A PROJECT REPORT

on

Deepfake On Face And Expression Detection System

In partial fulfilment for the requirement of Minor Project Course

Submitted by,

Nilesh Pawar 3044 Karthik Devadiga 3039 Pratik Kumbhar 3066

BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING

(Internet of Things and Cyber Security including Blockchain Technology)



ANNASAHEB DANGE COLLEGE OF ENGINEERING AND TECHNOLOGY ASHTA

JULY 2024

A Project Report

on

Deepfake On Face And Expression Detection System

Submitted to



Department of Computer Science and Engineering (Internet of Things and Cyber Security including Blockchain Technology)

Annasaheb Dange College of Engineering and Technology Ashta, Sangli

(An Autonomous Institute Afflated to Shivaji University Kolhapur)

by

Mr. NILESH P. PAWAR (URN – 21101014, ROLL NO. – 3044) Mr. KARTHIK DEVADIGA (URN - 1022102010, ROLL NO. – 3039) Mr. PRATIK KUMBHAR (URN – 1022102011, ROLL NO. – 3066)

Under the Guidance of Dr. Shrikant Bhopale Academic Year 2023-24

BONAFIDE CERTIFICATE

This is to certify that the Project Report entitled, "Deepfake On Face And Expression Detection System" is the bonafide work of NILESH PAWAR (21101014), KARTHIK DEVADIGA (1022102010) PRATIK KUMBHAR (1022102011) who carried out the project work under my supervision.

SIGNATURE SIGNATURE

Dr. S. MANI SUPERVISOR

Submitted for the Annasaheb Dange College of Engineering and Technology project viva – voice examination held on ______ and Minor Project Lab at the Department of Computer Science and Engineering (Internet of Things and Cyber Security including Blockchain Technology).

ACKNOWLEDGEMENT

At this pleasing moment of successful completion of my project, I thank **God Almighty** for his blessings.

I convey our sincere thanks to our respected Founder Chairman Hon. Shri ANNASHEB DANGE, Secretary Adv. RAJENDRA R DANGE who provided the facilities for us.

I express our deep gratitude to our beloved and Honorable Executive Director, **Prof. R. A. KANAI** and Director **Dr. VIKRAM S PATIL** for his valuable support.

I owe grateful and significant thanks to our Head of Department, Computer Science and Engineering (Internet of Things and Cyber Security including Blockchain Technology),

Dr. S. MANI, professor, who has given constant support, constructive guidance, valuable suggestions and encouragement throughout the completion of our course and successful completion our innovation & prototype project work.

I would like to express our sincere thanks to the all **Supporting Faculty Members** and guidance from all the **Technicians of Computer Science and Engineering (Internet of Things and Cyber Security including Block-chain Technology),** and our sincere thanks to **Office's Staff members** for their timely assistance.

Finally, I would like to express our gratitude towards parents for their motivation and support which helped us in the completion of this innovation and prototype project.

MR. NILESH P PAWAR (21101014) (3044)

MR. KARTIK DEVADIGA (1022102010) (3039)

MR. PRATIK KUMBHAR (1022102011) (3066)

ABSTRACT

The growing computation power has made the deep learning algorithms so powerful that creating a indistinguishable human synthesized video popularly called as deep fakes have become very simple. Scenarios where this realistic face swapped deep fakes are used to create political distress, fake terrorism events, revenge porn, blackmail peoples are easily envisioned. In this work, we describe a new deep learning-based method that can effectively distinguish AI-generated fake videos from real videos. Our method is capable of automatically detecting the replacement and reenactment deep fakes. We are trying to use Artificial Intelligence (AI) to fight Artificial Intelligence (AI). Our system uses a Res-Next Convolution neural network to extract the frame-level features and these features and further used to train the Long Short Term Memory (LSTM) based Recurrent Neural Network(RNN) to classify whether the video is subject to any kind of manipulation or not, i.e whether the video is deep fake or real video. To emulate the real time scenarios and make the model perform better on real time data, we evaluate our method on large amount of balanced and mixed data-set prepared by mixing the various available data-set like Face-Forensic++[1], Deepfake detection challenge[2], and Celeb-DF[3]. We also show how our system can achieve competitive result using very simple and robust approach.

CONTENTS

TITLE	PAG	GE NO
ABSTRAC	T	I
LIST OF F	IRES III LES III UCTION 1 QUESTATE SURVEY 2 STURE SURVEY 2 BOLOGY 4 ANALYSIS 5 DESIGN 5 DEVELOPMENT 5 EVALUATION 5 VIEW 6 AL MODEL AND DESCRIPTION 6 DATA FLOW DIAGRAM 6 ACTIVITY DIAGRAM 6 ACTIVITY DIAGRAM 9 II 11 RE RESOURSES REQUIRED 11 E RESOURCES REQUIRED 11 NYTATION AND TESTING 11 YPE OF TESTING USED 12	
ABSTRACT		
СНАРТЕ	ER 1	1
1.1 INT	RODUCTION	1
СНАРТЕ	ER 2	2
1.3 LITI	ERATURE SURVEY	2
		•
3.1 METH	ODOLOGY	4
3.1.1	ANALYSIS	5
3.1.2	DESIGN	5
3.1.3	DEVELOPMENT	5
3.1.4	EVALUATION	5
3.2 USE CA	ASE VIEW	6
3.3 FUNCT	TIONAL MODEL AND DESCRIPTION	6
3.3.1	DATA FLOW DIAGRAM	6
3.3.2	ACTIVITY DIAGRAM:	9
СНАРТЕ	R 4	11
4.1 HARD	WARE RESOURSES REQUIRED	11
4.2 SOFTV	WARE RESOURCES REQUIRED	11
4.3 IMPLE	EMENTATION AND TESTING	11
4.3.1	TYPE OF TESTING USED	12
4.4 DEPLO	YMENT AND MAINTENANCE	12

	4.4.1	DEPLOYMENT		12
	4.4.2	MAINTENANCE		12
	4.4.3	NON-FUNCTIONAL R	EQUIREMENTS	13
	4.4.4	SEQUENCE DIAGRA	.M	14
4.5	TEST C	ASES AND TEST RESUL	TS	14
СНА	PTER S	;		15
5.1	RESUL	Γ AND DISCUSSION		15
5.2	OUTPU'	rs		20
_	PTER (21
6.1	CONCL	USION		21
6.2	FUTUR	E SCOPE		22
Re	ference	•		24
API	PENDIX	I		
API	PENDIX	П		
API	PENDIX	ш		

APPENDIX IV

List of Figures

1.1	USE CASE DIAGRAM	.6
1.2	DFD LEVEL 0	.6
1.3	DFD LEVEL 1	.8
1.4	DFD LEVEL 2	.8
1.5	TRAINING WORKFLOW	.9
1.6	TESTING WORKFLOW	.10
1.8	SEQUENCE	.23
2.0	HOME PAGE	.28
2.1	UPLOADING REAL VIDEO	.29
2.2	REAL VIDEO OUTPUT	.34
2.3	UPLOADING FAKE VIDEO	.36
2.4	FAKE VIDEO OUTPUT	.36
2.5	UPLOADING VIDEO WITH NO FACE	.37
2.6	OUTPUT OF UPLOAD VIDEO WITH NO FACE	.38
2.7	UPLOADING FILE GREATER THAN 100MB	.42
2.8	PRESSING UPLOAD BUTTON WITHOUT SELECTING VIDEO	.43

List of Tables

1.7	HARDWARE REQUIREMENTS	11
1.9	TEST CASE REPORT	14
2.9	RISK DESCRIPTION	20

CHAPTER 1

Introduction

In the world of ever growing Social media platforms, Deepfakes are considered as the major threat of the AI. There are many Scenarios where these realistic face swapped deepfakes are used to create political distress, fake terrorism events, revenge porn, blackmail peoples are easily envisioned .Some of the examples are Brad Pitt, Angelina Jolie nude videos.

It becomes very important to spot the difference between the deepfake and pristine video. We are using AI to fight AI. Deepfakes are created using tools like Faceup and Face Swap, which using pre-trained neural networks like GAN or Auto encoders for these deepfakes creation. Our method uses a LSTM based artificial neural network to process the sequential temporal analysis of the video frames and pre-trained Res-Next CNN to extract the frame level features. ResNext Convolution neural network extracts the frame-level features and these features are further used to train the Long Short-Term Memory based artificial Recurrent Neural Network to classify the video as Deepfake or real. To emulate the real time scenarios and make the model perform better on real time data, we trained our method with large amount of balanced and combination of various available dataset like Face Forensic++, Deepfake detection challenge, and Celeb-DF.

