DEEPFAKE VIDEO DETECTION

Under the guidance of Dr. Mohammad Masum

Group 3:

Nupur Pathak
Sree Divya Cheerla
Vani Bhat

Agenda

I. Introduction
II. Project Motivation
III. Problem Statement and Solution
IV. Dataset
V. Pre-processing
VI. Methodology
VII. Architecture
VIII. Experimental Settings
IX. Experimental Results
X. Conclusion and Future Work

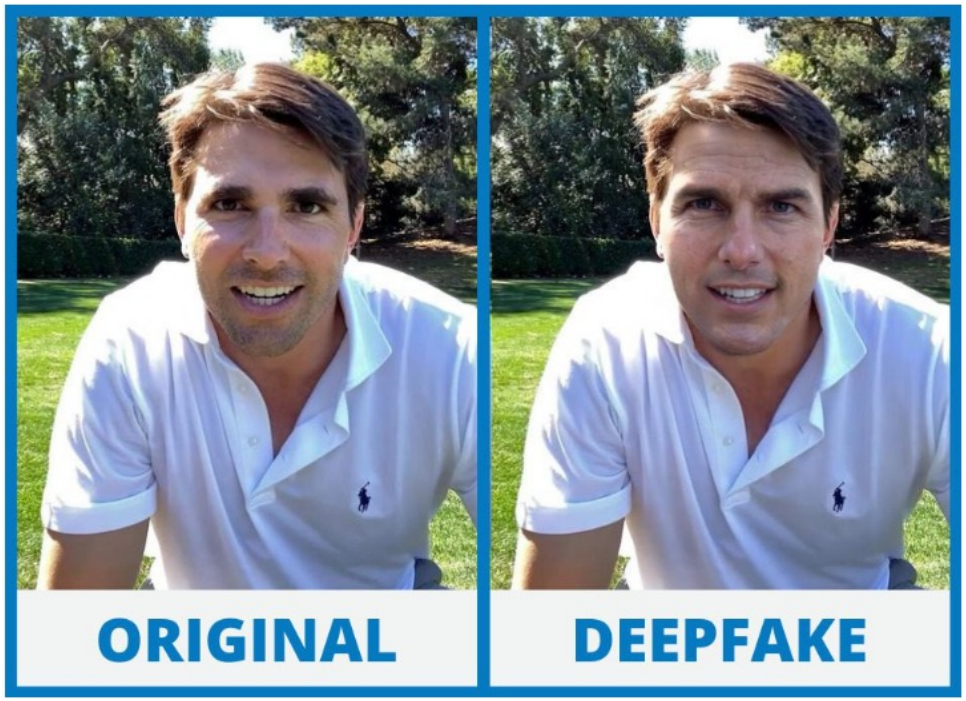
INTRODUCTION

SJSU SAN JOSÉ STATE UNIVERSITY

What are deep fakes?

- Manipulated videos, audio recordings, or images that are created using artificial intelligence and machine learning techniques.
- Generate highly realistic media that can be difficult to distinguish from authentic content.
- Used for spreading misinformation, manipulating public opinion, or creating fake news.
- Concern areas: journalism, politics, and entertainment.

PROJECT MOTIVATION



YouTube Very realistic Tom Cruise Deepfake | AI Tom Cruise - YouTube

- Combat the spread of misinformation and deception that deep fake videos can cause.
- These videos can be used to damage someone's reputation or influence public opinion.
- Therefore, it is essential to develop effective techniques for detecting deep fake videos.

PROBLEM STATEMENT

? It is challenging to distinguish between real and fake videos, even for human experts and

? The amount of damage that it can cause in today's AI world is humungous.

SOLUTION

✓ How AI is used to create deep fakes Likewise, we are using AI to address this problem by detecting deep fake videos using state of art deep learning technology techniques

DATASET

- Deepfake Detection Challenge (DFDC) dataset consists of more than 100,000 videos.
- It is created by Meta AI in partnership with other industry leaders and academic experts in September 2019 and is publicly available.
- The DFDC dataset used in this project consists of two parts: a CSV file and video folder.
- Sampled Dataset:
  - 50 videos were selected randomly from the original dataset.
  - To ensure that the dataset is balanced and representative of both real and fake videos, 25 real and 25 fake videos are selected.
  - This balance is important to ensure that the deep fake detection models are able to accurately distinguish between real and fake videos.

