IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⪤ Peer-reviewed & Refereed journal ⪤ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11518

"Combatting Deceptive Media : An In- depth disquisition of Machine Learning ways for relatingFake Multimedia Content"

Lakshmi K K[1], M Divyashree[2], Poornima MC[3], Rupa Puthineedi[4], Tanmayee R[5]

Assistant Professor, Artificial Intelligence and Machine Learning, K.S. Institute of Technology, Bengaluru, India[1]

Student, Artificial Intelligence and Machine Learning, K.S. Institute of Technology, Bengaluru, India[2-5]

Abstract: With the rapid progress of technologies like Artificial Intelligence (AI), deep learning, and Machine Learning(ML), the ability to manipulate and modify images has become more accessible. This has led to the emergence of a concerning phenomenon known as deepfakes, where criminals can generate deceptive videos, images, or audio content. In addressing this growing challenge, the present paper introduces implementation of numerous approaches including Residual Networks (ResNet), Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNN) and Random forest with reference to identification of fake content. Despite the video, audio and image deepfake detection, this paper also introduces about live creation of the deepfakes.

Keywords: Deepfake, Residual Networks, LSTM, CNN, and Random Forest

I. INTRODUCTION

In this rapidly advancing tech era, manipulating images, videos, and audios through AI and ML has become surprisingly simple. This not only jeopardizes privacy but also opens the door to serious issues like shaping public opinion, spreading fake news, and even allowing criminals to create misleading impressions. Tackling this challenge requires a united front involving tech experts, policymakers, and society as a whole. Striking the right balance between innovation and ethical considerations is pivotal in finding effective solutions. Efforts are needed to create reliable detection tools and authentication protocols, especially to safeguard legal proceedings from the potential use of manipulated media as false evidence. Collaborative initiatives, bringing together tech companies, legal experts, and ethical hackers, are key to staying one step ahead of deceptive techniques and safeguarding against the misuse of transformative technologies.

Deepfakes are AI generated synthetic media that replace or overlay pre-existing information with freshly created, frequently faked content. A crucial step in the production of deepfakes is deep image generation. In real-time deepfake generation, the provided image serves as the reference point, and during the live process, the individual appearing on camera undergoes transformation to resemble the source image.

A deep fake image is a digitally altered picture generated using sophisticated artificial intelligence, often indistinguishable from authentic images. ResNet50 and LSTM combined can assist to take use of each architecture's advantages and increase the detection accuracy of deepfake movies, particularly for those that contain both sequential and image-based data [1]. Through [2] rigorous training and evaluation against birth models like CNN, the study contributes to the creation of automatic and precise deep fake discovery systems to attack the challenges posed by deceptive synthetic media.

Deepfake audio is the term for the application of AI and deep learning methods to produce synthetic audio files that accurately mimic the voice of a particular individual. It is possible to create authentic-sounding, modified audio recordings that may imitate several features of the target person's voice, such as speech patterns, intonations, and other vocal characteristics. Randomforest model is used to detect whether an audio file is genuine or spoofed [3].

A deepfake video is an artificially manipulated or synthesized video generated through AI, especially deep learning methods. These videos employ algorithms to modify or substitute the visual and auditory components of the original material, frequently producing convincing simulations of people. Xception and MobileNet are two algorithms utilized for deepfake detection. These models are trained on FaceForensics++ datasets generated by different deepfake technologies, achieving high accuracy [4].

DOI: 10.17148/IARJSET.2024.11518

The main objective of this paper is to provide an in-depth understanding of deepfakes which includes image, audio, video and live manipulation using artificial intelligence and machine learning techniques. The aim of this paper is to explore the risks associated with the widespread use of deepfake technology, including threats to privacy, potential manipulation of public opinion, dissemination of fake news, and the creation of misleading impressions.Back propagation minimizes loss in Neural Networks, but vanishing gradients in deep layers are addressed by ResNet, using skipping connections. Combining LSTM-CNN enhances deepfake detection, leveraging temporal and spatial analysis. The system initializes parameters individually, enabling rapid training with minimal images. The surge in realistic fake facial media from AI, exemplified by DeepFake, poses challenges due to potential social disturbances.

II. RELATED WORKS

From the literature, researchers have already used several strategies to create an effective DF detection system. Despite the different approaches, the basic ideas behind most remain the same, emphasizing the use of inconsistencies and manipulation traces left by GAN tools during the intergenerational network.One study

[1] uses different strategies to create an effective DF detection system that highlights inconsistencies and traces of manipulation.Study

[2] focuses on datasets and techniques, with an emphasis on multimodal data, to improve detection accuracy. misleading audiovisual content.Another study

[3] addresses the challenges of deep spoofing by comparing the effectiveness of the model on the FaceForensics++ dataset. The conclusion discusses the findings and possible directions for the development of deep fake detection technology.A multimodal study

[4] presents a deep fake detection method that achieves 92.9% accuracy for FakeAVCeleb. It performs good in all datasets (83.61% and 70% of world leaders and presidents datasets, respectively) using both IEML and IAML.
Insights are obtained through integrated gradient analysis.In a unique study

[5], the "Deepfake Video Detection System" uses CNNs and RNNs in a time-aware pipeline for automatic deep fake video detection. The system shows effectiveness against many deep fake videos even for its simplicity.
Another study

[6] found that deep fakes undermine trust in ALL social media news, but skepticism does not prevent certain frauds. This widespread suspicion actually feeds other false alarms, making people less confident about online resources. Advanced research on the D-CNN architecture.

[7] addresses frame-to-frame differences and achieves high accuracy in strong deep false detection of pictures Trained on different datasets, the model produces impressive results: 98.33% for AttGAN and 99.17% for StarGAN for real and deep fake images. A comprehensive study of DeepFake detection in human face photos and videos

[8] focuses on the realism which can be achieved. with generative deep learning algorithms. The goal is to promote deep learning applications in facial image and video DeepFake detection by classifying detection methods, exploring creative techniques and exploring datasets.Proposal

[9] presented a method for Deep Vision Deepfake detection by analyzing changes in human. eye blinking patterns. It achieves 87.5% accuracy in different videos.
Another work

[10] uses an advanced GAN technique, a better version of PGGAN, to solve the sparsity of medical image data in DEEPFAKE image synthesis. U-net metrics show that Enhanced-GAN performs better than PGGAN in segmentation tasks.With growing skepticism about average fakes,
This study

[11] identifies a disturbing paradox: even as overall trust in social media news decreases, certain deep fakes still can. to triumph . This highlights the need for AI-powered detection, which currently promises 90% accuracy, to continuously adapt and overcome evolvingfake video technology.

The deep learning techniques explored in [12] explore the production and detection of deep fakes in detail. The paper provides in-depth information on state-of-the-art approaches, helping researchers to understand and benchmark the development of deep fake photo and video detectionin social media materials.

The pioneering study [13] categorized the techniques into deep learning. , statistical and blockchain techniques. , and traditional machine learning, all show consistent superiority over other approaches.

A unique deep fake detector with a CNN-LSTM framework and two-wire network is presented in a remarkable study [14], highlighting its strong overall performance across all methods. The successful cross-modal testing of FaceForensic++ is a big step forward in the fight against deep fake fraud.