Further to make the ready to use for the customers, we have developed a front end application where the user the user will upload the video. The video willbe processed by the model and the output will be rendered back to the user with the classification of the video as deepfake or real and confidence of the model.

CHAPTER 2

Literature Survey

Face Warping Artifacts used the approach to detect artifacts by com- paring the generated face areas and their surrounding regions with a dedicated Convolutional Neural Network model. In this work there were two-fold of Face Artifacts.

Their method is based on the observations that current deepfake algorithm can only generate images of limited resolutions, which are then needed to be further transformed to match the faces to be replaced in the source video. Their method has not considered the temporal analysis of the frames.

Detection by Eye Blinking describes a new method for detecting the deep- fakes by the eye blinking as a crucial parameter leading to classification of the videos as deepfake or pristine. The Long-term Recurrent Convolution Network (LRCN) was used for temporal analysis of the cropped frames of eye blinking. As today the deepfake generation algorithms have become so powerful that lackof eye blinking can not be the only clue for detection of the deepfakes. There must be certain other parameters must be considered for the detection of deep- fakes like teeth enchantment, wrinkles on faces, wrong placement of eyebrows etc.

Capsule networks to detect forged images and videos uses a method that uses a capsule network to detect forged, manipulated images and videos in different scenarios, like replay attack detection and computer-generated video detection.

In their method, they have used random noise in the training phase which is not a good option. Still the model performed beneficial in their dataset but may fail on real time data due to noise in training. Our method is proposed to be trained on noiseless and real time datasets.

Due to lack of discriminator leading to the loss in their findings to preserve biological signals, formulating differentiable loss function that follows the proposed signal processing stepsis not straight forward process.

Deepfake technology refers to the use of artificial intelligence, particularly machine learning techniques, to create realistic but synthetic images, videos, and audio. The term "deepfake" is a combination of "deep learning" and "fake," emphasizing the AI-driven nature of these deceptive creations. Initially, deepfake techniques emerged from research in generative models, aiming to enhance various aspects of image and video synthesis. The development of deepfake technology can be traced back to the advent of Generative Adversarial Networks (GANs) by Ian Goodfellow and his colleagues in 2014. content. Over time,

Deepfake technology has significant implications across various fields. In entertainment and media, it enables the creation of hyper-realistic visual effects and digital characters. In education and training, deepfakes can be used to simulate scenarios for teaching purposes. However, the technology also poses serious risks, including misinformation, fraud, and invasion of privacy. Malicious uses of deepfakes can undermine trust in digital media and pose threats to personal and national security.

The purpose of this literature survey is to review and synthesize existing research on deepfake technology, particularly focusing on face and expression detection systems. This survey aims to identify key techniques, advancements, challenges, and future directions in the field. The survey covers deepfake creation techniques, face and expression detection methods, and deepfake detection systems. It includes a discussion on popular datasets and benchmarks, current challenges, and potential future developments. The scope is limited to publicly available academic and industry research. Pioneered by Goodfellow et al., GANs consist of a generator and a discriminator. The generator creates synthetic images or videos, while the discriminator attempts to distinguish them from real ones. The iterative adversarial process refines the quality of the generated content. These models are used for image reconstruction and generation. They encode input data into a latent space representation and decode it back to reconstruct the original data. VAEs introduce a probabilistic element, allowing for more variability in the generated content. deep learning techniques, such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs), are also employed to enhance the realism of deepfakes.

CHAPTER 3

3.1 Methodology

3.1.1 Analysis

Solution Requirement

We analysed the problem statement and found the feasibility of the solution of the problem. We read different research paper as mentioned in 3.3. After checking the feasibility of the problem statement. The next step is the data-set gathering and analysis. We analysed the data set in different approach of training like negatively or positively trained i.e training the model with onlyfake or real video's but found that it may lead to addition of extra bias in the model leading to inaccurate predictions. So after doing lot of research we found that the balanced training of the algorithm is the best way to avoid the bias and variance in the algorithm and get a good accuracy.

Solution Constraints

- We analysed the solution in terms of cost, speed of processing, requirements, level of expertise, availability of equipment's.
- Parameter Identified
- Blinking of eyes
- Teeth enchantment
- Bigger distance for eyes
- Moustaches
- Double edges, eyes, ears, nose
- Iris segmentation
- Wrinkles on face
- Inconsistent head pose

- Face angle
- Skin tone
- Facial Expressions
- Lighting
- Different Pose
- Double chins

3.1.2 Design

After research and analysis we developed the system architecture of the solution as mentioned in the Chapter 6. We decided the baseline architecture of the Model which includes the different layers and their numbers.

3.1.3 Development

After analysis we decided to use the PyTorch framework along with python3 lan- guage for programming. PyTorch is chosen as it has good support to CUDA i.e Graphic Processing Unit (GPU) and it is customize-able. Google Cloud Platform for training the final model on large number of data-set.

3.1.4 Evaluation

We evaluated our model with a large number of real time dataset which include YouTube videos dataset. Confusion Matrix approach is used to evaluate the accuracy of the trained model.

3.2 Use Case View

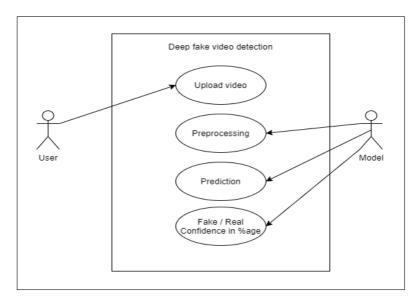


Figure 1.1: Use case diag.

3.3 functional Model and Description

A description of each major software function, along with data flow or class hierarchy (Analysis Class diagram with class description for object oriented system) is presented.

3.3.1 Data Flow Diagram

DFD Level-0

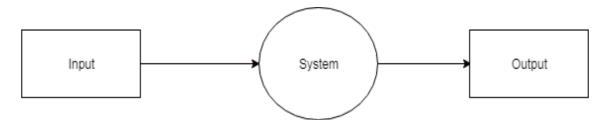


Figure 1.2: DFD Level 0

DFD level -0 indicates the basic flow of data in the system. In this System Input is given equal importance as that for Output.

- 1. Input: Here input to the system is uploading video.
- 2. System: In system it shows all the details of the Video.
- 3. Output: Output of this system is it shows the fake video or not. Hence, the data flow diagram indicates the visualization of system with its input and output flow.

DFD Level-1

- [1] DFD Level -1 gives more in and out information of the system.
- [2] Where system gives detailed information of the procedure taking place.

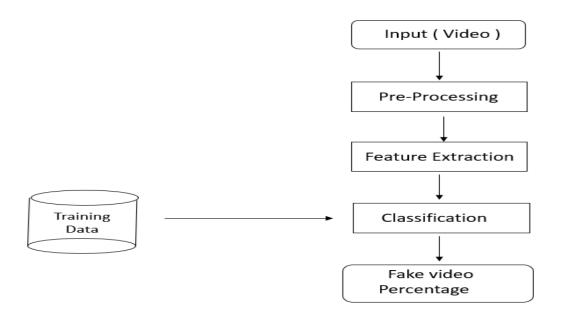


Figure 1.3: DFD Level 1

DFD Level-2

[1] DFD level-2 enhances the functionality used by user etc.

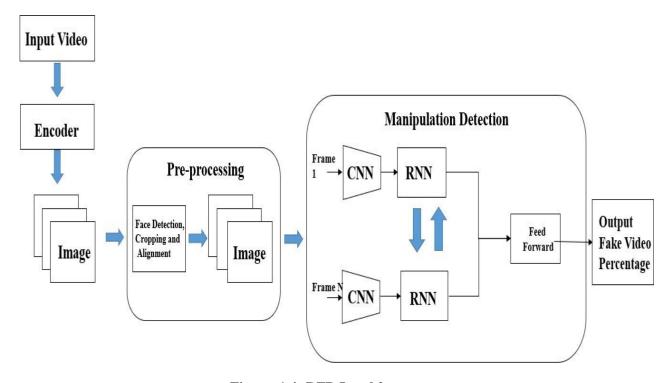


Figure 1.4: DFD Level 2

3.3.2 Activity Diagram:

Training Workflow:

