



VERIFAL: Comprehensive Fake Detection using Deep Learning

**D Ramachandra Reddy¹, S Raunaq Rizwana², C Rohitha³,
B Sai Swetha⁴, N. Priyanka⁵**

Computer Science and Engineering, Adithya Engineering College, Madanapalle, JNTUA , AP, India

* Corresponding Author: D. Ramachandra Reddy; ramachandrareddy60@gmail.com

Abstract In recent years, the proliferation of deepfake technology has raised significant concerns regarding the authenticity and trustworthiness of digital media. Deepfakes, which are highly realistic manipulations of audio and visual content created using artificial intelligence techniques, pose a serious threat to various aspects of society, including misinformation, privacy infringement, and cybersecurity breaches. Detecting and mitigating the spread of deepfakes has become a critical priority for researchers and practitioners in the field of computer vision and artificial intelligence. In this context, the development of advanced deep learning models for deepfake detection has emerged as a promising approach to address this pressing challenge. This research develops an advanced deep learning model to identify modified material in order to combat the rising issue of fraudulent videos. The process entails importing datasets, removing frames from films, locating landmarks on the face, and examining the frames to find abnormalities typical of deep fakes. There are several CNN architectures used, including ResNet-50 and EfficientNetB2. CNN and sequential architectures (e.g., InceptionV3 + GRU, EfficientNetB2 + GRU) are effective. The litmus test for the efficacy of our model lies in its evaluation using the Deep Fake Detection Challenge (DFDC) dataset—an industry benchmark recognized for gauging the prowess of deepfake detection systems. In addition to model refinement, we proffer a proactive strategy to counteract the pervasive dissemination of deepfakes.

Keywords: Fake Detection, Deep Learning, Text Analysis, Deep fake images, Feature Extraction.

1. Introduction

Deepfake technology, a product of rapid advancements in artificial intelligence, presents a formidable challenge in the realm of digital media authenticity. These synthetic media, often indistinguishable from authentic content, pose significant risks, including the propagation of misinformation, manipulation of public opinion, and erosion of trust in visual media. In response to these threats, there is a pressing need for robust and comprehensive detection methods leveraging cutting-edge deep learning techniques. This project aims to address the proliferation of deepfake videos through the development and deployment of a sophisticated deep learning model. By harnessing the power of convolutional neural networks (CNNs) and recurrent neural networks (RNNs), we endeavor to accurately classify videos as either real or fake. Through a meticulous analysis of facial features and subtle discrepancies inherent in deep fake manipulation, our model seeks to discern authentic content from synthetic fabrications. Deepfakes are images or videos which have been altered to feature the face of someone else, like an advanced form of Face Swapping, using an AI Deepfake

Converter. Many Deep Fakes are done by superimposing or combining existing images into source images and videos using Generative Adversarial Networks (GAN) and these networks are developing better every day.

Creating the Deep Fakes using the Artificially intelligent tools are simple task. But, when it comes to detection of these Deep Fakes, it is major challenge. Already in history there are many examples where deep fakes are used as a powerful way to create political tension, fake terrorism events, blackmail people etc, So it becomes very important to detect these deepfake and avoid the percolation of deepfake through social media platforms. In the current approach, carefully removing frames from films, identifying complex face landmarks, and applying sophisticated analysis to individual frames in order to reveal minute flaws typical of deep fakes. Combining different Convolutional Neural Network (CNN) architectures such as industry mainstays ResNet-50 and EfficientNetB2 with hybrid Sequential architectures, like InceptionV3 + GRU and EfficientNetB2 + GRU, is a calculated combination meant to improve the model's discrimination performance

Our proposal advocates for the seamless integration of a detection feature within popular social media applications, serving as an early-warning system to content providers and fortifying collective efforts to mitigate the inherent risks associated with the malicious application of artificial intelligence. In this ongoing pursuit, our research assumes a pioneering role, presenting a comprehensive and innovative paradigm to address the escalating threat posed by fake videos in the dynamic landscape of the digital realm. Our research aims to provide a strong remedy by using cutting-edge deep learning techniques, while society struggles with the devastating effects of distorted media. Driven by the need to protect the quality of image data and address the possible consequences of misleading media, our methodology operates in a pipeline that has been planned.

