.19990
72. Kandasamy, V., Hubálovský, Š., & Trojovský, P. (2022). Deep fake detection using a sparse autoencoder with a graph capsule dual graph CNN. PeerJ Computer Science, 8, e953. https://doi.org/10.7717/peerj-cs.953
73. Kanwal, S., Tehsin, S., & Saif, S. (2022). Exposing AI generated deepfake images using Siamese network with triplet loss. Computing and Informatics, 41(6), 1346–1366. https://doi.org/10.31577/cai_2022_6_1541
74. Karras, T., Aila, T., Laine, S., & Lehtinen, J. (2018). Progressive growing of GANs for improved quality, stability, and variation. 6th International Conference on Learning Representations (ICLR 2018) - Conference Track Proceedings. https://arxiv.org/abs/1710.10196
75. Kaur, J., & Kaur, P. (2018). A review: Artificial neural network. International Journal of Current Engineering and Technology, 8(4), 1258–1263. https://doi.org/10.14741/ijcet/v.8.4.2
76. Khalid, F., Akbar, M. H., & Gul, S. (2023). SWYNT: Swin Y-Net transformers for deepfake detection. 2023 International Conference on Robotics and Automation in Industry (ICRAI), 1–6. https://doi.org/10.1109/ICRAI57502.2023.10089585
77. Khalid, H., & Woo, S. S. (2020). OC-FakeDect: Classifying deepfakes using one-class variational autoencoder. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW 2020), 2880–2886. https://doi.org/10.1109/CVPRW50498.2020.00333
78. Khan, S. A., & Dang-Nguyen, D. T. (2022). Hybrid transformer network for deepfake detection. ACM International Conference Proceeding Series, 164–169. https://doi. org/10.1145/ 3549555.3549588
79. Khedkar, A., Peshkar, A., Nagdive, A., Gaikwad, M., & Baudha, S. (2022). Exploiting spatiotemporal inconsistencies to detect deepfake videos in the wild. International Conference on Emerging Trends in Engineering and Technology, ICETET, 2022-April. https://doi.org/10.1109/ICETET-SIP-2254415.2022.9791719.
80. Khodabakhsh, A., & Loiselle, H. (2020). Action-Independent Generalized Behavioral Identity Descriptors for Look-alike Recognition in Videos. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI), P-306.
81. Khodabakhsh, A., Ramachandra, R., Raja, K., Wasnik, P., & Busch, C. (2018). Fake Face Detection Methods: Can They Be Generalized? 2018 International Conference of the Biometrics Special Interest Group, BIOSIG 2018. https://doi.org/10.23919/BIOSIG.2018.8553251.
82. Khormali, A., & Yuan, J.-S. (2022). DFDT: An End-to-End DeepFake Detection Framework Using Vision Transformer. Applied Sciences. https://api.semanticscholar.org /CorpusID:247495859.
83. Ki Chan, C. C., Kumar, V., Delaney, S., & Gochoo, M. (2020). Combating Deepfakes: Multi-LSTM and Blockchain as Proof of Authenticity for Digital Media. 2020 IEEE / ITU International Conference on Artificial Intelligence for Good, AI4G 2020. https://doi.org/10.1109/AI4G50087.2020.9311067.
84. Kim, P. (2017). MATLAB Deep Learning. In MATLAB Deep Learning. https://doi.org/10.1007/978-1-4842-2845-6.
85. Kohonen, T. (1998). The self-organizing map. Neurocomputing, 21(1–3). https://doi.org/10.1016/ S0925-2312(98)00030-7.
86. Korshunov, P., & Marcel, S. (2019). Vulnerability assessment and detection of Deepfake videos. 2019 International Conference on Biometrics, ICB 2019. https://doi.org/10. 1109/ICB45273.2019.8987375.