One study [15] uses machine learning and deep learning - specifically MFCCs - on a fake or real dataset. detect a deep fake voice. It is noteworthy that SVM performs well in certain datasets, but in another study on the original dataset, the VGG-16 model performs better than other methods.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⪤ Peer-reviewed & Refereed journal ⪤ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11518

Another study [16] investigates GAN-based deep spoofing threats and improves detection by evaluation of the importance of facial regions and temporal information of video exploitation. Results from CelebDF and FaceForensics++ show that the extra temporal dimension significantlyimproves performance.
Another pioneering study [17] presents a robust facial forensics framework that performs exceptionally well in detecting manipulation, especially when dealing with different levels of video compression. It visualizes class activation maps to detect salient facial features and show violation traces using convolutional neural networks.
One paper [18] explores the creation and recognition of deeply rendered images through the lens of deep learning applications. Emphasizing the security and privacy concerns, it suggests the use of deep learning techniques for image augmentation to improve the quality of deep forgery.
Another study [19] proposes a hybrid face crime framework that combines convolutional and general-purpose neural network techniques and representations.Eexceptional durability and accuracy. It outperforms previous approaches on various datasets and provides insight into important facial features and hidden traces of forgery using class activation maps.
A pioneering study [20] evaluates the ability of deep face recognition to detect deep forgeries. Using various loss functions and deep falsification techniques, it achieves a remarkable 0.98 AUC and 7.1% EER with Celeb-DF, outperforming traditional two-class CNNs and eye-based approaches. In particular, Deep Face Detection perfectly adapts to evolving deep fake techniquesand ensures its effectiveness against future threats.
This section concludes with Table I, which highlights the contributions of researchers in the fieldof DeepFake.

Table 1: Prominent studies highlighting the significance of deepfake approaches towards nextanalysis.

Sl. No	Year of Publication	Title of paper	Description
1.	2023	Deep Fake Generation and Detection:Issues, Challenges, andSolutions	This article explores the challenges of detecting deepfake audio and video, emphasizing the potential harm in various contexts. It provides an overview of existingdetection models, datasets, challenges, and opportunities.
2.	2023	A Comparative Study: Deepfake Detection Using Deep-learning	The study compares four deeplearning models- VGG16,MobileNetV2, XceptionNet and InceptionV3—thatwere trained on the FaceForensics++ dataset in aneffort to improve deep fake detection.
3.	2023	Multimodaltrace: Deepfake Detection using Audiovisual Representation Learning	This paper introduces "Multimodaltrace," a novel multimodal framework for detecting deepfakes by integrating audio and visual cues.
4.	2023	Deepfake Video Detection System Using Deep Neural Networks	In order to increase accuracy, this study investigates deepfake detection using a hybridarchitecture that incorporates ResNet50 and LSTM.
5.	2023	Deep learning based DeepFake videodetection	In order to distinguish between real and fake movies, this study proposes a deep learning model based on transfer learning from the VGG16 neural network, which tackles the growing threat posed byDeepFake face-swapping technology. detection algorithms inthe face of developing DeepFake technology.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁒ Peer-reviewed & Refereed journal ⁒ Vol. 11, Issue 5, May 2024
DOI: 10.17148/IARJSET.2024.11518

6.	2023	Artificial Intelligence into Multimedia Deepfakes Creation andDetection	The commercial viability of deepfakes, facilitated by artificial intelligence, has led to a paradox where people are less likely to believe social media news but are more prone to skepticism than outright deception by deepfakes.
7.	2023	An Improved Dense CNN Architecture for Deepfake ImageDetection	In order to address the issue of inter-frame dissimilarities that are frequently disregarded by current methods, this study presents an enhanced deep-CNN (D-CNN) architecture for deepfake detection.
8.	2022	DeepFake Detection for Human Face Images and Videos: A Survey	This article delves into DeepFake technology, covering its basics, risks, and GAN-based applications. It emphasizes the challenges in current detection methods and the ongoing need for improved data integrity measures.
9.	2022	DeepVision: Deepfakes Detection Using Human Eye Blinking Pattern	This study presents DeepVision, an algorithm utilizing changes in eye blinking patterns to detect GANs- generated Deepfakes with an 87.5% success rate.
10.	2022	Deepfake video detection using InceptionResnetV2	The need to distinguish real from false videos has increased due to the increasing ubiquity of deepfake face-swapping technologies, which has sparked research into deep learning model creation.
11.	2022	DEEPFAKE Image Synthesis for Data Augmentation	Enhanced-GAN excels in DEEPFAKE image generation, surpassing PGGAN in AM and Mode scores. Combined with real data, its synthesized DEEPFAKE data enhances U-net segmentation model performance in Schema-C.
12.	2022	Deepfake Detection in Videos and Picture: Analysis of Deep Learning Models and Dataset	With deep learning serving as the central technique, this study explores the critical need ofdeepfake identification as these altered graphics become more common. In response to the demand for reliable algorithms, the research investigates several techniques— such as Generative Adversarial Nets (GANs)—and offers a comparative analysis to improve the effectiveness of deepfake detection and prevention.

DOI: 10.17148/IARJSET.2024.11518

13.	2022	Deepfake Detection: A Systematic LiteratureReview	The methodology for the systematic literature review (SLR) on Deepfake detection involves three main stages: Planning the Review, Conducting the Review, and Reporting the Review.
14.	2022	Generalized Deepfake Video DetectionThrough Time- Distribution and Metric Learning	In this paper, a time-distributed network that uses a two-stream network with a CNN-LSTM backbone to use spatial and temporal information is presented as a generalized deepfake detector.
15.	2022	Deepfake Audio Detection via MFCC Features Using Machine Learning	This study employs deep learning and machine learning techniques to identify deepfake audio. Specifically, it applies the Mel- frequency cepstral coefficients (MFCCs) technique on the Fake-or- Real dataset. Experimental results suggest that the VGG-16 model surpasses other state-of-the-art methods, demonstrating its usefulness in deepfake audio detection, while the support vector machine (SVM) excels in accuracy on particular datasets.
16.	2021	Deepfake Video Detection with Facial Features and Long- Short Term MemoryDeep Networks	This research addresses the dynamic landscape of generative models by investigating how temporal information from videos might be used to improve state-of- the-art deepfake detection techniques.
17.	2021	Detecting Deepfakes Using Deep Learning	This work presents an improved model that uses Deep Learning, CNN, and Error Level Analysis (ELA) to precisely identify modified facial photos produced by AI, especially GAN-generated images.
18.	2021	Exposing Fake Faces Through Deep Neural Networks Combining Content and Trace Feature	The paper introduces a robust fake face detection model using multi- channel constrained convolution, achieving high accuracy against Face2Face and DeepFake manipulations.
19.	2021	DeepFake Creation andDetection:A Survey	The phrase "DeepFake," which refers to multimedia content produced with realistic deep learning technology, presents serious risks to national security and privacy since it allows for the unapproved exchange of faces and aids in the dissemination of false information.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11518

20.	2021	An Experimental Evaluation on Deepfake Detection using Deep Face Recognition	This work provides a thorough assessment of deep face recognition's performance in detecting deepfakes using a range of loss functions and deepfake creation methods. With a maximum Area Under Curve (AUC) of 0.98 and Equal Error Rate (EER) of 7.1% on Celeb-DF.
21.	2020	Manipulation Classification for JPEGImages Using Multi-Domain	MCNet excels in classifying manipulation algorithms in JPEG compressed images, utilizing spatial, frequency, and compression domain features. Its superior performance makes it promising for real-world applications, includingDeepFake detection and integrity authentication.
22.	2020	DeepVision: Deepfakes Detection Using HumanEye Blinking Pattern	Our technology, DeepVision, which uses patterns in the blinking of the eyes, identified Deepfakes in 87.5% of the videos. Although encouraging, it has drawbacks when it comes to people who have mental health problems, which emphasizes the necessity for continuous advancements in cybersecurity techniques.
23.	2019	Combating Deepfake Videos Using Blockchain and Smart Contracts	The solution utilizes a decentralized system with IPFS, Ethereum, and a reputation system to verify the authenticity of digital videos, providing a robust method to counter deepfake content.
24.	2019	An Adversarial Approach to Few-ShotLearning	I suggest a system that handles few- shot learning problems using the conceptually straightforward and universal MetaGAN framework.
25.	2018	A novel contrast enhancement forensics based on convolutional neural networks	First- and second-order statistics can be used to create relatively simple handcrafted characteristics for Contrast Enhancement (CE) forensic approaches, yet these methods have had trouble identifying contemporary counter-forensic attacks.
26.	2018	Fake Face Detection Methods: Can They Be Generalized?	The current advancements in computer vision technologies have made it possible to create fake faces through the use of fresher, alternative techniques. A group of CNN-based systems and Local Binary Patterns (LBP) are taken into consideration.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024
DOI: 10.17148/IARJSET.2024.11518