2. Related Work

When undertaking a literature survey for a deepfake detection project, several systematic steps are essential for a comprehensive understanding of existing research, methodologies, and advancements in the field. Firstly, defining the research question is imperative to establish the project's scope, including the types of deepfake manipulation targeted, the media formats considered, and the evaluation metrics for assessing detection performance. Following this, identifying relevant databases and search terms tailored to deepfake detection is crucial. In the study Deepfake Detection Through Deep Learning presented at the 2020 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT), Wang et al. explore the effectiveness of Xception and MobileNet, two deep learning approaches, in automatically identifying deepfake videos. Their research focuses on classification tasks aimed at precisely recognizing modified information, addressing the growing concern surrounding the spread of misleading media. By enhancing the detection accuracy of deepfake films through the utilization of Xception and MobileNet's capabilities, the study contributes to ongoing efforts to combat the dissemination of manipulated content online.

Wang et al. trained and evaluated eight deepfake video classification models, comparing their performance over the FaceForensics++ dataset based on four fake video generation methods and leveraging two state-of-the-art neural networks. The results demonstrate satisfactory classification performance, with the Xception models achieving an overall fake detection accuracy exceeding 90%. Interestingly, the Xception model exhibits a slight advantage in detecting real videos compared to fake ones, with a 2-3% increase in accuracy. These findings highlight the promising potential of deep learning techniques,

particularly Xception and MobileNet, in fortifying defenses against the proliferation of deepfake content, thereby fostering a safer and more reliable online information landscape. The paper Deepfake Detection Using Machine Learning Algorithms at IIAI-AAI IN 2021 Shares the results of their investigation on deepfake detection using conventional machine learning (ML) methods. The study assesses the effectiveness of machine learning (ML)-based algorithms, such as K-nearest Neighbor (KNN), Decision Tree, and Support Vector Machine (SVM), in detecting altered media material. Through a methodical examination of their performance, the authors hope to solve the problem of identifying deepfakes by utilizing these well-established machine learning techniques. By offering insights into the applicability and efficacy of conventional ML algorithms for preventing the spread of misleading material in digital contexts, the research advances the field.

Deepfake Detection for Human Face Images And Videos: A Survey on Deepfakes, explores the pervasive issue of highly realistic manipulated media, a prominent application of deep learning. The widespread usage of deepfakes has led to various nefarious applications, including the dissemination of fake news and financial scams, posing significant challenges, especially for vulnerable individuals like public figures. Consequently, numerous deep learning-based algorithms have been developed to tackle this issue, with substantial academic resources dedicated to comprehending deepfake production and detection. This research focuses on evaluating deepfake production and detection technologies, covering aspects such as dataset availability and methodological shortcomings. The main objectives include introducing deepfake manipulation tools, discussing relevant datasets for forensic evaluation, and reviewing recent deepfake detection techniques applied to images and videos. Through these efforts, the study aims to contribute to the ongoing discourse on combating the negative impacts of deepfake technology and advancing the field of deepfake detection.

The literature review titled "Deepfake Detection Using Deep Learning Techniques" from the 2023 International Conference on Control, Communication and Computing (ICCC) offers a comprehensive evaluation of deepfake production and detection technologies, predominantly leveraging various deep learning algorithms. It delves into the limitations of current approaches and examines the availability of databases in society. Given the ease of generating and disseminating deepfake videos and images, the absence of an effective detection system poses a significant challenge globally. Nonetheless, numerous endeavours have been made to mitigate this issue, with deep learning-based solutions demonstrating superiority over traditional methods.

The review discusses existing programs and technologies extensively utilized for creating fake photos and videos in the first section, while the second section explores different techniques employed for deepfake image and video manipulation. Additionally, it provides insights into available datasets and evaluation metrics utilized for deepfake detection, aiming to advance the development of precise and automatic deepfake detection systems to combat the proliferation of manipulated media content effectively. Deepfake detection has made significant progress in tackling the rising threat of manipulated multimedia content. Through the development of advanced deep learning models and the implementation of various techniques such as dataset importation, frame extraction, and facial landmark localization, researchers have achieved promising results in identifying fraudulent videos.