87. Kosarkar, U., Sarkarkar, G., & Gedam, S. (2023). Revealing and Classification of Deepfakes Kuang, L., Wang, Y., Hang, T., Chen, B., & Zhao, G. (2022). A dual-branch neural network for DeepFake video detection by detecting spatial and temporal inconsistencies. Multimedia Tools and Applications, 81(29), 41879–41900. https://doi.org/10.1007/s11042-021-11539-y
88. Kumar, A., & Bhavsar, A. (2020). Detecting Deepfakes with metric learning. 2020 8th International Workshop on Biometrics and Forensics (IWBF), 1–6. https://doi.org/10.1109/IWBF49977.2020.9107962

89. LeCun, Y., Boser, B., Denker, J. S., Henderson, D., Howard, R. E., Hubbard, W., & Jackel, L. D. (1989a). Backpropagation applied to digit recognition. Neural Computation, 1(4), 541–551.
90. LeCun, Y., Boser, B., Denker, J. S., Henderson, D., Howard, R. E., Hubbard, W., & Jackel, L. D. (1989b). Backpropagation applied to handwritten zip code recognition. Neural Computation, 1(4), 541–551. https://doi.org/10.1162/neco.1989.1.4.541
91. Lee, U., & Lee, I. (2022). Efficient sampling-based inverse reliability analysis combining Monte Carlo simulation (MCS) and feedforward neural network (FNN). Structural and Multidisciplinary Optimization, 65(1), 181–198. https://doi.org/10.1007/s00158-021-03144-2
92. Li, Q., Gao, M., Zhang, G., & Zhai, W. (2023). Defending Deepfakes by saliency-aware attack. IEEE Transactions on Computational Social Systems. https://doi.org/10.1109/TCSS.2023.3271121
93. Li, Y., & Lyu, S. (2019). Exposing DeepFake videos by detecting face warping artifacts. [Manuscript in preparation].
94. Li, Y., Chang, M. C., & Lyu, S. (2018). In Ictu Oculi: Exposing AI-created fake videos by detecting eye blinking. 10th IEEE International Workshop on Information Forensics and Security (WIFS 2018), 1–7. https://doi.org/10.1109/WIFS.2018.8630787
95. Li, Y., Yang, X., Sun, P., Qi, H., & Lyu, S. (2019a). Celeb-DF: A large-scale challenging dataset for DeepFake forensics. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 3204–3213. https://doi.org/10.1109/CVPR42600.2020.00327
96. Li, Y., Yang, X., Sun, P., Qi, H., & Lyu, S. (2019b). Celeb-DF: A large-scale challenging dataset for DeepFake forensics. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 3204–3213. https://doi.org/10.1109/CVPR42600.2020.00327
97. Liang, D., Krishnan, R. G., Hoffman, M. D., & Jebara, T. (2018). Variational autoencoders for collaborative filtering. Proceedings of the 2018 World Wide Web Conference (WWW 2018), 689–698. https://doi.org/10.1145/3178876.3186150
98. Lin, H., Huang, W., Luo, W., & Lu, W. (2023). DeepFake detection with multi-scale convolution and vision transformer. Digital Signal Processing: A Review Journal, 134, Article 103895. https://doi.org/10.1016/j.dsp.2022.103895
99. Lin, X., Yang, X., & Li, Y. (2019). A deep clustering algorithm based on Gaussian mixture model. Journal of Physics: Conference Series, 1302(3), 032012. https://doi.org/10.1088/1742-6596/1302/3/032012
100. Liu, C., Li, J., Duan, J., & Huang, H. (2022). Video forgery detection using spatio-temporal dual transformer. Proceedings of the 2022 11th International Conference on Computing and Pattern Recognition, Article 3581847. https://doi.org/10.1145/3581807.3581847
101. Liu, P. (2021). Automated Deepfake detection. arXiv Preprint. https://arxiv.org/abs/2106.10705
102. Liu, Y., Zhang, Y., & Liu, W. (2022). A novel face forgery detection method based on augmented dual-stream networks. ACM International Conference Proceeding Series. https://doi.org/10.1145/3573942.357403
103. Liu, Z., Luo, P., Wang, X., & Tang, X. (2015). Deep learning face attributes in the wild. 2015 IEEE International Conference on Computer Vision (ICCV), 3730–3738. https://doi.org/10.1109/ICCV.2015.425
104. Mahmud, B. U., & Sharmin, A. (2021). Deep insights of DeepFake technology: A review. arXiv Preprint. https://arxiv.org/abs/2105.00192
105. Majeed, M. A., Shafri, H. Z. M., Zulkafli, Z., & Wayayok, A. (2023). A deep learning approach for dengue fever prediction in Malaysia using LSTM with spatial attention. International Journal of Environmental Research and Public Health, 20(5), Article 4130. https://doi.org/10.3390/ijerph20054130