27.	2018	A Large-scale Video Dataset for Forgery Detection in HumanFaces	Recent developments in deep learning have made it feasible to use Face2Face, Computer Generated Face picture (CGFI), Snap-Chat, picture morphing, Generative Adversarial Networks (GAN), and Snap-Chat to create modified photographs and videos in real-time.
28.	2018	Data AugmentationGenerative Adversarial Networks	Even in target domains with limiteddata, the Data Augmentation Generative Adversarial Network
			(DAGAN) facilitates efficient neural network training. Moving data points to other points of equivalent class, the DAGAN captures the cross-class transformations because it is not dependent on the classes themselves.
29.	2018	Anatomically-aware Facial Animation from aSingle Image	In addition to creating new expressions, the StarGAN architecture may alter the appearance of age, gender, and hair color on the face. Despite its generality, StarGAN can only modify one specific face characteristic out of a limited set of attributes determined by the dataset's annotation granularity.
30.	2018	Deepfake Video Detection Using Recurrent NeuralNetworks	In order to automatically recognize deepfake films, this study presents a temporal-aware pipeline that uses a convolutional neural network (CNN) to extract frame-level characteristics. The suggested approach shows competitive results in identifying edited videos from several sources by combining these features with a recurrent neural network (RNN), demonstrating effectiveness with a simple design.
31.	2018	Deep LearningAlgorithms for Detecting Fake News in Online Text	This study addresses the pervasive problem of fake news on social media, emphasizing how it shapes events and societal opinions. The study finds that GRU is the most successful RNN model (vanilla, GRU, LSTM). This leads to additional investigation into a hybrid GRU and CNN model to improve accuracy on the LAIR dataset.
32.	2017	Detecting Computer Generated Images with	This research presents a novel method that uses transfer learning

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11518

		Deep ConvolutionalNeural Networks	and a deep convolutional neural network based on ResNet-50 to recognize computer-generated images.
33.	2017	Discrimination Between Genuine Versus Fake Emotion Using Long- Short Term Memory with Parametric Bias and Facial Landmarks	This article presents a novel method that combines deep recurrent networks, namely long-short term memory (LSTM) with parametric bias (PB), and mirror neuron modeling to distinguish between real and artificial emotions.

III. METHODOLOGY

Every day, professionals rely on tools like Photoshop and After Effects, but merely installing these programs isn't sufficient to create realistic images and videos. Similarly, crafting believable face-swapped videos is a challenging task. Like any creative endeavor, the final outcome depends on acombination of skill, dedication, and using the right tools.

The initial foray into deepfake creation began with FakeApp, developed by a Reddit user using an autoencoder-decoder blending framework. In this method, the autoencoder extracts latent features from facial images, and the decoder reconstructs them. To swap faces between source and target images, two sets of encoder-decoder pairs are needed, where each pair is trained on a separate image set, sharing the encoder's parameters between them. In simpler terms, both pairs share the same encoder network. The process of deepfake creation involves 3 stages:

i) Extraction
ii) Training
iii) Creation

i) Extraction:
As we know, deep learning requires large data sets. It takes thousands of different images to create a deep fake video. The extraction process refers to the process of extraction, face detection and alignment of all frames. Alignment is a critical process, a neural network is used to shift, and all faces must be the same size
.

ii) Training:
Training is a special term of machine learning. In this situation, it refers to a procedure that allows the nervous system to change over the face to another. Despite the few hours, the preparation step only needs to be done once. Once this is done, it can change across the face from Person A to Person B.

iii) Creation:
Once training is complete, it's time to create a deepfake. Starting with either a video or an image, all frames are extracted and facial features are adjusted. Then, each frame is transformed using the trained neural network. The final step involves integrating the transformed face back into the original frame.
A deepfake generation model employs two encoder-decoder pairs: one for each subject. These networks share the same encoder but have different decoders during training. An image of Subject A's face is encoded and decoded by Subject B's decoder to generate a deepfake. Similarly, facial features can be exchanged by passing Subject A's latent face to Subject B's decoder and vice versa. If the network has successfully generalized, the latent space will represent facial expressions and orientations. This implies that generating Subject B's face involves using the same expressions and orientations as Subject A. It's crucial that the two subjects used in training share as many similarities as possible. This ensures that the shared encoder can capture key features that are easyto transfer.

iv) Detection:
The fundamental architecture for creating deepfakes involves an encoder-decoder setup, where the encoder captures features from both the target and source faces, and the decoder's role is to obtain encoding features from the target face to generate a fake video. Through advanced processing, video quality is improved and residual traces, invisible to the naked eye, are removed.These leftover traces serve as crucial features for our detection model.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⪾ Peer-reviewed & Refereed journal ⪾ Vol. 11, Issue 5, May 2024
DOI: 10.17148/IARJSET.2024.11518

The proposed model utilizes Inception ResNetV2 for feature extraction. These features are then used to train a recurrent neural network (RNN) tasked with analyzing whether a video has undergone manipulation. Since only a small portion of the video is manipulated, resulting in shorter deepfake segments, the video is split into small frames and fed into the detection model.

The dataset is compiled from various sources including the deepfake detection challenge dataset on Kaggle, FaceForenscis, and Celeb-deepfakeforensics, totalling approximately 6458 videos. These videos include authentic footage manipulated by paid actors, converted into deepfake videos using various generator methods. Seventy percent of the dataset is allocated for training, while the remaining 30 percent is for testing, with accompanying labels provided during training. During preprocessing, frames indicating the transition from original to deepfake are captured and analyzed, resulting in an average of 147 frames per video. Due to computational constraints, a limited number of frames are used for training, with the remaining frames processed in batches.

The modeling approach involves conducting image categorization analysis on each frame extracted from the video. We employ a pretrained CNN model, Inception ResNetV2, in conjunction with RNN and LSTM layers. Additionally, defining loss functions, optimizers, and other hyperparameters is essential for the training process. The learning rate is adjusted based on the training model's state to minimize loss values. Random Forest is applied in audio deepfake detection by training a group of decision trees with preprocessed features from real and fake audio. This method selects random features at each decision point and aggregates the trees' outputs to classify new audio as real or fake, leveraging its robustness and feature assessment capabilities.