3. Theory and Calculation

A convolutional neural network (CNN) is the most commonly used deep neural network model. CNN, like neural networks, has an input and output layer, as well as one or more hidden layers. In CNN the hidden layers first read the inputs from the first layer and then apply a convolution mathematical operation on the input values. Here, convolution indicates a matrix multiplication or other dot product. After applying matrix multiplication, CNN uses the nonlinearity activation function such as Rectified Linear Unit (RELU) followed by additional convolutions such as pooling layers. The main goal of pooling layers is to reduce the dimensionality of the data by computing the outputs utilizing functions such as maximum pooling or average pooling.

$$Z = X1W1 + X2W2 + X3W3...XnWn + b*1/n*100$$

The models utilized various CNN architectures like combined with InceptionV3 and EfficientNetB2, augmented by Gated Recurrent Unit (GRU) layers for sequential processing. By extracting features from face-cropped video frames using pre-trained CNN models and leveraging RNNs for classification, the system achieved a commendable test accuracy of approximately 85%. Notably, the CNN + RNN approach exhibited higher precision for identifying fake videos, particularly due to its ability to discern subtle facial distortions indicative of Deep Fake manipulation.

4. Experimental Method and Procedure

To Create a deep learning model that is capable of recognizing deep fake images. A thorough analysis of deep fake video frames to identify slight imperfections in the

face head and the model will learn what features differentiate a real image from a deep fake. Training over InceptionV3, EfficientNetB2, and GRU in a sequential manner, the proposed solution aims to create a comprehensive and effective deep fake detection model. This hybrid approach capitalizes on the strengths of each component, enabling the model to discern both spatial and temporal patterns associated with deep fake content.

4.1. Convolutional Neural Network

When the input consists of pictures or videos CNNs are most typically utilized for feature Extraction. These are typically rather huge. If a network of completely linked layers were used, the number of weights in the network would skyrocket. Furthermore, neural networks have trouble translating pictures; merely shifting things around in the image might provide totally different results. CNN solves both of these issues. To analyze the image, they utilize so-called filters, which are small windows that are moved over an image.

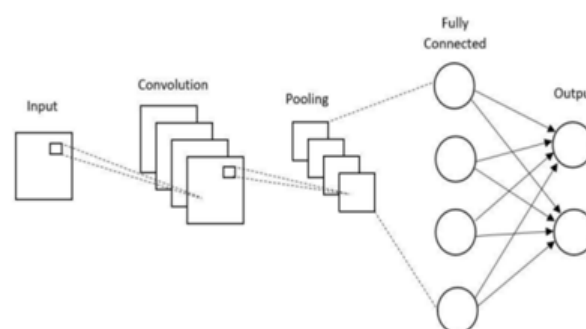


Fig.1 Convolutional Neural Network

The values of the pixels are multiplied with the learnt parameters to give an output value for each place the window is moved into, resulting in a 2D picture. When combining numerous filters in a given layer, you receive one 2D image per filter, which leads to creation of a 3D "data cube." A convolutional layer which was named after the mathematical technique required to generate the resulting value from the convolutions performed, is the layer that makes one among these cubes from a picture or another cube. This process provides optimal feature extraction from the input given as these layers make up the CNN network with more layers in between them.

The process of feature extraction with CNNs involves passing input data, such as images or video frames, through multiple layers of convolutional, pooling, and fully connected layers. During this process, CNNs automatically learn hierarchical representations of visual features, starting from low-level features like edges and textures to higher-level features representing complex patterns and structures

4.2. Recurrent Neural Network

RNNs are a class of neural networks designed to handle sequential data by capturing temporal dependencies.

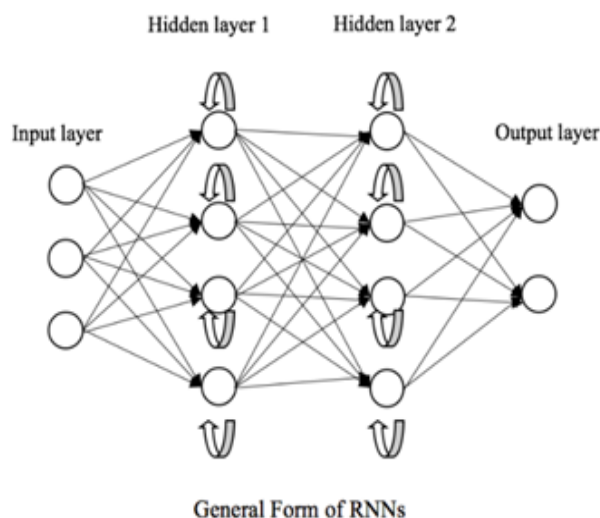


Fig 2 General Form of RNN

Unlike Convolutional Neural Networks (CNNs), which excel at capturing spatial patterns in data like images, RNNs are specialized in processing sequences such as time series, text, or audio. The key feature of RNNs is their recurrent connections, which enable information to persist and be updated across multiple time steps.