Filename	Label
xugmhbetrw.mp4	REAL
uqtqhiqymz.mp4	REAL
jawgcggquk.mp4	REAL
yexeazbqig.mp4	REAL
uaukglhmje.mp4	FAKE
dtjcyzgdts.mp4	FAKE
viuioldtnu.mp4	FAKE
wnaweyzlqh.mp4	FAKE

DATA PRE-PROCESSING AND FEATURE EXTRACTION

Input Video

Height: 1080
Width: 1920
FPS: 30
Frames: 300
Duration: 10 sec

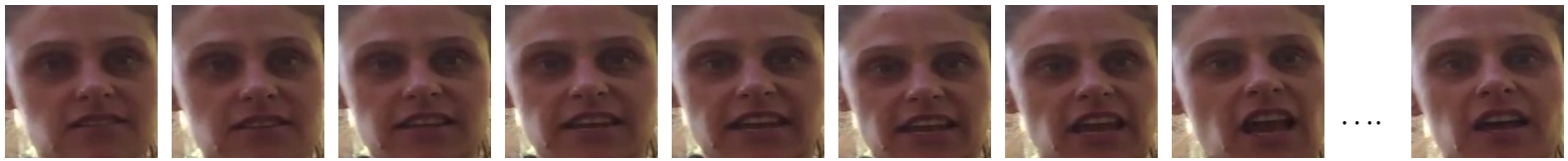
Split video to frames

Height: 1080
Width: 1920
N frames

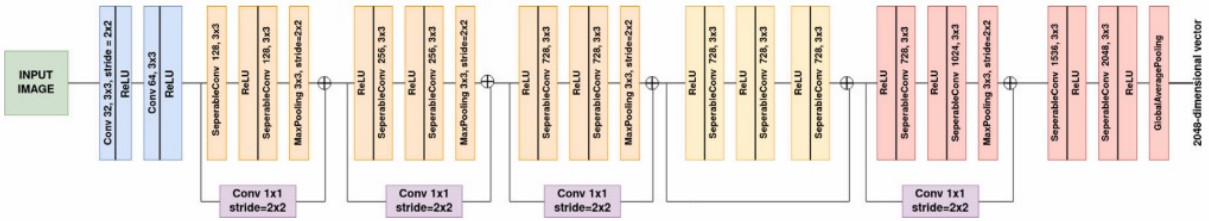
Face Detection
+
Face Cropping

N frames
224 * 224 * 3

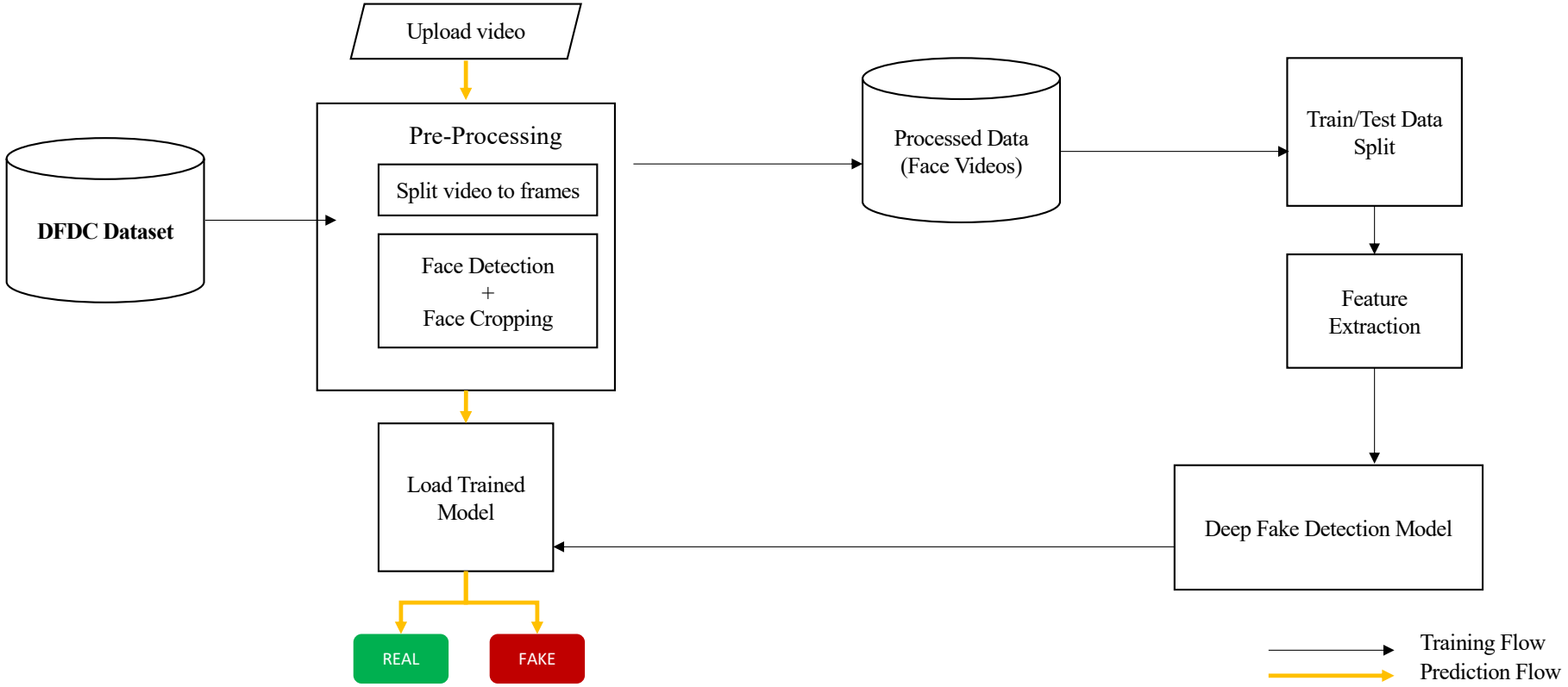
Feature Extraction



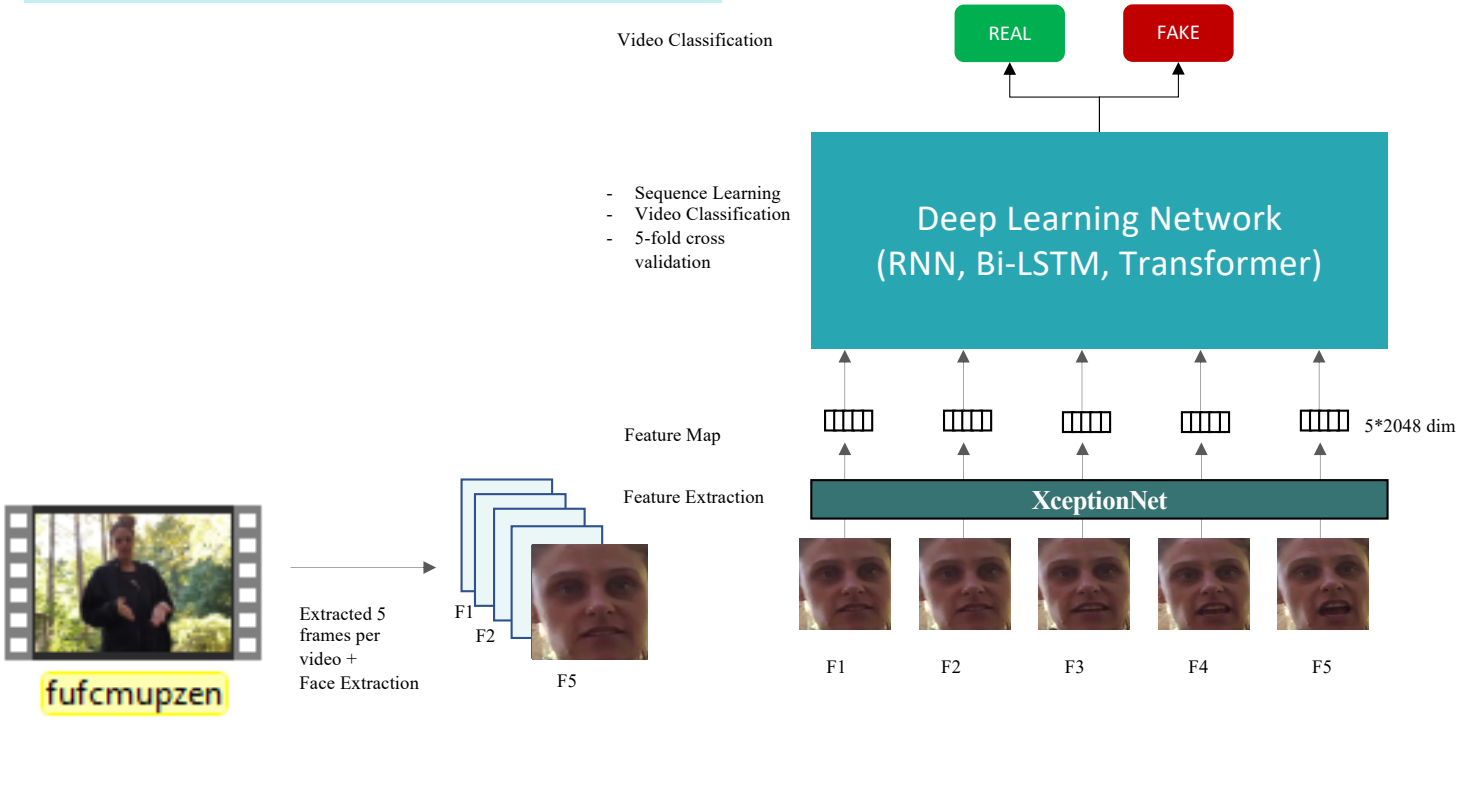
Xception architecture



METHODOLOGY



ARCHITECTURE



EXPERIMENTAL SETTINGS

SJSU SAN JOSÉ STATE UNIVERSITY

	Model - 1	Model - 2	Model - 3