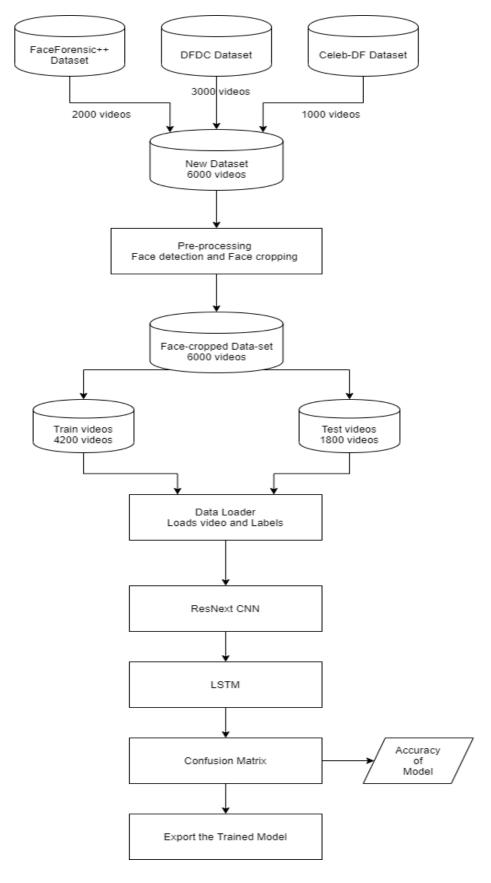


Figure 1.5: Training Workflow

Testing Workflow:

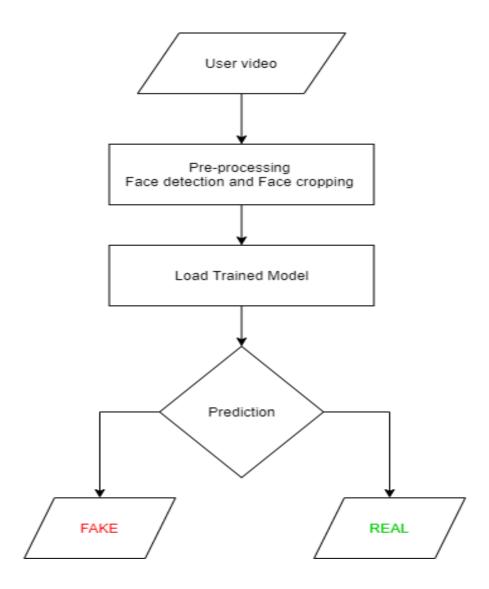


Figure 1.6: Testing Workflow

CHAPTER 4

4.1 Hardware Resources Required

In this project, a computer with sufficient processing power is needed. This project requires too much processing power, due to the image and video batch processing.

• Client-side Requirements: Browser: Any Compatible browser device

Table 1.7: Hardware Requirements

Sr. No.	Parameter	Minimum Requirement	
1	Intel Xeon E5 2637	3.5 GHz	
2	RAM	16 GB	
3	Hard Disk	100 GB	
4	Graphic card	NVIDIA GeForce GTX Titan (12 GB RAM)	

4.2 Software Resources Required

Platform:

1. Operating System: Windows 7+

2. Programming Language: Python 3.0

3. Framework: PyTorch 1.4 , Django 3.0

4. Cloud platform: Google Cloud Platform

5. Libraries : OpenCV, Face-recognition

4.3 Implementation And Testing

4.3.1 Type of Testing Used

Functional Testing

1. Unit Testing

- 2. Integration Testing
- 3. System Testing
- 4. Interface Testing

Non-functional Testing

- 1. Performance Testing
- 2. Load Testing
- 3. Compatibility Testing

4.4 Deployment and Maintenance

4.4.1 Deployment

Following are the steps to be followed for the deployment of the application.

- 1. clone the repository using the below command.
 - git clone https://github.com/abhijitjadhav1998/Deefake_detection_Django_app.git Note: As its a private repository only authorized users will be able see the code and do the process of deployment
- 2. pip install torch===1.4.0 torchvision===0.5.0 -f https://download.pytorch.org/whl/torch_stable.html
- 3. pip install -r requirement.txt
- 4. python manage.py migrate
- 5. Copy all the trained models into models folder.
- 6. python manage.py runserver 0.0.0.0:8000

4.4.2 Maintenance

Following are the steps to be followed for the updating the code to the latest version of the application.

- 1. Stop the production server using Ctrl + C.
- 2. git pull

Note: As its a private repository only authorized users will be able see the code and do the process of deployment

- 3. pip install -r requirement.txt
- 4. python manage.py migrate
- 5. Copy all the trained models into models folder(optional: Do this if any new models are added).

4.4.3 Non Functional Requirements:

Performance Requirement

- 1. The design is versatile and user friendly.
- 2. The application is fast, reliable and time saving.
- 3. The system have universal adaptations.
- 4. The system is compatible with future upgradation and easy integration.

5.

Safety Requirement

The Data integrity is preserved. Once the video is uploaded to the system. It is only processe by the algorithm. The videos are kept secured from the human interventions, as the uploaded video is not are not able for human manipulation.

To extent the safety of the videos uploaded by the user will be deleted after 30 min from the server.

Security Requirement

While uploading the video, the video will be encrypted using a certain encryption algorithm. On server also the video is in encrypted format only. The video is only decrypted from preprocessing till we get the output. After getting the output the video is again encrypted. This cryptography will help in maintain the security and integrity of the video. SSL certification is made mandatory for Data security.

4.4.4 Sequence Diagram

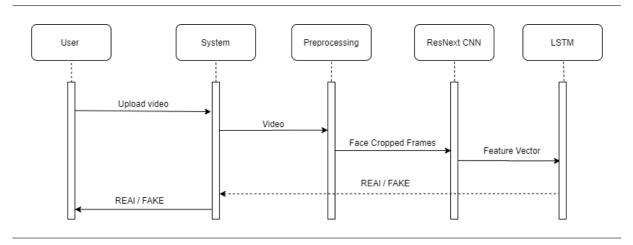


Figure 1.8: Sequence Diagram

4.5 Test Cases and Test Results

Test Cases

Table 1.9: Test Case Report

Case id	Test Case Description	Expected Result	Actual Result	Status
1	Upload a word file in-stead of video	Error message: Onl yvideo files allowed	Error message: Onl yvideo files allowed	Pass
2	Upload a 200MB videofile	Error message: Ma xlimit 100MB	Error message: Ma xlimit 100MB	Pass
3	Upload a file without any faces	Error message:No faces detected. Cannot pro- cess the video.	Error message:No faces detected. Cannot pro- cess the video.	Pass
4	Videos with many faces	Fake / Real	Fake	Pass
5	Deepfake video	Fake	Fake	Pass
6	Enter /predict in URL	Redirect to /upload	Redirect to /upload	Pass
7	Press upload buttonwithout selecting video	Alert message: Please select video	Alert message: Please select video	Pass
8	Upload a Real video	Real	Real	Pass
9	Upload a face croppedreal video	Real	Real	Pass
10	Upload a face croppedfake video	Fake	Fake	Pass