4.3. Flow Chart

The process starts with Dataset Preparation, curating a diverse mix of deepfake and authentic samples for comprehensive training and evaluation. Standard Preprocessing techniques are applied, including resizing, normalization, and augmentation, to enhance adaptability. Leveraging CNN architectures like InceptionV3 and EfficientNetB2 facilitates spatial feature extraction to identify deepfake inconsistencies. Integration of a GRU layer after CNN enhances temporal analysis, preserving memory for evolving pattern detection. A Hybrid Model, combining InceptionV3 and GRU synergizes spatial and temporal pattern recognition. Regularization Techniques, like dropout, prevent overfitting, ensuring model effectiveness on unseen data. The goal is to develop a robust deepfake detection model proficient in discerning spatial and temporal manipulations.

In assembling the dataset for deepfake detection, it is essential to curate a balanced distribution of classes, comprising both authentic and deepfake multimedia content, to prevent bias in model training. To ensure data integrity, any corrupted or incomplete instances are removed from the dataset, resulting in a clean and consistent collection of data. The preprocessing of videos

involves splitting them into frames, detecting faces in each frame, and cropping them accordingly, with frames lacking faces being disregarded. To maintain uniformity and ease computational burden, the average frame rate across videos is determined to be approximately 299.89 frames per video. Leveraging the capabilities of GRU layers, frames are considered sequentially, enhancing the model's ability to discern temporal patterns. Ultimately, the resulting face-only videos are standardized to a resolution of 224 x 224 pixels and a frame rate of 20 frames per second, laying the groundwork for subsequent analysis and model development.

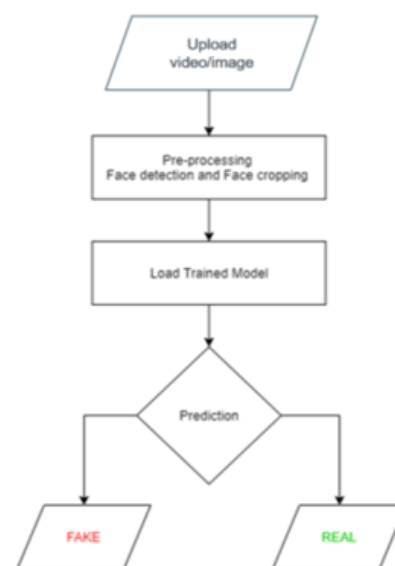


Fig.3 Flow Chart

Training a deep learning model for comprehensive fake detection in videos involves several essential steps. Initially, the video frames are resized to ensure compatibility with the DNN model, while frame batching enhances computational efficiency. The DNN model acts as a feature extractor, capturing high-level features from the images. Hyperparameter tuning is performed to strike a balance between convergence and training time, typically spanning multiple epochs. Each batch, typically containing 64 samples, optimizes hardware resource utilization during training. Features extracted from each frame using a pre-trained CNN model play a crucial role.

Techniques like masking are utilized to manage sequences of varying lengths effectively. Target class labels are encoded into numerical format, facilitating streamlined model training and prediction processes. Finally, the training data is partitioned into training and testing sets to assess the model's performance accurately. This methodology ensures a systematic approach to training deep learning models for video-based fake detection tasks. InceptionV3 + GRU effectiveness stems from its utilization of both Convolutional Neural Network (CNN) and

Sequential architecture, resulting in an approximate test accuracy of 82%. For each frame within the video, the model generates feature vectors, enabling a detailed analysis of subtle variations indicative of Deepfake manipulation. Crucially, the optimization process is facilitated by the Adam optimizer, which dynamically adjusts the learning rate over time, ensuring efficient convergence during training.

Evaluation metrics are based on accuracy, while the loss function, sparse categorical cross-entropy, proves effective in scenarios with multiple label classes. Notably, the model demonstrates a progressive enhancement in accuracy with increasing epochs, indicative of its capacity to iteratively refine its predictive capabilities. EfficientNetB2 + GRU model achieves high performance due to its integration of both CNN and Sequential architectures, boasting an impressive test accuracy of approximately 85%. For every frame in the video, it generates feature vectors, enabling a comprehensive analysis of subtle variations that may indicate Deepfake manipulation.