106. Maksutov, A. A., Morozov, V. O., Lavrenov, A. A., & Smirnov, A. S. (2020). Methods of DeepFake detection based on machine learning. 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 1923–1927. https://doi.org/10.1109/EIConRus49466.2020.9039057
107. Malolan, B., Parekh, A., & Kazi, F. (2020). Explainable DeepFake detection using visual interpretability methods. 3rd International Conference on Information and Computer Technologies (ICICT 2020), 225–229. https://doi.org/10.1109/ICICT50521.2020.00051

108. Masi, I., Killekar, A., Mascarenhas, R., Gurudatt, S. P., & AbdAlmageed, W. (2020). Two-branch recurrent network for isolating DeepFakes in videos. In European Conference on Computer Vision (ECCV 2020) (pp. 659–675). Springer. https://doi.org/10.1007/978-3-030-58571-6_39
109. Masih, D. R. A. J. D. R. J. (2023). Enhancing employee efficiency and performance in Industry 5.0 organizations through artificial intelligence integration. European Economic Letters (EEL), 13(4). https://doi.org/10.52783/eel.v13i4.589
110. Masood, M., Nawaz, M., Javed, A., Nazir, T., Mehmood, A., & Mahum, R. (2021). Classification of DeepFake videos using pre-trained convolutional neural networks. 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2 2021), 1–6. https://doi.org/10.1109/ICoDT252288.2021.9441519
111. Melin, P., Miramontes, I., & Prado-Arechiga, G. (2018). A hybrid model based on modular neural networks and fuzzy systems for classification of blood pressure and hypertension risk diagnosis. Expert Systems with Applications, 107. https://doi.org/10.1016/j.eswa.2018.04.023.
112. Miao, Y., Dong, H., Al Jaam, J. M., & El Saddik, A. (2019). A deep learning system for recognizing facial expression in real-time. ACM Transactions on Multimedia Computing, Communications and Applications, 15(2). https://doi.org/10.1145/3311747
113. Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. ACM Computing Surveys (CSUR), 54(1), 1–41.
114. Mirza, M., & Osindero, S. (2014). Conditional Generative Adversarial Nets.
115. Mitra, A., Mohanty, S. P., Corcoran, P., & Kougianos, E. (2020). A Novel Machine Learning based Method for Deepfake Video Detection in Social Media. Proceedings - 2020 6th IEEE International Symposium on Smart Electronic Systems, ISES 2020. https://doi.org/10.1109/iSES50453.2020.00031
116. Mittal, H., Saraswat, M., Bansal, J. C., & Nagar, A. (2020). Fake-Face Image Classification using Improved Quantum-Inspired Evolutionary-based Feature Selection Method. 2020 IEEE Symposium Series on Computational Intelligence, SSCI 2020. https://doi.org/10.1109/SSCI47803.2020.9308337
117. Mo, H., Chen, B., & Luo, W. (2018). Fake faces identification via convolutional neural network. IH and MMSec 2018 - Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security. https://doi.org/10.1145/3206004.3206009
118. Montserrat, D. M., Hao, H., Yarlagadda, S., Baireddy, S., Shao, R., Horváth, J., Bartusiak, E. R., Yang, J., Guera, D., Zhu, F., & Delp, E. (2020). Deepfakes Detection with Automatic Face Weighting. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), null, 2851–2859. https://doi.org/10.1109/CVPRW50498.2020.00342
119. Naik, N., Hameed, B. M. Z., Sooriyaperakasam, N., Vinayahalingam, S., Patil, V., Smriti, K., Saxena, J., Shah, M., Ibrahim, S., Singh, A., Karimi, H., Naganathan, K., Shetty, D. K., Rai, B. P., Chlosta, P., & Somani, B. K. (2022). Transforming healthcare through a digital revolution: A review of digital healthcare technologies and solutions. In Frontiers in Digital Health (Vol. 4). https://doi.org/10.3389/fdgth.2022.919985
120. Park, J., Lee, W., & Huh, K. Y. (2022). Model order reduction by radial basis function network for sparse reconstruction of an industrial natural gas boiler. Case Studies in Thermal Engineering, 37. https://doi.org/10.1016/j.csite.2022.102288
121. Passos, L. A., Jodas, D., Costa, K. A. P., Souza Júnior, L. A., Rodrigues, D., Del Ser, J., Camacho, D., & Papa, J. P. (2024). A review of deep learning-based approaches for deepfake content detection. Expert Systems. https://doi.org/10.1111/exsy.13570
122. Patel Nimitt, Jethwa Niket, Mali Chirag, and Deone Jyoti. (2022). Deepfake Video Detection using Neural Networks. ITM Web Conf., 44, 3024. https://doi.org/10.1051/itmconf/20224403024