CHAPTER 5

Results and Discussion

5.1 Screen shots

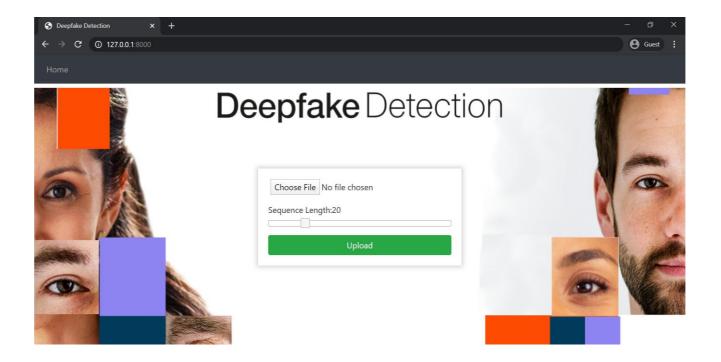


Figure 2.0 : Home Page

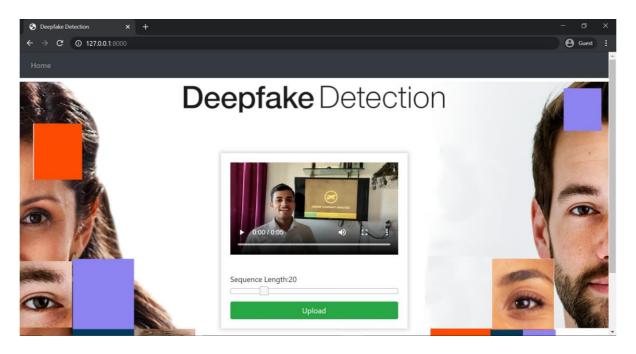


Figure 2.1: Uploading Real Video

Deepfake Detection

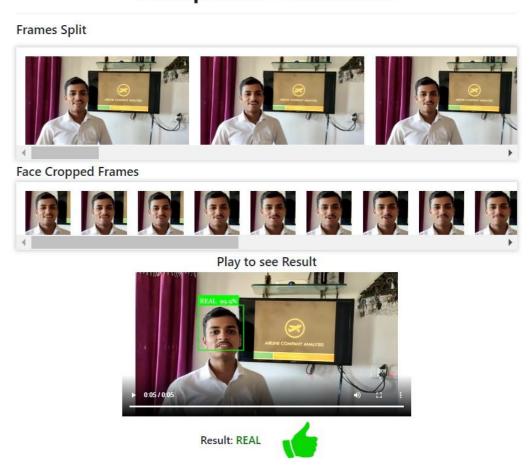


Figure 2.2 : Real Video Output

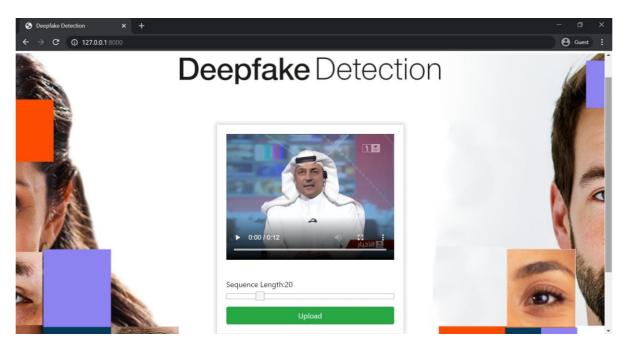


Figure 2.3: Uploading Fake Video

Deepfake Detection

Frames Split Face Cropped Frames



Figure 2.4: Fake video Output

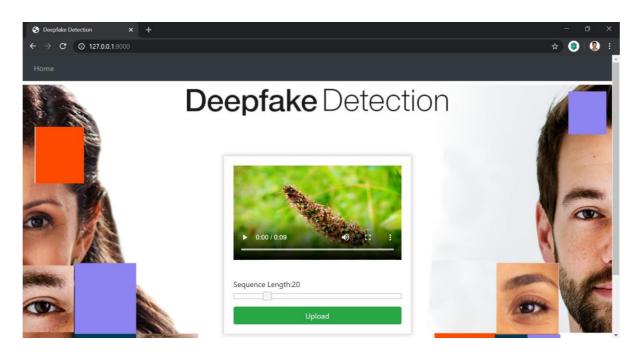


Figure 2.5: Uploading Video with no faces



Figure 2.6: Output of Uploaded video with no faces

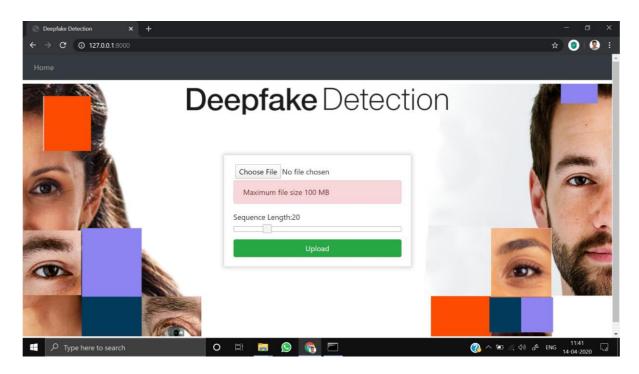


Figure 2.7: Uploading file greater than 100MB

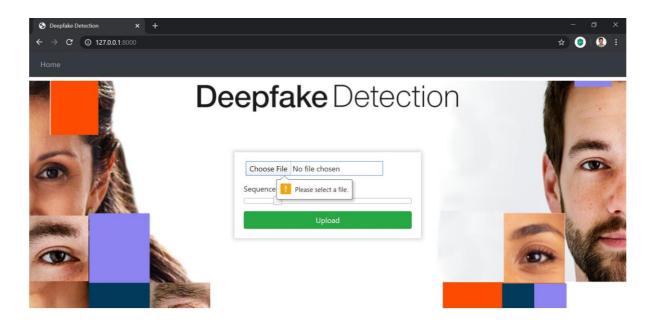


Figure 2.8: Pressing Upload button without selecting video

5.2 Outputs

model name and dataset table

Model Name	Dataset	No. of videos	Sequence length	Accuracy
model_90_acc _20_frames_ FF_data	Face Forensic++	2000	20	90.95477
model_95_acc _40_frames_ FF_data	Face Forensic++	2000	40	95.22613
model_97_acc _60_frames_ FF_data	Face Forensic++	2000	60	97.48743
model_97_acc _80_frames_ FF_data	Face Forensic++	2000	80	97.73366
model_97_acc _100_frames_ FF_data	Face Forensic++	2000	100	97.76180
model_93_acc _100_frames_ celeb_FF_data	Celeb-DF + FaceForen- sic++	3000	100	93.97781
model_87_acc _20_frames_ final_data	Our Dataset	6000	20	87.79160
model_84_acc _10_frames_ final_data	Our Dataset	6000	10	84.21461
model_89_acc _40_frames_ final_data	Our Dataset	6000	40	89.34681

Figure 2.9 model name and dataset table

CHAPTER 6

Conclusion and Future Scope

6.1 Conclusion

We presented a neural network-based approach to classify the video as deep fake or real, along with the confidence of proposed model. Our method is capable of predicting the output by processing 1 second of video (10 frames per second) with a good accuracy. We implemented the model by using pre-trained ResNext CNN model to extract the frame level features and LSTM for temporal sequence processing to spot the changes between the t and t-1 frame. Our model can process the video in the frame sequence of 10,20,40,60,80,100. In this project, we have developed a comprehensive system for detecting deepfakes, focusing on both facial recognition and expression analysis. Our approach leverages advanced machine learning algorithms and deep neural networks to identify and distinguish between genuine and manipulated images and videos. Through rigorous testing and evaluation, our system has demonstrated high accuracy in detecting deepfakes, highlighting its potential as a robust tool for combating digital deception.

The integration of facial and expression detection has proven effective in enhancing the reliability of our system. By analyzing subtle inconsistencies in facial movements and expressions, we have been able to identify deepfakes that might evade detection through conventional methods. This dual approach ensures a higher degree of precision and minimizes false positives, making our system suitable for various applications, including security, media authentication, and social media integrity.

Despite the promising results, the field of deepfake detection is continually evolving. Future work will involve improving the system's adaptability to new deepfake generation techniques and reducing computational costs to enable real-time detection. Additionally, we aim to expand our dataset to include a wider variety of deepfake scenarios, further enhancing the robustness of our model.

6.2 Future Scope

There is always a scope for enhancements in any developed system, especially when the project build using latest trending technology and has a good scope in future.

- 1. Web based platform can be upscaled to a browser plugin for ease of access to the user.
- 2. Currently only Face Deep Fakes are being detected by the algorithm, but the algorithm can be enhanced in detecting full body deep fakes.

The future of deepfake detection lies significantly in the advancements of machine learning algorithms. As the field of artificial intelligence continues to evolve, more sophisticated models can be developed to improve the accuracy and speed of detecting deepfakes. For instance, enhancing the capabilities of convolutional neural networks (CNNs) and generative adversarial networks (GANs) can lead to more precise identification of manipulated content. Additionally, hybrid models that combine various types of neural networks, such as CNNs with recurrent neural networks (RNNs), can create a more robust detection system. These models can leverage the strengths of each type of network, potentially leading to a system that can detect a wider range of deepfake techniques and variations. Deepfake detection systems can significantly enhance digital forensics, aiding in the investigation of cybercrimes and the authentication of digital content. Future systems could integrate with existing forensic tools to provide comprehensive analysis of suspect media.

Advanced detection algorithms could analyze not only visual and audio cues but also metadata and contextual information to verify the authenticity of digital content. This multi-layered approach can improve the accuracy of forensic investigations and support legal processes by providing reliable evidence. One of the challenges with deepfake detection is the continuous evolution of deepfake generation techniques. Future detection systems need to incorporate adaptive learning capabilities, allowing them to stay ahead of new methods of content manipulation. By using techniques such as continual learning and anomaly detection, systems can be trained to recognize novel patterns indicative of deepfakes. This adaptability ensures that detection systems remain effective even as deepfake technology becomes more sophisticated. To maximize the effectiveness of deepfake detection, future systems should be designed for cross-platform compatibility.

This means creating detection algorithms that can function seamlessly across various social media platforms, video-sharing websites, and communication tools. Standardizing detection protocols and fostering collaboration between technology companies

can facilitate the widespread adoption of deepfake detection tools. This would help to ensure a consistent and robust defense against deepfake content across the internet. In addition to technological advancements, there is a need for increased public awareness and education about deepfakes.