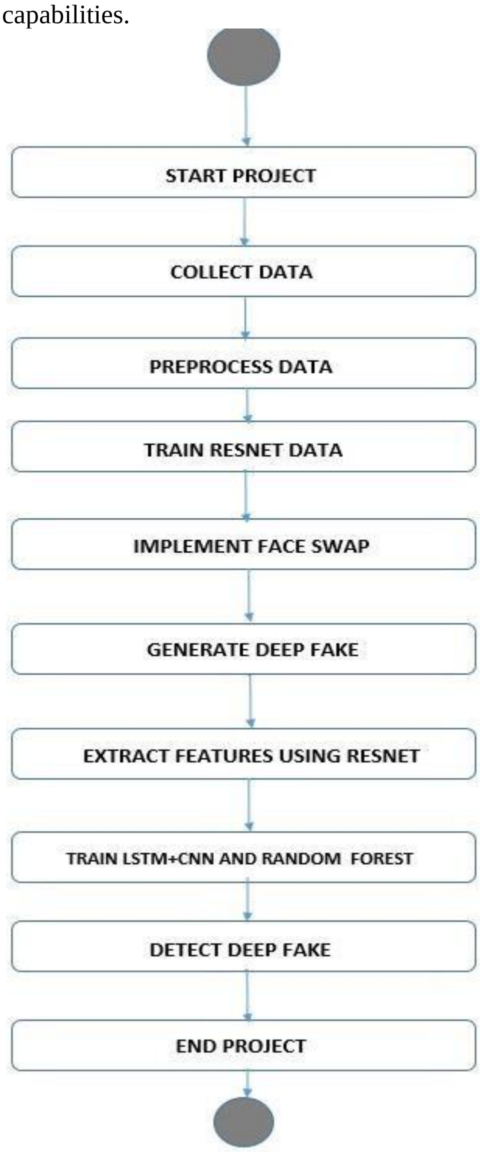

Fig 1 : Deepfake methodology used

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⅔ Peer-reviewed & Refereed journal ⅔ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11518

IV. RESULT

In summary, our project employs cutting-edge deep learning methods alongside intricate preprocessing and feature extraction techniques to generate and identify deepfakes efficiently. The process involves extracting facial features, feeding frames into a trained neural network for transformation, and integrating the altered face back into the original frame. Our modeling strategy includes analyzing image categories within each video frame. We utilize a pre-trained CNN model, specifically Inception ResNetV2, along with RNN and LSTM layers for images and videos and R. Furthermore, it's crucial to define loss functions, optimizers, and other hyperparameters to facilitate the training process. Adjustments to the learning rate are made depending on the state of the training model to minimize loss values. Consequently, our model can both generate deepfakesand identify them. It also creates the deepfake live.

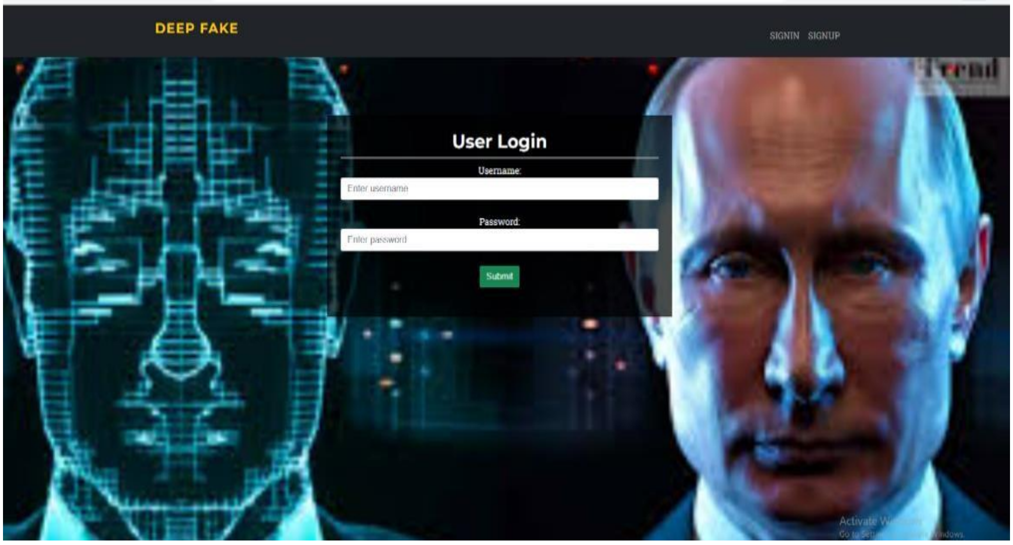

Fig 2 : Login Page

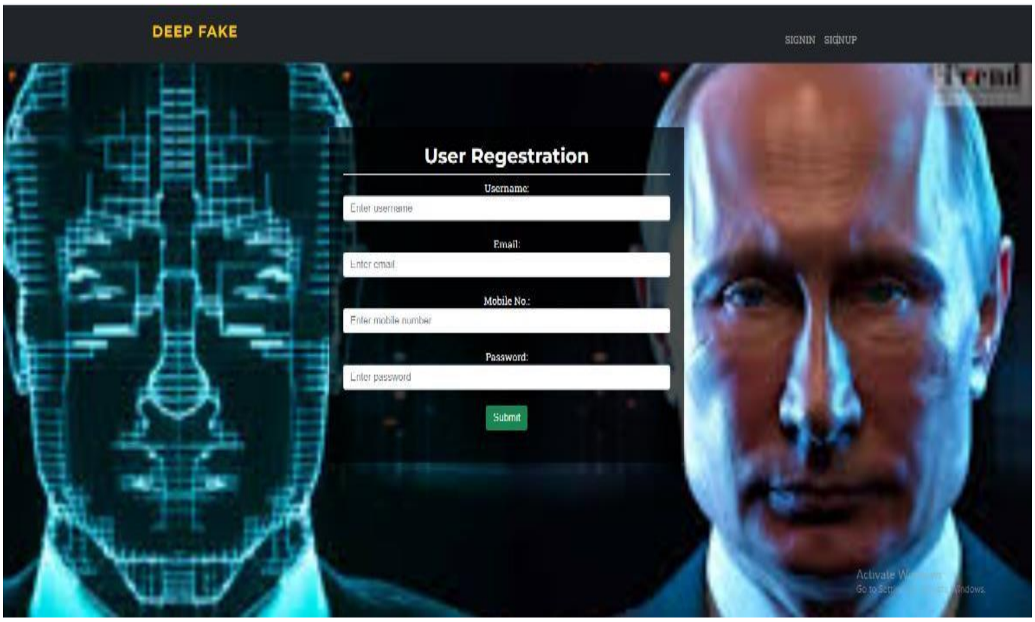

Fig 3 : Registration page

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁘ Peer-reviewed & Refereed journal ⁘ Vol. 11, Issue 5, May 2024
DOI: 10.17148/IARJSET.2024.11518