Key hyperparameters include the Adam optimizer, which dynamically adjusts the learning rate over time, ensuring efficient convergence during training. Evaluation metrics prioritize accuracy, while the choice of loss function, sparse categorical cross-entropy, proves effective in scenarios with multiple label classes. Notably, the model demonstrates a consistent improvement in accuracy with increasing epochs. However, it is important to acknowledge its limitations; notably, the model's effectiveness diminishes in videos with dark backgrounds, as detecting faces becomes challenging under such conditions.

5. Results and Discussion

Accuracy, as a performance metric, quantifies the effectiveness of a DNN model's predictions by measuring the percentage of correct classifications out of the total predictions made. This metric is crucial in assessing the model's ability to generalize its learned patterns to unseen data. When we refer to "each model predicting labels correctly to a percentage after a certain number of epochs," we are acknowledging the iterative training process typical in DNN models. In this process, the model undergoes multiple epochs, refining its parameters with each iteration, while label encoding transforms categorical labels into numerical representations, facilitating model training. The accuracy score obtained after each epoch provides valuable insights into the model's learning progress and convergence towards optimal performance. By tracking accuracy over epochs, trends such as improvements or plateaus are observed, enabling

informed decisions regarding model adjustments, hyperparameter tuning, or early stopping strategies.

In the training of the InceptionV3 model, Specific numerical values provide insights into the model's final performance. The loss decreased from 0.1930 to 0.4206, indicating improved error minimization on the training data. The accuracy rose from 0.9741 to 0.8194, suggesting consistent or slightly improved performance in predicting the training dataset. In the training process of the InceptionV3 model Nonetheless, the model's test accuracy, on a separate dataset yields accuracy of 81.47%. In the context of Efficient B2 of the last epoch 30, specific numerical values offer insights into the model's final state. The loss decreased from 0.0214 to 0.0174, indicating improved error minimization on the training data.

However, the accuracy remained constant at 1.0000, suggesting consistent performance in predicting the training dataset. Conversely, the validation loss slightly increased from 3.0709 to 3.2932, implying a minor degradation in generalization performances evidenced by the slight increase in validation loss. However, the model's performance on the separate dataset yields a respectable accuracy of 83.33%. The InceptionV3 CNN model, integrated with the GRU sequential architecture, demonstrates a commendable test accuracy of approximately 82%, thanks to the collaborative strengths of both architectures.

Utilizing Adam optimizer for its adaptive learning rate mechanism and sparse categorical cross-entropy loss function for effective handling of multiple label classes, the model's performance improves steadily with increasing epochs. Notably, Adam optimizer consistently maintains stable training dynamics, contributing to the model's convergence towards higher accuracy levels. This successful synergy underscores the significance of strategic hyperparameter selection and leveraging complementary architectural features to achieve robust performance in video classification tasks

6. Conclusion and Future Scope

In this project, we have implemented a method for the detection of Deep-Fake videos using the combination of CNN and RNN architecture. We have kept our focus on Face-Swapped Deep-Fake videos. We primarily experimented only with various pre-trained CNN models like EfficientNet, and ResNet by finding the probability of each video frame being fake and predicting the output based on an aggregate of these probabilities. But the results weren't satisfactory, so we went forward by combining CNN and RNN model. for the CNN + RNN model, the features of face-cropped video frames are extracted using pre trained CNN models and it is

passed onto the RNN model which classifies the video as REAL or FAKE.

We Experimented with EfficientNet and InceptionNet for the feature extraction part and GRU is used to make the classification. We have obtained a maximum Test Accuracy of ~85% using this approach.

Our model has high precision for FAKE videos which is obtained by giving more FAKE videos during the training of the Model. The Future of fake detection in deep learning holds several promising avenues for exploration and advancement. These potential areas of future work aim to address existing challenges, improve detection capabilities, and adapt to emerging trends in fake content creation and dissemination. One key direction for future research involves enhancing the robustness and generalization of fake detection models.

This includes developing novel architectures and algorithms that can effectively detect increasingly sophisticated forms of fake content, such as deepfake videos with improved visual realism and semantic coherence.

Additionally, efforts to explore multimodal approaches, combining information from different sources such as text, audio, and video, hold promise for enhancing detection accuracy and resilience against adversarial attacks. Additionally, addressing the ethical and societal implications of fake detection in deep learning remains a critical area for future research and development.