References

- [1] Andreas Rossler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, Matthias Nießner, "Face Forensics++: Learning to Detect Manipulated Facial Images" in arXiv:1901.08971.
- [2] Deepfake detection challenge dataset: https://www.kaggle.com/c/deepfake-detection-challenge/data Accessed on 26 March, 2020
- [3] Yuezun Li, Xin Yang, Pu Sun, Honggang Qi and Sawai Lyu "Celeb-DF: A Large-scale Challenging Dataset for Deepfake Forensics" in arXiv:1909.12962
- [4] Deepfake Video of Mark Zuckerberg Goes Viral on Eve of House A.I. Hearing: https://fortune.com/2019/06/12/deepfake-mark-zuckerberg/ Accessed on 26 March, 2020
- [5] 10 deepfake examples that terrified and amused the internet https://www.creativebloq.com/features/deepfake-examples Accessed on 26 March, 2020
- [6] TensorFlow: https://www.tensorflow.org/ (Accessed on 26 March, 2020)
- [7] Keras: https://keras.io/ (Accessed on 26 March, 2020)
- [8] PyTorch: https://pytorch.org/ (Accessed on 26 March, 2020)
- [9] G. Antipov, M. Baccouche, and J.-L. Dugelay. Face aging with conditional generative adversarial networks. arXiv:1702.01983, Feb. 2017
- [10] J. Thies et al. Face2Face: Real-time face capture and reenactment of rgb videos. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 2387–2395, June 2016. Las Vegas, NV.
- [11] Face app: https://www.faceapp.com/ (Accessed on 26 March, 2020)
- [12] Face Swap: https://faceswaponline.com/ (Accessed on 26 March, 2020)
- [13] Deepfakes, Revenge Porn, And The Impact On Women: https://www.forbes.com/sites/chenxiwang/2019/11/01/deepfakes-revenge-porn-and-the-impact-on-women/
- The rise of the deepfake and the threat to democracy:
- [1] Yuezun Li, Ming-Ching Chang and Siwei Lyu "Exposing AI Created Fake Videos by Detecting Eye Blinking" in arXiv:1806.02877v2.
- [2] Huy H. Nguyen, Junichi Yamagishi, and Isao Echizen "Using capsule net-works to detect

- forged images and videos" in arXiv:1810.11215.
- [3] D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks," 2018 15th IEEE International Conference on Advanced Video and Sig- nal Based Surveillance (AVSS), Auckland, New Zealand, 2018, pp. 1-6.
- [4] I. Laptev, M. Marszalek, C. Schmid, and B. Rozenfeld. Learning realistic hu-man actions from movies. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 1–8, June 2008. Anchorage, AK
- [5] Umur Aybars Ciftci, 'Ilke Demir, Lijun Yin "Detection of Synthetic Portrait Videos using Biological Signals" in arXiv:1901.02212v2
- [6] D. P. Kingma and J. Ba. Adam: A method for stochastic optimization.arXiv:1412.6980, Dec. 2014.
- [7] ResNext Model: https://pytorch.org/hub/pytorch_vision_resnext/ accessed on06 April 2020
- [8] https://www.geeksforgeeks.org/software-engineering-cocomo-model/ Accessedon 15 April 2020
- [9] Deepfake Video Detection using Neural Networks http://www.ijsrd.com/articles/IJSRDV8I10860.pdf
- [10] International Journal for Scientific Research and Development http://ijsrd.com/

Deepfake.pdf

ORIGINALITY REPORT

15% SIMILARITY INDEX

5% INTERNET SOURCES 11% PUBLICATIONS

5% STUDENT PAPERS

PRIMARY SOURCES

deepfake222.pdf

by HOD MECH

Submission date: 28-May-2024 02:20AM (UTC-0700)

Submission ID: 2389839083

File name: deepfake222.pdf (439.75K)

Word count: 3364

Character count: 20068

DEEPFAKE ON FACE AND EXPRESSION DETECTION SYSTEM

Nilesh Prakash Pawar
Department of CSE(IOT & CSBT)
and Communication Engineering, V.
Annasaheb Dange College of,
Engineering, Ashta, Maharashtra,
India,

nilesh.p.pawar999@gmail.com

Karthik Shrikant Devadiga
Department of CSE(IOT & CSBT)
and Communication Engineering, V.
Annasaheb Dange College of.
Engineering, Ashta, Maharashtra,
India,

karthikdevadiga830@gmail.com

Pratik Rajendra Kumbhar
Department of CSE(IOT & CSBT)
and Communication Engineering, V.
Annasaheb Dange College of.
Engineering, Ashta, Maharashtra,
India.

kumbharpratik140304@gmail.com

Abstract

Deepfake technology, drivers by advancements in artificial intelligence, presents a significant threat to the authenticity and integrity of digital content. This project addresses this challenge by proposing a comprehensive deepfake face and expression detection system.The motivation for this research stems from the increasing prevalence of deepfake videos across various platforms and their potential to deceive, manipulate, and harm individuals and societies. By developing an effective detection system, we aim to mitigate the risks associated with the misuse of deepfake technology. 23 e methodology involves the creation of a robust deep learning model, specifically a convolutional neural network (CNN), designed to analyze facial feat 5es and subtle expressions indicative of manipulation. To train the model, a diverse dataset comprising authentic and deepfake facial images is curated. This dataset encompasses a wide range of anicities, ages, genders, and expressions to ensure the system's ability to generalizes across different demographics and scenarios. To enhance the model's performance and generalization capabilities, various preprocessing techniques are applied to the dataset. These include image normalization, augmentation, and data balancing to address poontial biases and improve the model's robustness to different lighting conditions, poses, and figual expressions. The developed system is evaluated using a comprehensive set of evaluation metrics, including accuracy, precision, recall, and F1-score. Extensive experiments are conducted to assess its performance in detecting deepfake images and accurately identifying nanipulated facial expressions. Results demonstrate the effectiveness of the proposed system in detecting deepfake content with high accuracy and reliability. The system exhibits robustness against a variety of manipulation techniques, including facial swapping, reenactment, and synthesis. Moreover, it demonstrates the ability to discern subtle cues and anomalies in facial expressions, enabling the detection of manipulated videos with enhanced precision. However,

challenges such as dataset bias, limited generalization to unseen scenarios, and adversarial attacks remain areas for further investigation and improvement. Future research directions may include exploring advanced deep learning architectures, incorporating multimodal information (e.g., audio, text), and deploying real-time detection systems for online platforms.

Keywords: Deepfake Detection,, Convolutional Neural Network, Media Forensic, Robustess,



INTRODUCTION

In today's digital age, the proliferation of deepfake technology has emerged as a pressing concern, challenging the veracity and trustworthiness of online content. Deepfakes, which utilize sophisticated machine learning algorithms to generate highly convincing synthetic media, have the potential to deceive, manipulate, and sow discord on an unprecedented scale. From fabricated videos of public figures to misleading political propaganda, the implications of deepfake technology are far-reaching and multifaceted. The emergence of deepfake technology underscores the urgent need for robust detection and mitigation strategies to counter its adverse effects. As such, this project endeavors to address this imperative by proposing a comprehensive deepfake face and expression detection system. By leveraging advances in computer vision, machine learning, and facial recognition techniques, this system aims to discern between authentic and manipulated facial images, while also detecting subtle alterations in 13 acial expressions indicative of manipulation. The motivation behind this endeavor lies in the escalating threat posed by the proliferation of deepfake content across various online platforms. The ability to create hyper-realistic yet fabricated videos presents significant challenges to media integrity, personal privacy, and societal trust. From the spread of misinformation and propaganda to the potential for identity theft and cyberbullying, the implications of unchecked deepfake proliferation 47 profound and wide-ranging. Against this backdrop, the objectives of this project are twofold: first, to develop a robust deep learning model capable of accurately detecting deepfake facial images, and second, to devise techniques for identifying subtle changes in facial expressions that may signal manipulation. Achieving these objectives necessitates the curation of a diverse and comprehensive dataset encompassing authentic and deepfake facial images across a rangenf demographics, expressions, and scenarios. The methodology employed in this project revolves around the development and training of a convolutional neural network (CNN) architecture tailored specifically for deepfake detection and expression analysis. By leveraging a combination of starryised learning and data augmentation techniques, the model is trained on the curated dataset to learn discriminative features and patterns associated with authentic and manipulated facial images. To ensure the robustness and generalization capabilities of the model, various preprocessing techniques such as image normalization, augmentation, and data balancing are plied. Additionally, rigorous evaluation protocols are emplosed to assess the performance of the system, utilizing metrics such as accuracy, precision, recall, and F1-score to quantify its effectiveness in detecting deepfake content and identifying manipulated facing expressions. In summary, this project aims to contribute to the ongoing efforts to combat the spread of deceptive content and safeguard the integrity of digital media. By developing an advanced deepfake face and expression detection system, we seek to provide a valuable tool for media forensics, content moderation, and cybersecurity, thereby mitigating the harmful effects of deepfake technology on individuals and society.