123. Polson, N. G., & Sokolov, V. O. (2018). Deep Learning - Nature Review. Nature, 521(7553).
124. Preeti, Kumar, M., & Sharma, H. K. (2022). A GAN-Based Model of Deepfake Detection in Social Media. Procedia Computer Science, 218. https://doi.org/10.1016/j.procs.2023.01.191
125. Pu, W., Hu, J., Wang, X., Li, Y., Hu, S., Zhu, B., Song, R., Song, Q., Wu, X., & Lyu, S. (2022). Learning a deep dual-level network for robust DeepFake detection. Pattern Recognition, 130. https://doi.org/10.1016/j.patcog.2022.108832

126. Qing, L., Mengqiu, Y., Zhaoping, L., & Jiancheng, L. (2021). Research on video automatic feature extraction technology based on deep neural network. Proceedings of IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers, IPEC 2021. https://doi.org/10.1109/IPEC51340.2021.9421272
127. Quadrana, M., Karatzoglou, A., Hidasi, B., & Cremonesi, P. (2017). Personalizing Session-Based Recommendations with Hierarchical Recurrent Neural Networks. Proceedings of the Eleventh ACM Conference on Recommender Systems, 130–137. https://doi.org/10.1145/3109859.3109896
128. Qurat-Ul-Ain, Nida, N., Irtaza, A., & Ilyas, N. (2021). Forged Face Detection using ELA and Deep Learning Techniques. Proceedings of 18th International Bhurban Conference on Applied Sciences and Technologies, IBCAST 2021. https://doi.org/10.1109/IBCAST51254.2021.9393234
129. Rafique, R., Nawaz, M., Kibriya, H., & Masood, M. (2021). DeepFake Detection Using Error Level Analysis and Deep Learning. Proceedings - 2021 IEEE 4th International Conference on Computing and Information Sciences, ICCIS 2021. https://doi.org/10.1109/ICCIS54243.2021.9676375
130. Rajalaxmi, R. R., Sudharsana, P. P., Rithani, A. M., Preethika, S., Dhivakar, P., & Gothai, E. (2023). Deepfake detection using Inception-ResNet-V2 network. Proceedings of the 7th International Conference on Computing Methodologies and Communication (ICCMC 2023). https://doi.org/10.1109/ICCMC56507.2023.10083584
131. Rani, R., Kumar, T., & Sah, M. P. (2022). A review on deepfake media detection. Lecture Notes in Networks and Systems, 461. https://doi.org/10.1007/978-981-19-2130-8_28
132. Ranjan, P., Patil, S., & Kazi, F. (2020). Improved generalizability of deepfakes detection using transfer learning-based CNN framework. In 2020 3rd International Conference on Information and Computer Technologies (ICICT) (pp. 86–90). https://doi.org/10.1109/ICICT50521.2020.00021
133. Rebello, L., Tuscano, L., Shah, Y., Solomon, A., & Shrivastava, V. (2023). Detection of deepfake video using deep learning and MesoNet. Proceedings of the 8th International Conference on Communication and Electronics Systems (ICCES 2023). https://doi.org/10.1109/ICCES57224.2023.10192854
134. Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2018). FaceForensics: A large-scale video dataset for forgery detection in human faces. ArXiv preprint arXiv:1803.09179.
135. Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2019). FaceForensics++: Learning to detect manipulated facial images. In Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV 2019) (pp. 1–10). https://doi.org/10.1109/ICCV.2019.00009
136. S, L., & Sooda, K. (2022). Deepfake detection through key video frame extraction using GAN. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 859–863). https://doi.org/10.1109/ICACRS55517.2022.10029095
137. Saber, A. M., Hassan, M. T., Mohamed, M. S., ElHusseiny, R., Eltaher, Y. M., Abdelrazek, M., & Omar, Y. M. K. (2022). Deepfake video detection. In 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) (pp. 425–431).
138. Saif, S., Tehseen, S., Ali, S. S., Kausar, S., & Jameel, A. (2022). Generalized deepfake video detection through time-distribution and metric learning. IT Professional, 24(2). https://doi.org/10.1109/MITP.2022.3168351
139. Saraswathi, R. V., Gadwalkar, M., Midhun, S. S., Goud, G. N., & Vidavaluri, A. (2022). Detection of synthesized videos using CNN. Proceedings of the International Conference on Augmented Intelligence and Sustainable Systems (ICAISS 2022). https://doi.org/10.1109/ICAISS55157.2022.10011073
140. Saraswathi, R. V., Gadwalkar, M., Midhun, S. S., Goud, G. N., & Vidavaluri, A. (2022). Detection of Synthesized Videos using CNN. Proceedings - International Conference on Augmented Intelligence and Sustainable Systems, ICAISS 2022. https://doi.org/10.1109/ICAISS55157.2022.10011073
141. Sarker, I. H. (2021). Deep learning: A comprehensive overview on techniques, taxonomy, applications and research directions. SN Computer Science, 2(6). https://doi.org/10.1007/s42979-021-00815-1
142. Saxena, A., Yadav, D., Gupta, M., Phulre, S., Arjariya, T., Jaiswal, V., & Bhujade, R. K. (2023). Detecting deepfakes: A novel framework employing XceptionNet-based convolutional neural networks. Traitement Du Signal, 40(3). https://doi.org/10.18280/ts.400301
143. Şengür, A., Akhtar, Z., Akbulut, Y., Ekici, S., & Budak, Ü. (2019). Deep feature extraction for face liveness detection. 2018 International Conference on Artificial Intelligence and Data Processing, IDAP 2018. https://doi.org/10.1109/IDAP.2018.8620804

144. Sherstinsky, A. (2020). Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. Physica D: Nonlinear Phenomena, 404. https://doi.org/10.1016/j.physd.2019.132306
145. Shiohara, K., & Yamasaki, T. (2022a). Detecting deepfakes with self-blended images. In 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 18699–18708). https://doi.org/10.1109/CVPR52688.2022.01816
146. Shiohara, K., & Yamasaki, T. (2022b). Detecting deepfakes with self-blended images. In 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 18699–18708). https://doi.org/10.1109/CVPR52688.2022.01816
147. Shobha Rani, R. B., Kumar Pareek, P., Bharathi, S., & Geetha, G. (2023). Deepfake video detection system using deep neural networks. In 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS 2023) (pp. 1–6). https://doi.org/10.1109/ICICACS57338.2023.10099618
148. Sille, R., Choudhury, T., Sharma, A., Chauhan, P., Tomar, R., & Sharma, D. (2023). A novel generative adversarial network-based approach for automated brain tumour segmentation. Medicina, 59, 119. https://doi.org/10.3390/medicina59010119
149. Sohn, I. (2021). Deep belief network based intrusion detection techniques: A survey. Expert Systems with Applications, 167. https://doi.org/10.1016/j.eswa.2020.114170
150. Song, H., Kim, H., & Lee, H. (2022). Countering deepfake threats to corporate reputation: The roles of media, stakeholders, and crisis communication strategies. Corporate Communications: An International Journal, 28(1), 18–34. https://doi.org/10.1108/CCIJ-07-2021-0083
151. Song, Y., Liu, Y., Wang, M., & Tan, T. (2023). Deepfake detection using attention-based fusion and contrastive learning. Neurocomputing, 523, 111–122. https://doi.org/10.1016/j.neucom.2022.10.018