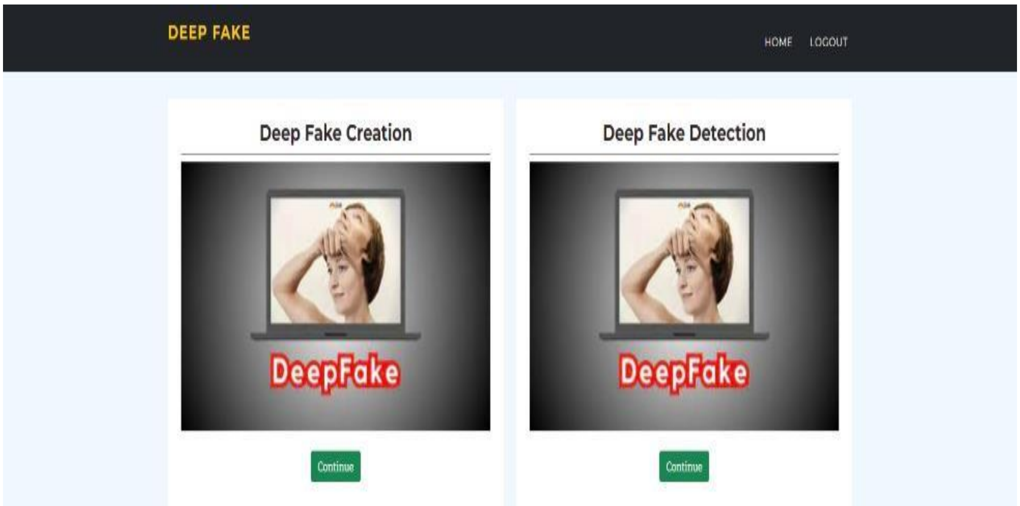

Fig 3 : Home page

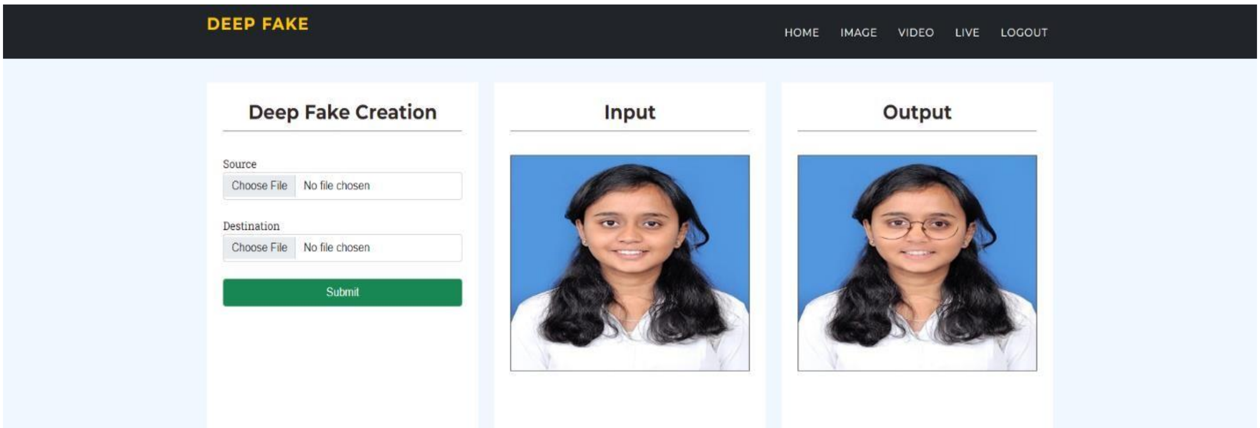

Fig 4 : Deepfake image creation

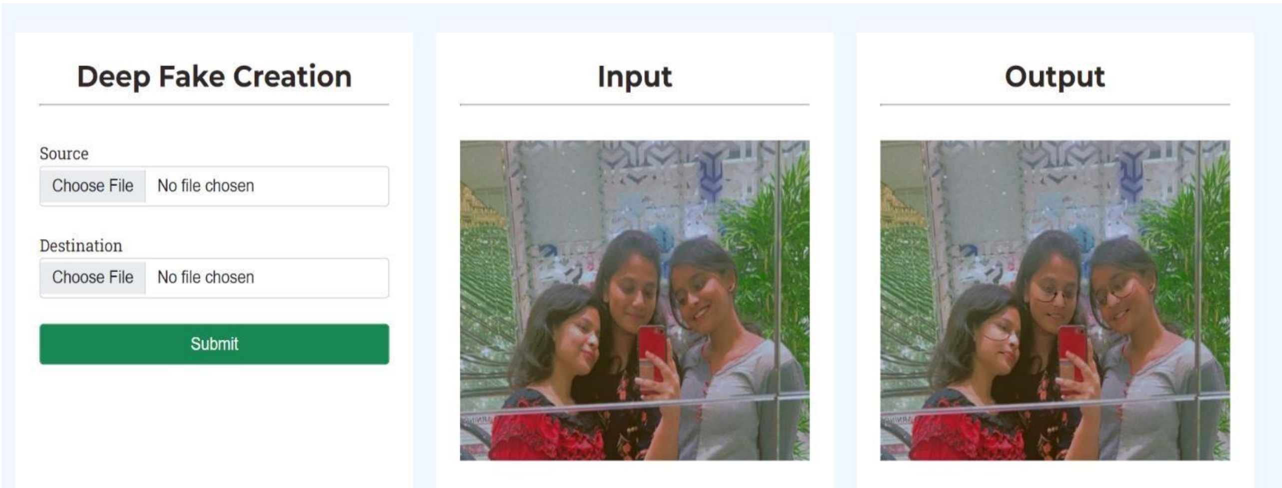

Fig 5 :Deepfake image creation for multiple faces

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11518

Fig 6: deepfake video creation

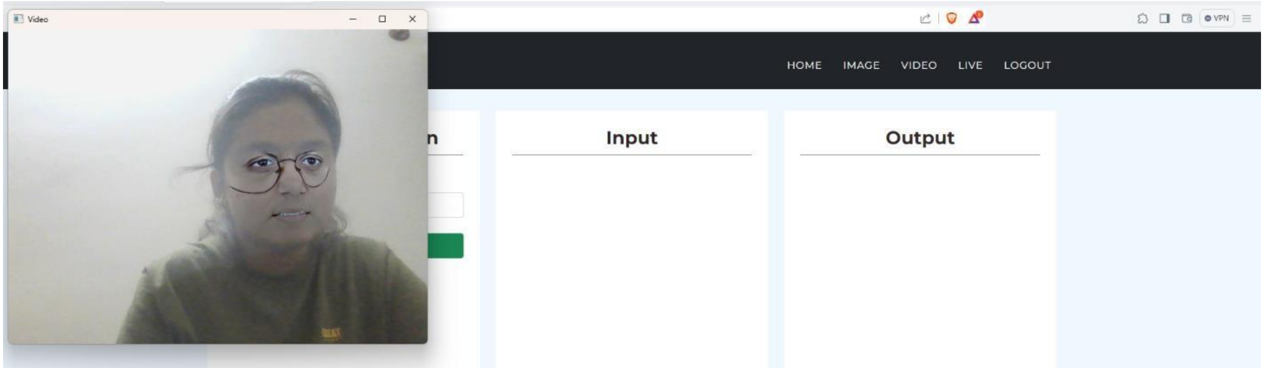

Fig 7 : deepfake live creation

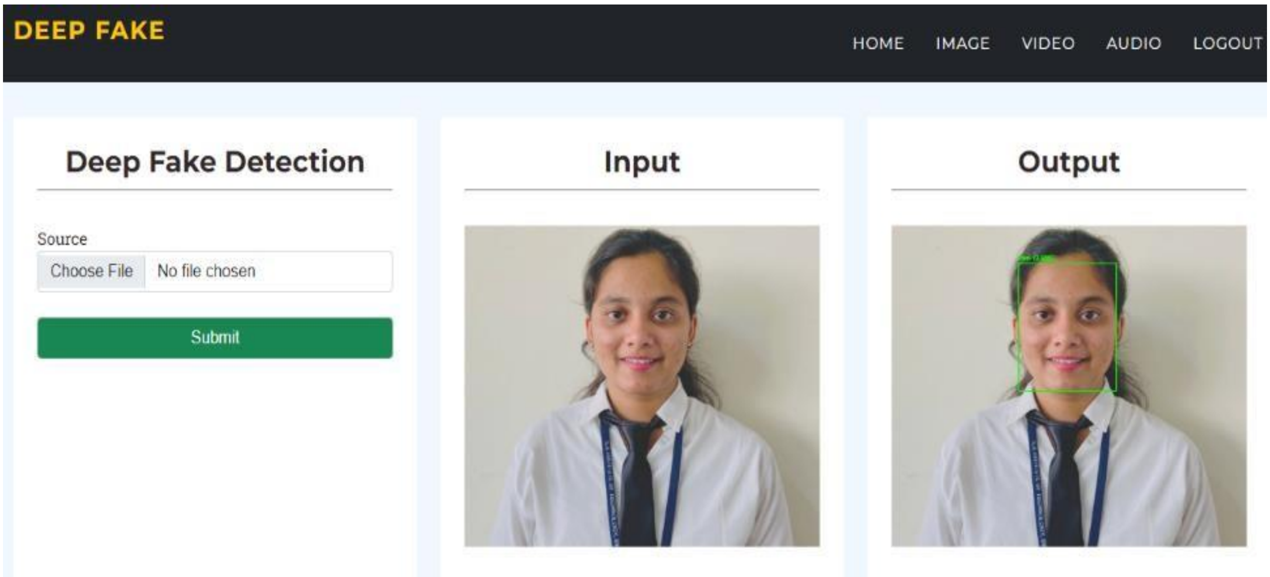

Fig 8 : deepfake image detection

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁘ Peer-reviewed & Refereed journal ⁘ Vol. 11, Issue 5, May 2024
DOI: 10.17148/IARJSET.2024.11518