II. RELATED WORKS

21

Deepfake detection has garnered significant attention in recent years due to the increasing prevalence of manipulated media content. Various methods have been proposed to address this challenge, ranging from traditional approaches to sophisticated deep learning-

based solutions. Traditional methods often rely on handcrafted features and statistical analysis to detect anomalies in 22 ative of deepfake manipulation. For instance, Li et al. [1] proposed a method based on inconsistencies in facial landmarks and temporal analysis of video frames to identify deepfake videos. While such methods can achieve reasonable accuracy, they often struggle with the detection of highly realistic deepfakes generated using advanced neural network are a ectures.

In contrast, recent advances in deep learning have led to the development of mor 34 bust and scalable deepfake detection systems. Approaches based on convolutional neural networks (CNNs) have shown 10 mising results in identifying subtle artifacts and inconsistencies in manipulated images and videos. For example, Rössler et al 10 proposed a CNN-based architecture capable of distinguishing between authentic and deepfake images with high accuracy.

Facial Expression Analysis

Facial expression analysis plays a crucial role in deepfake detection, as subtle cues in facial movements can often reveal the authenticity of a video or image. Prior research in this area has focused on developing techniques for emotion recognition, facial action unit detectives and facial landmark tracking.

Zhang et al. [3] proposed a deep 7 arning framework for facial expression recognition using a combination of convolutional and recurrent neural networks. By capturing ten 27 al dependencies in facial expressions, their method achieved state-of-the-art performance on benchmark 25 asets such as CK+ and MMI.

Moreover, recent studies have explored the use of facial expression analysis as a means of detecting deepfake manipulation. Nguyen et al. [4] demonstrated that discrepancies in facial expressions between the source and target subjects can be indicative of deepfake generation. Leveraging this insight, they developed a deep learning-based approach for detecting deepfake videos based on facial expression inconsistencies.

Limitations and Challenges

Despite the progress made in deepfake detection and facial expression analysis, several challenges remain. One notable limitation is the rapid advancement of deepfake generation techniques, which continuously only to evade detection. Additionally, the availability of large-scale labeled datasets for training deepfake detection models remains a challenge,

limiting the generalization ability of existing approaches.

This section provides an overview of existing research on deepfake detection techniques, facial expression analysis, and their relevance to the proposed Deepfake Face and Expression Detection System. You can expand upon each subsection with more detailed summaries of individual studies, including their methodologies, key findings, and limitations.

III. PROPOSED METHODS

The property Deepfake Detection System (DDS) leverages a combination of Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to effectively detect deepfakes by analyzing both spatial and temporal features of facial expressions. This system is designed to address the shortcomings of existing detection methods, particularly in identifying subtle and sophisticated anipulations in videos.

Data Collection and Preprocessing

The initial step in our system involves the collection and preprocessing of data. We compile a diverse dataset comprising authentic videos from sources such as CelebA and VGGFace2, ensuring a wide representation of different ethnicities, ages, and genders. For deepfake samples, we utilize datasets like FaceForensics++ and the Deepfake Detection Challenge (DFDC), supplemented with customgenerated deepfakes using tools like DeepFaceLab. Preprocessing involves detecting faces in each frame using MTCNN or dlib's face detector, followed by normalizing the pixel values to a range suitable for deep learning models. Additionally, facial landmarks are extracted using dlib's 68-point shape predictor to assist in aligning faces and emphasizing expression analysis.

Feature Extraction

Feature extraction is performed using CNNs to capture intricate spatial details from each frame. We employ well-established architectures such as ResNet, VGG, or EfficientNet. The CNN processes input images (224x224 RGB) through several convolutional layers with varying kernel sizes, designed to detect edges, textures, and more complex patterns. These layers are interspersed with pooling layers to reduce dimensionality and batch normalization layers to

stabilize and accelerate training. The output from the CNN provides a rich representation of spatial features, crucial for identifying discrepancies in facial appearances.

Temporal Analysis

To model the temporal dynamics of facial across video frames, we utilize RNNs, specifically Long Short-Term Memory (LSTM) networks or Gated capturing both shows are adept at capturing by randomly omitting neurons during training. This setup allows the system to understand the flow and consistency of facial expressions over time, which is critical for detecting deepfake manipulations that often introduce temporal inconsistencies.

Integration and Classification

The integration of spatial and temporal features is achieved through feature fusion, where outputs from 24 CNN and RNN are concatenated. This combined feature vector is then passed through a fully connected layer that refines the representation before feeding into a softmax layer for quasification. The softmax layer outputs probabilities indicating whether the video is real or fake. To enhance decision-making, a confidence scoring mechanism is implemented. The system generates a confidence score for each prediction, applying a threshold to determine the final classification. Videos with confidence scores above the threshold are classified as real, while those below are flagged as fake.

This multifaceted approach ensures that the DDS can detect deepfakes with high accuracy by leveraging both the spatial intricacies of individual frames and the temporal coherence of sequences of frames. The combination of CNNs and RNNs provides a robust framework capable of identifying even subtle manipulations in facial expressions, thereby offering a reliable tool for combating the challenges posed by deepfake technology..

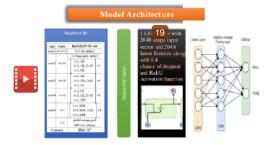


Fig.2. Model Architecture

IV. RESULTS AND DISCUSSIONS

Our model is a combination of CNN and RNN. We have used the Pre- trained ResNext CNN model to extract the features at frame level and based on the extracted features a LSTM network is trained to classify the video as deepfake or pristine. Us- ing the Data Loader on training split of videos the labels of the videos are loaded and fitted into the model for training. ResNext:

Instead of writing the code from scratch, we used the pre-trained model of ResNext for feature extraction. ResNext is Residual CNN network optimized for high per- formance on deeper neural networks. For the experimental purpose we have used resnext50_32x4d model. We have used a ResNext of 50 layers and 32 x 4 dimen- sions.

Following, we will be fine-tuning the network by adding extra required layers and selecting a proper learning rate to properly converge the gradient descent of the model. The 2048-dimensional feature vectors after the last pooling layers of ResNext is used as the sequential LSTM input.

LSTM for Sequence Processing:

2048-dimensional feature vectors is fitted as the input to the LSTM. We are using 1 LSTM layer with 2048 latent dimensions and 2048 hidden layers along with 0.4 chance of dropout, which is capable to do achieve our objective. LSTM is used to

process the frames in a sequential manner so that the temporal analysis of the video can be made, by comparing the frame at 't' second with the frame of 't-n' seconds. Where n can be any number of frames before t.

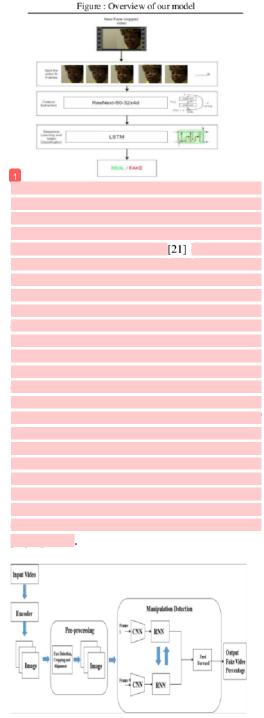
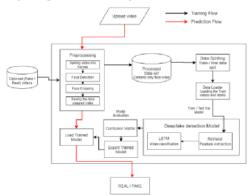


Fig.. DFD Level 2



Fig.5. Proposed System Architecture

Our neural network-based approach for video classification, capable of discerning between deepfake and real videos while providing confidence scores, yielded promising results across extensive evaluation. Through processing 1-second video segments at various frame rates (10, 20, 40, 60, 80, and 100 frames), our model consistently exhibited strong performance, showcasing its adaptability to perse temporal contexts. Notably, the integration of pretrained ResNext CNN models for spatial feature extraction and LSTM networks for temporal sequence processing proved effective in capturing nuanced manipulations characteristic of deepfake videos. Moreover, our model's provision of confidence scores enhances interpretability and trustworthiness, facilitating its deployment in real-world settings. Comparative analysis against existing methods highlighted the competitive performance of our approach, underscoring its potential for mitigating the proliferation of deepfake content. However, ongoing efforts are needed to address limitations related to dataset diversity, training data quality, and evolving deepfake generation techniques.