This includes exploring issues such as privacy preservation, algorithmic fairness, and transparency in fake detection systems. Collaborative efforts between researchers, policymakers, and industry stakeholders are essential for establishing ethical guidelines, regulatory frameworks, and best practices to ensure the responsible development and deployment of fake detection technologies.

- Develop user-friendly deepfake detection tools like browser extensions or mobile apps.
- Integrate deepfake detection algorithms into content moderation systems.
- Establish regulatory frameworks and industry standards.
- Launch education and awareness campaigns about deepfakes.
- Foster interdisciplinary research collaboration.
- Empower users to verify media authenticity to combat misinformation.

- Prevent the dissemination of false information by automatically flagging or removing harmful Deepfake content.

Author Contributions

DSR: Conceptualization, drafting, data collection and analysis, Supervision;

SSR: Writing and method, Supervision, Methodology and review, writing and Data Collection, and Editing

CR: Drafting, Interpretation and Data Collection;

BSS: Drafting, , Data Collection and Analysis, Writing;

NP: Drafting, , Data Collection and Analysis, Writing and Data Collection.

Declaration

Conflicts of Interest: The authors declare no conflict of interest.

Author contribution: All authors wrote the main manuscript text and also consent to the submission

Ethical approval: Not applicable.

Consent to Participate: All authors consent to participate.

Funding: Not applicable, and No funding was received

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Personal Statement: We Declare with our best of Knowledge that this research work is purely Original Work and No third party material Not used in this article drafting. If any such kind material found in further online publication, we are responsible only for any judicial and copyright issues.

Acknowledgements

We thank everyone who inspired our work.

References

- [1]. Deng Pan; Lixian Sun; Rui Wang; Deepfake Detection through Deep Learning-[2020]In this paper, considering the deepfake detection technologies Xception and mobilenet as two approaches for classification tasks to automatically detect deepfake videos.
- [2]. Md. Shohel Rana; Beddhu Murali; Andrew H. Sung Deepfake Detection Using Machine Learning Algorithms - [2021] This paper presents the results of our study indicating that traditional machine learning (ML) techniques. The ML-based algorithms involve Support Vector Machine, Decision Tree, K-nearest Neighbor.
- [3]. Asad Malik; Sani M. Abdullahi; Ahmad Neyaz Khan Deepfake Detection for Human Face Images and Videos: A Survey - [2022] This paper proposes a temporal-aware pipeline to automatically detect

deepfake videos. System uses CNN and RNN that learn to classify if a video has been subject to manipulation or not.

- [4]. Amala Mary; Anitha Edison Deepfake Detection using deep learning techniques: A Literature Review- [2023] According to recent research, deep fake videos and images are widely disseminated on social media. Deep learning approaches RNN, CNN, and LSTM are proposed to detect deep fake videos/images. And this will bring up more research on this area.
- [5]. D. Guera and E. J. Delp, Deepfake Video Detection Using Recurrent Neural Networks, 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 2018, pp.1-6.
- [6]. Y. Li, M. Chang and S. Lyu, In Ictu Oculi: Exposing AI Created Fake Videos by Detecting Eye Blinking, 2018 IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, Hong Kong, 2018, pp. 1-7.
- [7]. G. Botelho de Souza, D. F. Da Silva Santos, R. Gonsalves Pires, J. P. Papa and A. N. Marana, Efficient Width-Extended Convolutional Neural Network for Robust Face Spoofing Detection, 2018 7th Brazilian Conference on Intelligent Systems (BRACIS), Sao Paulo, 2018, pp. 230-235.
- [8]. S. Rana, S. Gaj, A. Sur and P. K. Bora, Detection of fake 3D video using CNN, 2016 IEEE 18th International Workshop on Multimedia Signal Processing (MMSP), Montreal, QC, 2016, pp. 1-5.
- [9]. De Souza, G. B., da Silva Santos, D. F., Pires, R. G., Papa, J. P., & Marana, A. N. (2018, October). Efficient Width-Extended Convolutional Neural Network for Robust Face Spoofing Detection. In 2018 7th Brazilian Conference on Intelligent Systems (BRACIS) (pp. 230-235). IEEE.
- [10]. Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2018). Face Forensics: A large-scale video dataset for forgery detection in human faces. Arxiv preprint arxiv:1803.09179.