152. Srinivasan, R., Rajendran, P., & Uma, G. V. (2021). A novel framework for deepfake detection using optimal feature selection. Journal of Ambient Intelligence and Humanized Computing, 12, 11271–11281. https://doi.org/10.1007/s12652-021-02979-2
153. Sundararaj, V., Chithra, N., Vinayakumar, R., & Soman, K. P. (2022). DeepFake detection: A new benchmark dataset and method for face and voice forgery detection using a capsule network. Applied Soft Computing, 118, 108439. https://doi.org/10.1016/j.asoc.2022.108439
154. Thakur, M., & Maheshkar, S. (2023). Deepfake menace and regulations: The laws of United States and India. International Journal of Law and Management, 65(1), 77–89. https://doi.org/10.1108/IJLMA-08-2022-0200
155. Tolosana, R., Romero-Tapiador, S., & Fierrez, J. (2023). Deepfakes evolution and detection: Recent advances and open challenges. IEEE Transactions on Pattern Analysis and Machine Intelligence, 45(1), 552–569. https://doi.org/10.1109/TPAMI.2022.3168322
156. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. Information Fusion, 64, 131–148. https://doi.org/10.1016/j.inffus.2020.07.007
157. Vakharia, M. P., & Kumar, P. R. (2021). A comprehensive study of generative adversarial networks and their applications. Procedia Computer Science, 192, 1705–1714. https://doi.org/10.1016/j.procs.2021.08.175
158. Varol, C., Gürkan, H., & Çetinoğlu, E. K. (2021). Deepfake video detection using frame transition consistency. In 2021 29th Signal Processing and Communications Applications Conference (SIU) (pp. 1–4). https://doi.org/10.1109/SIU53274.2021.9477739
159. Verdoliva, L. (2020). Media forensics and deepfakes: An overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910–932. https://doi.org/10.1109/JSTSP.2020.2998603
160. Verdoliva, L., & Gragnaniello, D. (2023). Recent advances in deepfake detection: Challenges, opportunities and future directions. Information Fusion, 91, 190–209. https://doi.org/10.1016/j.inffus.2023.01.012
161. Wang, S. Y., Wang, O., Zhang, R., Owens, A., & Efros, A. A. (2020). CNN-generated images are surprisingly easy to spot... for now. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 8695–8704). https://doi.org/10.1109/CVPR42600.2020.00872
162. Wang, X., Peng, W., & Wang, Y. (2021). A survey on deepfake detection techniques. Computational Intelligence and Neuroscience, 2021, Article ID 5573475. https://doi.org/10.1155/2021/5573475

163. Westerlund, M. (2019). The emergence of deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52. https://doi.org/10.22215/timreview/1282
164. Yang, X., Li, Y., & Lyu, S. (2019). Exposing deep fakes using inconsistent head poses. In ICASSP 2019 – 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 8261–8265). https://doi.org/10.1109/ICASSP.2019.8683164
165. Yousuf, M. A., & Qureshi, M. A. (2021). A comprehensive review of deepfake detection techniques: State-of-the-art and future directions. Multimedia Tools and Applications, 80, 29333–29363. https://doi.org/10.1007/s11042-021-11100-1
166. Zhang, H., Liu, H., Wang, X., & Zhang, Y. (2022). Face X-ray for more general face forgery detection. IEEE Transactions on Information Forensics and Security, 17, 624–639. https://doi.org/10.1109/TIFS.2021.3119237
167. Zhang, Y., Wang, X., & Qian, Y. (2023). A novel multimodal framework for deepfake video detection. Neurocomputing, 519, 372–384. https://doi.org/10.1016/j.neucom.2022.09.042
168. Zhao, H., Liu, Z., Zhou, Y., & Shi, J. (2021). Multi-scale attention-based deepfake detection. In Proceedings of the AAAI Conference on Artificial Intelligence, 35(4), 3563–3571. https://doi.org/10.1609/aaai.v35i4.16498
169. Zhou, P., Han, X., Morariu, V. I., & Davis, L. S. (2018). Two-stream neural networks for tampered face detection. In 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (pp. 1831–1839). https://doi.org /10.1109/CV PRW.2017.228.