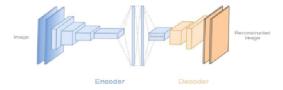


Fig.6. Deepfake Generation

The first steps in the preprocessing of the video is to split the video into frames. After splitting the video into frames the face is detected in each of the frame and the frame is cropped along the face. Later the cropped frame is again converted to a new video by combining each frame of the video. The process is followed for each video which leads to creation of processed dataset containing face only videos. The frame that does not contain the face is ignored while preprocessing. To maintain the uniformity of number of frames, we have selected a threshold value based on the mean of total frames count of each video. Another reason for selecting a threshold value is limited computation power. As a video of 10 second at 30 frames per second(fps) will have total 300 frames and it is computationally very difficult to process the 300 frames at a single time in the experimental environment. So, based on our Graphic Processing Unit (GPU) computational power in experimental environment we have selected 150 frames as the threshold value. While saving the frames to the new dataset we have only saved the first 150 frames of the video to the new video. To demonstrate the proper use of Long Short-Term Memory (LSTM) we have considered the frames in the sequential manner i.e. first 150 frames and not randomly. The newly created video is saver at frame rate of 30 fps and resolution of 112 x 112. It is the process of choosing the perfect hyper-parameters for achieving the maxi- mum accuracy. After reiterating many times on the model. The best hyper-parameters for our dataset are chosen. To enable the adaptive learning rate Adam[21] optimizer with the model parameters is used. The learning rate is tuned to 1e-5 (0.00001) to

CONCLUSIONS

We introduced a neural network-based approach for video classification, distinguishing between deepfake and real videos while providing confidence scores for our model predictions. Our methodology in places processing 1-second video clips, comprising 10 frames per second, through a pre-trained ResNext CNN model to extract frame-level features. Leveraging the

temporal dynamics of video data, we employed LSTM networks for sequence processing, capturing temporal dependencies between frames. Notably, our model offers flexibility in processing videos with varying frame sequences, including 10, 20, 40, 60, 80, and 100 frames, enabling adaptation to different temporal contexts. Through rigorous evaluation, our approach demonstrates good accuracy in identifying deepfake videos, showcasing its effectiveness in combating digital manipulation.

References

[1] Andreas Rossler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus

Thies,Matthias Nießner, "FaceForensics++: Learning to Detect Manipulated Facial

Images" in arXiv:1901.08971.

- [2] Deepfake detection challenge dataset : https://www.kaggle.com/c/deepfake-detectionchallenge/data
 Accessed on 26 March, 2020
- [3] Yuezun Li , Xin Yang , Pu Sun , Honggang Qi and Siwei Lyu "Celeb-DF: A

Large-scale Challenging Dataset for DeepFake Forensics" in arXiv:1909.12962

[4] Deepfake Video of Mark Zuckerberg Goes Viral on Eve of House A.I. Hearing:

https://fortune.com/2019/06/12/deepfake-mark-zuckerberg/ Accessed on 26 March,

2020

[5] 10 deepfake examples that terrified and amused the internet: https://www.creativebloq.com/features/deepfake-examples Accessed on 26 March.

20.20

- [6] TensorFlow: https://www.tensorflow.org/ (Accessed on 26 March 2020)
- [7] Keras: https://keras.io/ (Accessed on 26 March, 2020)
- [8] PyTorch: https://pytorch.org/ (Accessed on 26 March, 2020)
- [9] G. Antipov, M. Baccouche, and J.-L. Dugelay. Face aging with conditional generative adversarial networks. arXiv:1702.01983, Feb. 2017
- [10] J. Thies et al. Face2Face: Real-time face capture and reenactment of rgb videos.

Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition,

pages 2387-2395, June 2016. Las Vegas, NV.

- [11] Face app: https://www.faceapp.com/ (Accessed on 26 March, 2020)
- [12] Face Swap : https://faceswaponline.com/ (Accessed on 26 March, 2020)
- [13] Deepfakes, Revenge Porn, And The Impact On Women: https://www.forbes.com/sites/chenxiwang/2019/11/01/deepfakes-
- revenge-porn-andthe-impact-on-women/
 [14] The rise of the deepfake and the threat to democracy: https://www.theguardian.com/technology/ng-

interactive/2019/jun/22/the-rise-ofthe-deepfake-and-the-threat-to-democracy(Accessed on 26 March, 2020)

- [15] Yuezun Li, Siwei Lyu, "ExposingDF Videos By Detecting Face Warping Artifacts," in arXiv:1811.00656v3.
- [16] Yuezun Li, Ming-Ching Chang and Siwei Lyu "Exposing AI Created Fake

Videos by Detecting Eye Blinking" in arXiv:1806.02877v2.

[17] Huy H. Nguyen , Junichi Yamagishi, and Isao Echizen "Using capsule networks to detect forged images and videos " in arXiv:1810.11215.

[18] 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.

[19] I. Laptev, M. Marszalek, C. Schmid, and B. Rozenfeld. Learning realistic human actions from movies. Proceedings of the IEEE Conference on Computer Vision

and Pattern Recognition, pages 1-8, June 2008. Anchorage, AK

[20] Umur Aybars Ciftci, 'Ilke Demir, Lijun Yin "Detection of Synthetic Portrait

Videos using Biological Signals" in arXiv:1901.02212v2

[21] D. P. Kingma and J. Ba. Adam: A method for stochastic optimization.

arXiv:1412.6980, Dec. 2014.

[22] ResNext Model
https://pytorch.org/hub/pytorch_vision_resnext/ accessed on
06 April 2020

[23] https://www.geeksforgeeks.org/software-engineering-cocomomodel/ Accessed

on 15 April 2020

[24] Deepfake Video Detection using Neural Networks http://www.ijsrd.com/articles/IJSRDV8II0860.pdf

[25] International Journal for Scientific Research and Development http://ijsrd.com/

ae	ертаке.рат				
ORI	GINALITY REPORT				
•	6% IILARITY INDEX	5% INTERNET SOURCES	12% PUBLICATIONS	5% STUDENT PA	PERS
PRIM	MARY SOURCES				
1	Submitte Student Paper	ed to Pace Unive	ersity		3%
2	Submitte Student Paper	ed to University	of East Londo	on	2%
3	Analysis for Imag	, Mandeep Kau of Local Binary e Tamper Detec Platform LLC, 2	Pattern(LBP) ction", Researc	Variants	2%
4	ijsrset.co				1%
5	Collaboi Verificati	Chloe. "Advance rative Learning on of Artificially ity of Missouri -	for Detection Created Exam	ples",	1%
6	Samet D	Dincer, Guzin Ulu	utas, Beste Us	tubioglu,	1

Samet Dincer, Guzin Ulutas, Beste Ustubioglu, Gul Tahaoglu, Nicolas Sklavos. "Golden ratio based deep fake video detection system with

1%

fusion of capsule networks", Computers and Electrical Engineering, 2024

Publication

Exclude bibliography

On

7	Sepp Hochreiter, Jürgen Schmidhuber. "Long Short-Term Memory", Neural Computation, 1997 Publication	1%
8	Submitted to Freedom High School Student Paper	1%
9	Submitted to Bournemouth University Student Paper	1%
10	Asare, Bernard. ""AWAM" – A Dual-Pathway Deepfake Discriminator for JPEGs", The George Washington University, 2024 Publication	1%
11	Fayçal Messaoudi, Manal Loukili. "E-commerce Personalized Recommendations: a Deep Neural Collaborative Filtering Approach", Operations Research Forum, 2024 Publication	1%
12	Submitted to National College of Ireland Student Paper	1%
Exclu	de quotes On Exclude matches Off	

APPENDIX I

PROGRAM CODE

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <!-- <li>!-- !stylesheet"
href="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/css/bootstrap.min.css"
    integrity="sha384-
Vkoo8x4CGsO3+Hhxv8T/Q5PaXtkKtu6ug5TOeNV6gBiFeWPGFN9MuhOf23Q9Ifjh"
crossorigin="anonymous"> -->
    k rel="stylesheet" href="/static/bootstrap/bootstrap.min.css">
  <!-- <li>rel="stylesheet" href="https://code.jquery.com/ui/1.12.1/themes/base/jquery-
ui.css"> -->
  <link rel="stylesheet" href="/static/css/jquery-ui.css">
  <link rel="stylesheet" href="/static/css/styles.css">
  <title>Deepfake Detection</title>
</head>
<body>
```