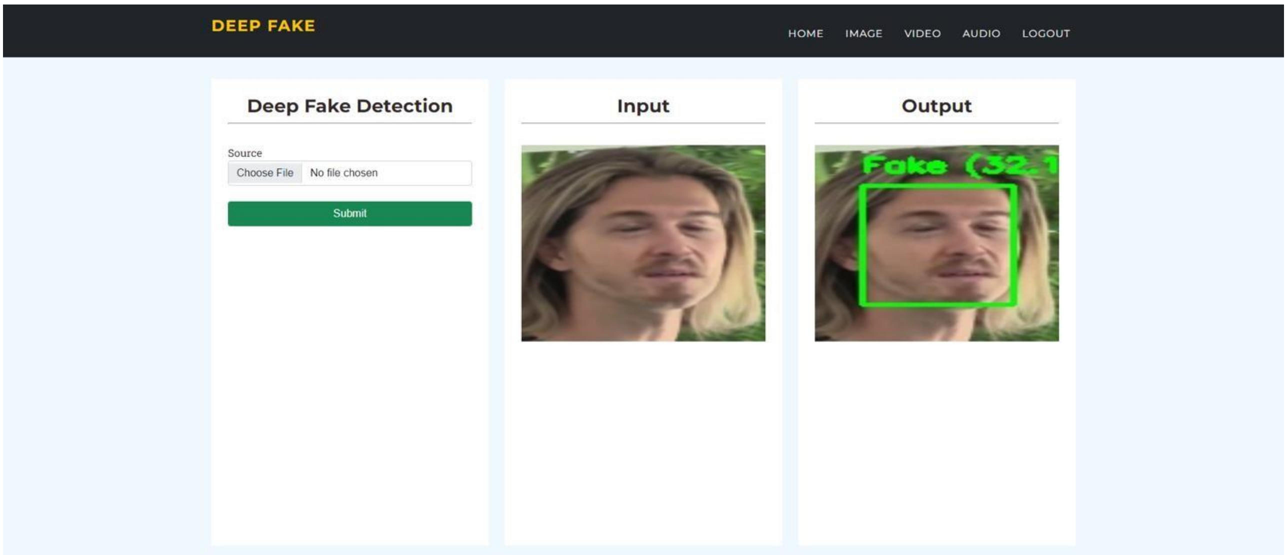

Fig 9 : deepfake image detection

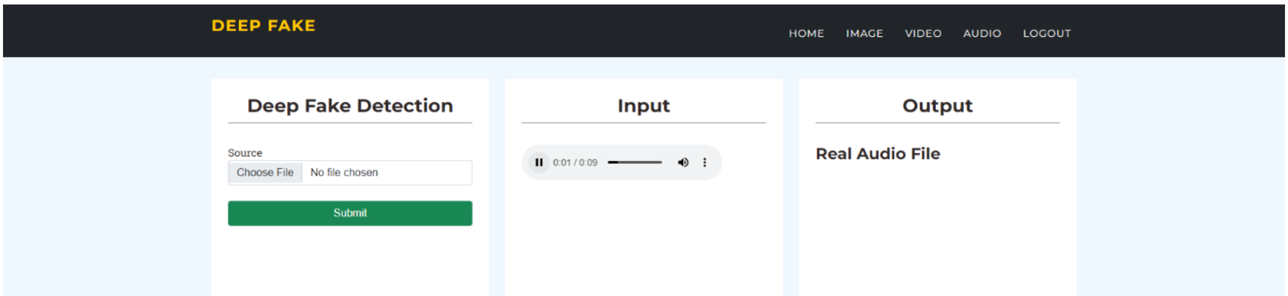

Fig 10: real audio detection

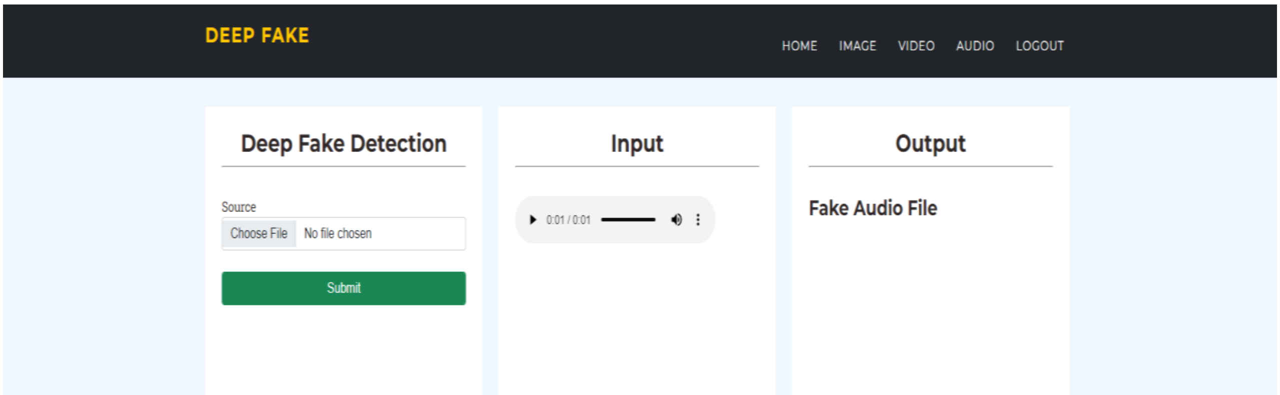

Fig 11: fake audio detection

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 11, Issue 5, May 2024
DOI: 10.17148/IARJSET.2024.11518