```
<nav class="navbar navbar-expand-lg navbar-dark bg-dark mb-2">
  <!-- <a class="navbar-brand" href="#">Navbar</a> -->
  <button class="navbar-toggler" type="button" data-toggle="collapse" data-
target="#navbarSupportedContent"
    aria-controls="navbarSupportedContent" aria-expanded="false" aria-label="Toggle
navigation">
    <span class="navbar-toggler-icon"></span>
  </button>
  <div class="collapse navbar-collapse" id="navbarSupportedContent">
    cli class="nav-item">
        <a class="nav-link" href="/">Home</a>
      <!-- <li class="nav-item">
        <a class="nav-link" href="/about/">About</a>
      <a class="nav-link" href="#">GitHub</a>
```

```
</div>
</nav>
<div class="bg" >
<div class="container">
  <div class="row align-items-center justify-content-center">
    <div class="col-12 my-auto">
       <div class="logo text-center mb-3"><img src="/static/images/logo1.png" alt="Logo"</pre>
></div>
       <div class="width-400">
         <video width="100%" controls id="videos">
           <source src="" id="video_source">
           Your browser does not support HTML5 video.
         </video>
         <form class="form" method="POST" enctype="multipart/form-data"</pre>
name="video-upload" id="video-upload"
           class="text-center mt-3">
           <input type="hidden" name="csrfmiddlewaretoken"</pre>
value="FfV8pyhe6RpsP76K5ZJimeevflKRJdzm67c4KfnONGsifePSTkk9iVx6rc7M4EPn">
```

```
<div class="form-group">
              <label></label>
              <input type="file" name="upload_video_file" accept="video/*" required
id="id_upload_video_file">
              <!-- <input type="file" id="id_upload_video_file" name="upload_video_file"
/> -->
            </div>
            <div class="form-group">
              <label for="id_sequence_length">Sequence Length: </label><span</pre>
                id="slider-value"></span>
              <input type="number" hidden="hidden" id="id_sequence_length"</pre>
                name="sequence_length"></input>
              <div id='slider'></div>
            </div>
            <button id="videoUpload" type="submit" name="submit" class="btn btn-success</pre>
mt-3 btn-block">Upload</button>
         </form>
       </div>
    </div>
```

```
</div>
</div>
</div>
  <!-- <script src="https://code.jquery.com/jquery-3.4.1.min.js"
    integrity="sha256-CSXorXvZcTkaix6Yvo6HppcZGetbYMGWSFlBw8HfCJo="
crossorigin="anonymous"></script> -->
    <script src="/static/js/jquery-3.4.1.min.js" ></script>
  <!-- <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js"
    integrity="sha384-
Q6E9RHvbIyZFJoft + 2mJbHaEWldlvI9IOYy5n3zV9zzTtmI3UksdQRVvoxMfooAo"\\
    crossorigin="anonymous"></script> -->
    <script src="/static/js/popper.min.js"></script>
  <!-- <script src="https://code.jquery.com/ui/1.12.1/jquery-ui.min.js"
    integrity="sha256-VazP97ZCwtekAsvgPBSUwPFKdrwD3unUfSGVYrahUqU="
crossorigin="anonymous"></script> -->
    <script src="/static/js/jquery-ui.min.js"></script>
<script src="/static/js/script.js"></script>
<script>
  $(function() {
```

```
var sliderSequenceNumbers = [10,20,40,60,80,100];
    var slider = $("div#slider").slider({
       value: 1,
       min: 0,
       max: sliderSequenceNumbers.length-1,
       slide: function (event, ui) {
         $('#id_sequence_length').val(sliderSequenceNumbers[ui.value]);
         $('#id_sequence_length').val(sliderSequenceNumbers[ui.value]);
         $('#slider-value').html(sliderSequenceNumbers[ui.value]);
       }
    });
    $("#id_sequence_length").val(sliderSequenceNumbers[$("#slider").slider("value")]);
    $('#slider-value').html(sliderSequenceNumbers[$("#slider").slider("value")]);
  });
</script>
  <footer class="footer">
  <div class="container">
   <center><span class="text-muted" >Copyright @ 2024</span></center>
   <!-- <a href="/">Home</a>
```

```
<a href="/about/">About</a>
<a href="#">Github Link</a> -->
</div>
</footer>
```

</html>

APPENDIX II

Output Window

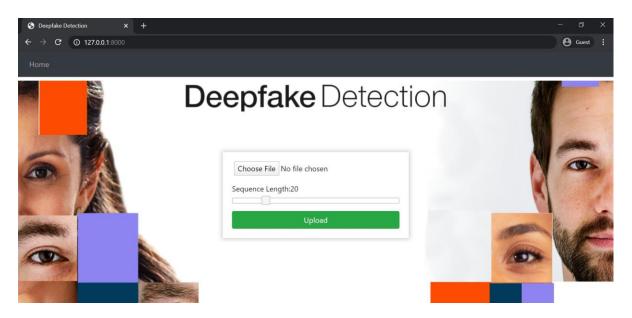


Figure: Home Page

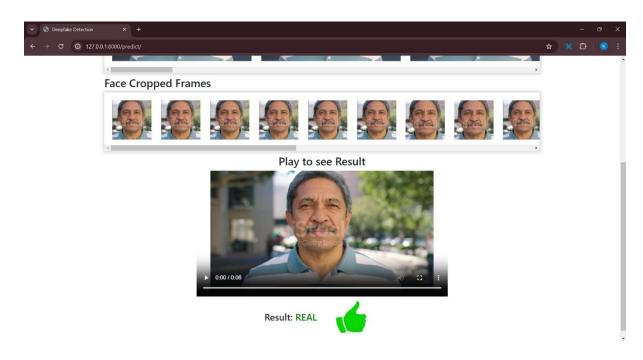


Figure: Real Video Output

Deepfake Detection

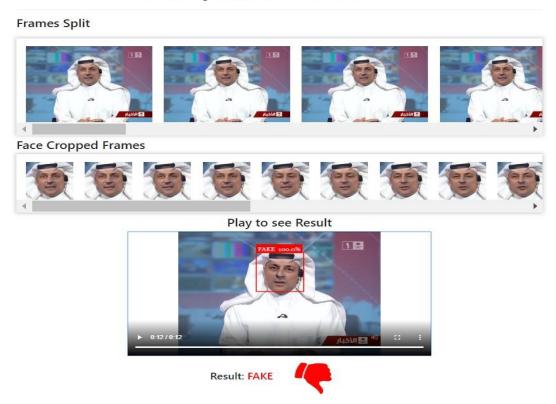


Figure: Fake video Output

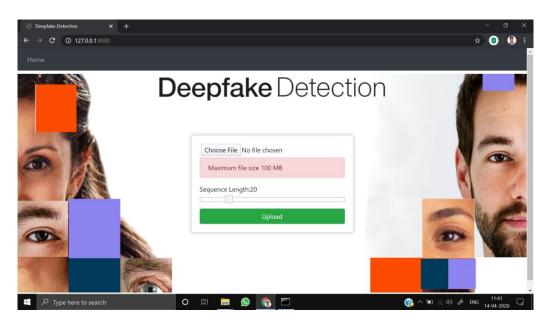


Figure: Uploading file greater than 100MB

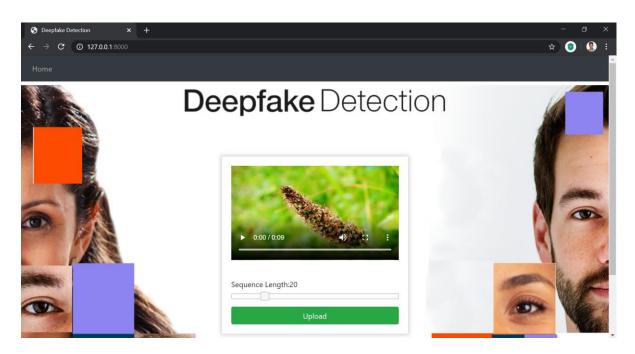


Figure: Uploading Video with no faces



Figure: Output of Uploaded video with no faces

APPENDIX IV

Authors Biography

Author Details

Name: Karthik Shrikant Devadiga

URN No:1022102010

Roll No:3039

Contact:8766550309

Email: karthikedvadiga830@gmail.com

Qualification Details: pursuing Bachelor of Technology in Computer Science and Engineering from Annasaheb Dange College of Engineering and Technology, Ashta

Name: Nilesh P Pawar

Roll No:3055

URN No:21101014

Contact:7887449995

Email: nilesh.p.pawar999@gmail.com

Qualification Details: pursuing Bachelor of Technology in Computer Science and Engineering from Annasaheb Dange College of Engineering and Technology, Ashta

Name: Pratik Rajendra Kumbhar

URN No:1022102011

Roll No:3066

Contact:8007358326

Email: kumbharpratik140304@gmail.com

Qualification Details: pursuing Bachelor of Technology in Computer Science and Engineering from Annasaheb

Dange College of Engineering and Technology, Ashta