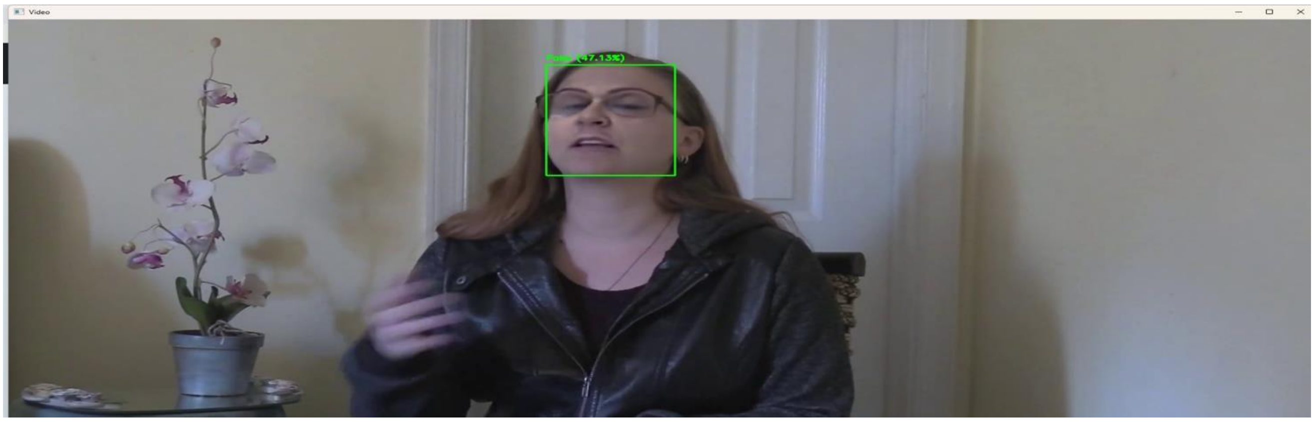

Fig 12: video detection

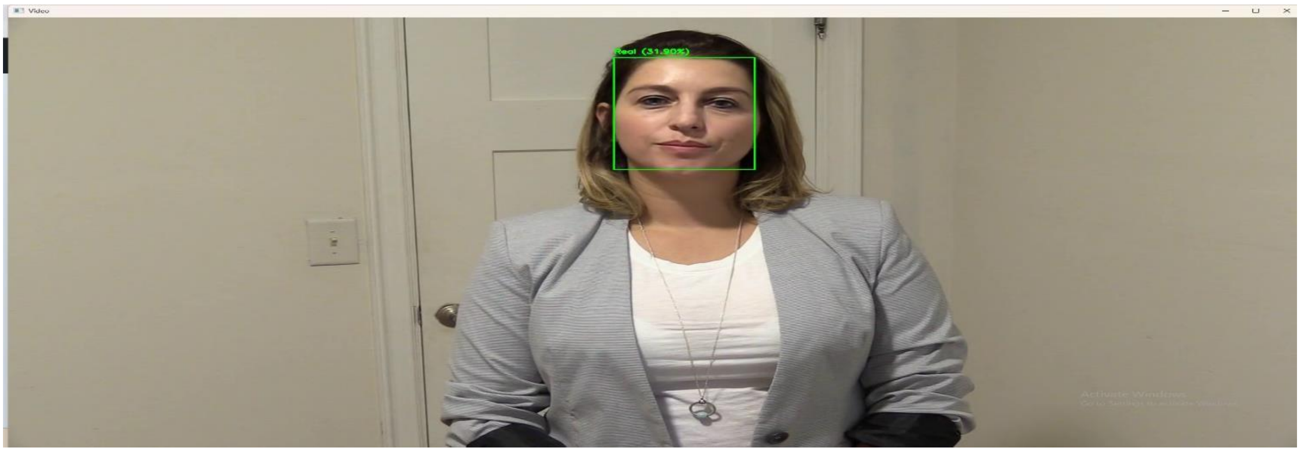

Fig 13: video detection

V. CONCLUSION

In conclusion, this research highlights the critical need to address the threats posed by deep counterfeiting as a result of advances in AI and artificial intelligence. The combination of ResNet50 and LSTM shows promise for improving detection accuracy, and the collaboration is crucial for advancing fraud techniques. As we navigate this landscape, continued development of reliable identification tools is critical to maintaining public trust in the digital age. The spread of deepfakes has weakened trust in media content, because seeing them no longer guarantees belief in their authenticity. These manipulated videos and images pose significant risks, such as harming the targeted individuals, spreading misinformation and hate speech, and potentially exacerbating political tensions or inciting violence. Due to the ease of creating deep fakes and the rapid spread of fake content on social media platforms, the impact can be widespread and harmful. In addition, deep fakes can be strategically targeted to specific audiences without mass distribution, increasing their malicious potential..

It is essential for individuals to be vigilant and discern between fake and real content. Videos and photos, often used as evidence in legal proceedings, can be manipulated using machine learning and artificial intelligence technologies, making it difficult for even experts in digital media forensics to authenticate them.

Recent advancements in deep learning have led to the creation of highly realistic human head images, often requiring large datasets for training personalized talking head models. However, in practical situations, there may be limited image views available, necessitating techniques for one-shot learning or minimal data training.

To address this, we propose a robust system capable of generating deepfakes from a single photograph (one-shot learning), with additional images improving personalization fidelity.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⫹ Peer-reviewed & Refereed journal ⫹ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11518

The proliferation of AI-driven fake face media, like DeepFake or Face2Face, poses significant challenges to privacy, societal harmony, and security at various levels. Detecting fake faces in media is crucial for safeguarding individual privacy and preventing social and political unrest.

Previous research in this domain has focused on general-purpose image forensics, which extracts hand-crafted features to detect manipulation, and face image forensics, which employs convolutional neural networks to extract content features. Our system integrates these approaches into a hybrid face forensics framework, enhancing manipulation detection performance by combining the strengths of both methods.

REFERENCES

[1]. S. R. B. R, P. Kumar Pareek, B. S and G. G, "Deepfake Video Detection System Using Deep Neural Networks," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6, doi: 10.1109/ICICACS57338.2023.10099618. Link: https://ieeexplore.ieee.org/document/10099618

[2]. A. Mary and A. Edison, "Deep fake Detection using deep learning techniques: A Literature Review," 2023 International Conference on Control, Communication and Computing (ICCC), Thiruvananthapuram, India, 2023, pp. 1-6, doi: 10.1109/ICCC57789.2023.10164881. Link: https://ieeexplore.ieee.org/document/10164881

[3]. G. Ulutas, G. Tahaoglu and B. Ustubioglu, "Forge Audio Detection Using Keypoint Features on Mel Spectrograms," 2022 45th International Conference on Telecommunications and Signal Processing (TSP), Prague, Czech Republic, 2022, pp. 413-416, doi: 10.1109/TSP55681.2022.9851327. Link: https://ieeexplore.ieee.org/document/9851327

[4]. D. Pan, L. Sun, R. Wang, X. Zhang and R. O. Sinnott, "Deepfake Detection through Deep Learning," 2020 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT), Leicester, UK, 2020, pp. 134-143, doi: 10.1109/BDCAT50828.2020.00001. Link: https://ieeexplore.ieee.org/document/9302547

[5]. S. Salman, J. A. Shamsi and R. Qureshi, "Deep Fake Generation and Detection: Issues, Challenges, and Solutions," in IT Professional, vol. 25, no. 1, pp. 52-59, Jan.-Feb. 2023, doi: 10.1109/MITP.2022.3230353. Link: https://ieeexplore.ieee.org/document/10077834

[6]. N. Khatri, V. Borar and R. Garg, "A Comparative Study: Deepfake Detection Using Deep- learning," 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2023, pp. 1-5, doi: 10.1109/Confluence56041.2023.10048888. Link:https://ieeexplore.ieee.org/document/10048888

[7]. M. Anas Raza and K. Mahmood Malik, "Multimodaltrace: Deepfake Detection using Audiovisual Representation Learning," 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Vancouver, BC, Canada, 2023, pp. 993-1000, doi: 10.1109/CVPRW59228.2023.00106. Link: https://ieeexplore.ieee.org/document/10208948

[8]. S. R. B. R, P. Kumar Pareek, B. S and G. G, "Deepfake Video Detection System Using Deep Neural Networks," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6, doi: 10.1109/ICICACS57338.2023.10099618. Link: https://ieeexplore.ieee.org/document/10099618

[9]. S. Guefrachi et al., "Deep learning based DeepFake video detection," 2023 International Conference on Smart Computing and Application (ICSCA), Hail, Saudi Arabia, 2023, pp. 1-8, doi: 10.1109/ICSCA57840.2023.10087584. Link:https://ieeexplore.ieee.org/document/10087584

[10]. M. A. Khder, S. Shorman, D. T. Aldoseri and M. M. Saeed, "Artificial Intelligence into Multimedia Deepfakes Creation and Detection," 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD), Manama, Bahrain, 2023, pp. 1-5, doi: 10.1109/ITIKD56332.2023.10099744. Link: https://ieeexplore.ieee.org/document/10099744

[11]. Y. Patel et al., "An Improved Dense CNN Architecture for Deepfake Image Detection," in IEEE Access, vol. 11, pp. 22081-22095, 2023, doi: 10.1109/ACCESS.2023.3251417. Link: https://ieeexplore.ieee.org/document/10057390

[12]. A. Malik, M. Kuribayashi, S. M. Abdullahi and A. N. Khan, "DeepFake Detection for Human Face Images and Videos: A Survey," in IEEE Access, vol. 10, pp. 18757-18775, 2022, doi: 10.1109/ACCESS.2022.3151186. Link: https://ieeexplore.ieee.org/document/9712265

[13]. T. Jung, S. Kim and K. Kim, "DeepVision: Deepfakes Detection Using Human Eye Blinking Pattern," in IEEE Access, vol. 8, pp. 83144-83154, 2020, doi: 10.1109/ACCESS.2020.2988660.
Link: https://ieeexplore.ieee.org/document/9072088

[14]. R. R. Rajalaxmi, S. P. P, R. A. M, P. S, D. P and G. E, "Deepfake Detection using Inception- ResNet-V2 Network," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode,

India, 2023, pp. 580-586, doi: 10.1109/ICCMC56507.2023.10083584. Link: https://ieeexplore.ieee.org/document/10083584

[15]. N. Waqas, S. I. Safie, K. A. Kadir, S. Khan and M. H. Kaka Khel, "DEEPFAKE Image Synthesis for Data Augmentation," in IEEE Access, vol. 10, pp. 80847-80857, 2022, doi: 10.1109/ACCESS.2022.3193668. Link: https://ieeexplore.ieee.org/document/9839427

[16]. S. S. Chauhan, N. Jain, S. C. Pandey and A. Chabaque, "Deepfake Detection in Videos and Picture: Analysis of Deep Learning Models and Dataset," 2022 IEEE International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2022, pp. 1-5, doi: 10.1109/ICDSIS55133.2022.9915885. Link: https://ieeexplore.ieee.org/document/9915885

[17]. M. S. Rana, M. N. Nobi, B. Murali and A. H. Sung, "Deepfake Detection: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 25494-25513, 2022, doi: 10.1109/ACCESS.2022.3154404. Link: https://ieeexplore.ieee.org/document/9721302

[18]. S. Saif, S. Tehseen, S. S. Ali, S. Kausar and A. Jameel, "Generalized Deepfake Video Detection Through Time-Distribution and Metric Learning," in IT Professional, vol. 24, no. 2, pp. 38-44, 1 March-April 2022, doi: 10.1109/MITP.2022.3168351. Link: https://ieeexplore.ieee.org/document/9770451

[19]. A. Hamza et al., "Deepfake Audio Detection via MFCC Features Using Machine Learning," in IEEE Access, vol. 10, pp. 134018-134028, 2022, doi: 10.1109/ACCESS.2022.3231480. Link: https://ieeexplore.ieee.org/document/9996362

[20]. D. -C. Stanciu and B. Ionescu, "Deepfake Video Detection with Facial Features and Long- Short Term Memory Deep Networks," 2021 International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 2021, pp. 1-4, doi: 10.1109/ISSCS52333.2021.9497385. Link: https://ieeexplore.ieee.org/document/9497385

[21]. H. A. Khalil and S. A. Maged, "Deepfakes Creation and Detection Using Deep Learning," 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, Egypt, 2021, pp. 1-4, doi: 10.1109/MIUCC52538.2021.9447642. Link: https://ieeexplore.ieee.org/document/9447642

[22]. E. Kim and S. Cho, "Exposing Fake Faces Through Deep Neural Networks Combining Content and Trace Feature Extractors," in IEEE Access, vol. 9, pp. 123493-123503, 2021, doi: 10.1109/ACCESS.2021.3110859. Link: https://ieeexplore.ieee.org/document/9531572

[23]. S. P and S. Sk, "DeepFake Creation and Detection:A Survey," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2021, pp. 584-588, doi: 10.1109/ICIRCA51532.2021.9544522. Link: https://ieeexplore.ieee.org/document/9544522

[24]. S. Ramachandran, A. V. Nadimpalli and A. Rattani, "An Experimental Evaluation on Deepfake Detection using Deep Face Recognition," 2021 International Carnahan Conference on Security Technology (ICCST), Hatfield, United Kingdom, 2021, pp. 1-6, doi: 10.1109/ICCST49569.2021.9717407. Link: https://ieeexplore.ieee.org/document/9717407

[25]. I. -J. Yu, S. -H. Nam, W. Ahn, M. -J. Kwon and H. -K. Lee, "Manipulation Classification for JPEG Images Using Multi-Domain Features," in IEEE Access, vol. 8, pp. 210837-210854, 2020, doi: 10.1109/ACCESS.2020.3037735. Link: https://ieeexplore.ieee.org/document/9258899

[26]. T. Jung, S. Kim and K. Kim, "DeepVision: Deepfakes Detection Using Human Eye Blinking Pattern," in IEEE Access, vol. 8, pp. 83144-83154, 2020, doi: 10.1109/ACCESS.2020.2988660. Link: https://ieeexplore.ieee.org/document/9072088

[27]. H. R. Hasan and K. Salah, "Combating Deepfake Videos Using Blockchain and Smart Contracts," in IEEE Access, vol. 7, pp. 41596-41606, 2019, doi: 10.1109/ACCESS.2019.2905689.
Link: https://ieeexplore.ieee.org/document/8668407

[28]. C. Fan and J. Huang, "Federated Few-Shot Learning with Adversarial Learning," 2021 19th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt), Philadelphia, PA, USA, 2021, pp. 1-8, doi: 10.23919/WiOpt52861.2021.9589192. Link: https://ieeexplore.ieee.org/document/9589192

[29]. A. El-Yamany, H. Fouad and Y. Raffat, "A Generic Approach CNN-Based Camera Identification for Manipulated Images," 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 2018, pp. 0165-0169, doi: 10.1109/EIT.2018.8500312. Link: https://ieeexplore.ieee.org/document/8500312

[30]. A. Khodabakhsh, R. Ramachandra, K. Raja, P. Wasnik and C. Busch, "Fake Face Detection Methods: Can They Be Generalized?," 2018 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2018, pp. 1-6, doi: 10.23919/BIOSIG.2018.8553251. Link: https://ieeexplore.ieee.org/document/8553251

[31]. L. Jiang, R. Li, W. Wu, C. Qian and C. C. Loy, "DeeperForensics-1.0: A Large-Scale Dataset for Real-World Face Forgery Detection," 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR),

Seattle, WA, USA, 2020, pp. 2886-2895, doi: 10.1109/CVPR42600.2020.00296. Link: https://ieeexplore.ieee.org/document/9156686

[32]. D. Yorioka, H. Kang and K. Iwamura, "Data Augmentation For Deep Learning Using Generative Adversarial Networks," 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE), Kobe, Japan, 2020, pp. 516-518, doi: 10.1109/GCCE50665.2020.9291963. Link: https://ieeexplore.ieee.org/document/9291963

[33]. T. Jung, S. Kim and K. Kim, "DeepVision: Deepfakes Detection Using Human Eye Blinking Pattern," in IEEE Access, vol. 8, pp. 83144-83154, 2020, doi: 10.1109/ACCESS.2020.2988660.
Link: https://ieeexplore.ieee.org/document/9072088

[34]. D. Güera 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, doi: 10.1109/AVSS.2018.8639163. Link: https://ieeexplore.ieee.org/document/8639163

[35]. S. Girgis, E. Amer and M. Gadallah, "Deep Learning Algorithms for Detecting Fake News in Online Text," 2018 13th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 2018, pp. 93-97, doi: 10.1109/ICCES.2018.8639198. Link: https://ieeexplore.ieee.org/document/8639198

[36]. E. R. S. de Rezende, G. C. S. Ruppert and T. Carvalho, "Detecting Computer Generated Images with Deep Convolutional Neural Networks," 2017 30th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI), Niteroi, Brazil, 2017, pp. 71-78, doi: 10.1109/SIBGRAPI.2017.16. Link: https://ieeexplore.ieee.org/document/8097296

[37]. Y. -G. Kim and X. -P. Huynh, "Discrimination Between Genuine Versus Fake Emotion Using Long-Short Term Memory with Parametric Bias and Facial Landmarks," 2017 IEEE International Conference on Computer Vision Workshops (ICCVW), Venice, Italy, 2017, pp. 3065-3072, doi: 10.1109/ICCVW.2017.362. Link: https://ieeexplore.ieee.org/document/8265573