Hyperparameters	**Xception+RNN**	**Xception+BiLSTM**	**Xception+Transformer**
Train videos	40	40	40
Test videos	10	10	10
Image size	224	224	224
Batch size	32	32	32
Epochs	15	15	15
Max frame count	5	5	5
Number of features	2048	2048	2048
Feature extractor	Xception	Xception	Xception
Deep learning network	RNN	BiLSTM	Transformer
Loss function	binary_crossentropy	binary_crossentropy	binary_crossentropy
Optimizer	adam	adam	adam
Initial learning rate	0.001	0.001	0.001
Activation Function (Hidden)	ReLU	ReLU	-
Activation Function (Output)	Sigmoid	Sigmoid	Sigmoid
Metrics	accuracy	accuracy	accuracy
k-fold Cross-validation	5-fold	5-fold	5-fold
No. of trainable parameters	99,882	267,098	16,826,374

EXPERIMENTAL RESULTS

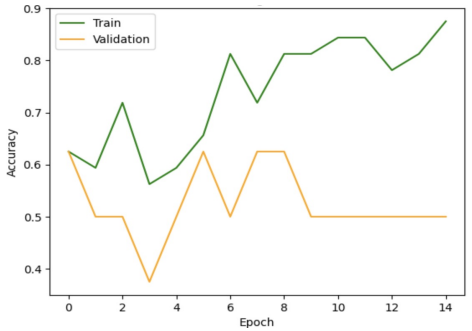
SJSU SAN JOSÉ STATE UNIVERSITY

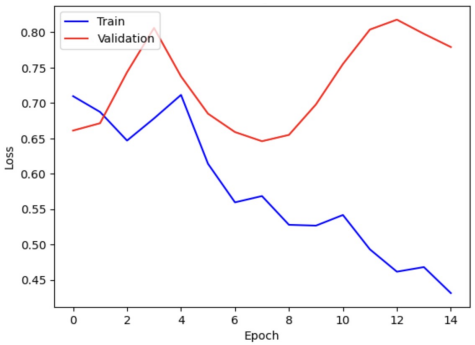
	Model - 1	Model - 2	Model - 3
Hyperparameters	**Xception+RNN**	**Xception+BiLSTM**	**Xception+Transformer**
Image size	224	224	224
Batch size	32	32	32
Epochs	15	15	15
Max frame count	5	5	5
Number of features	2048	2048	2048
Feature extractor	Xception	Xception	Xception
Deep learning network	RNN	BiLSTM	Transformer
Test accuracy +- std deviation	58% +-9.8%	70.0% +/- 8.94%	58% +- 11.66%

SJSU SAN JOSÉ STATE UNIVERSITY

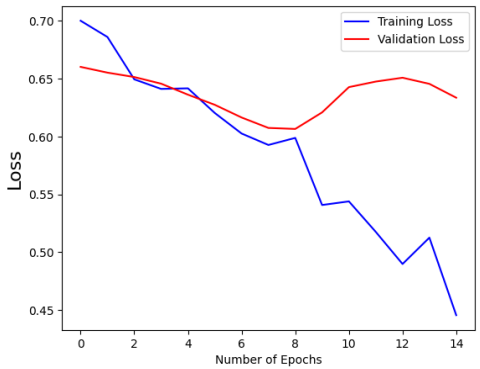
LEARNING CURVES

Xception+RNN

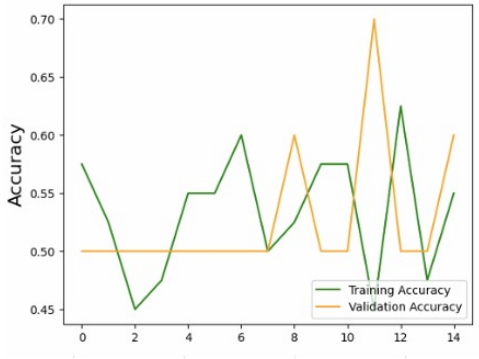


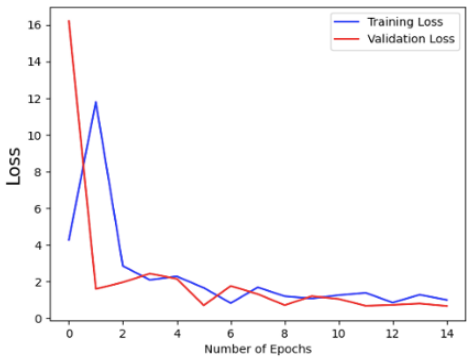


Xception+BiLSTM



Xception+Transformer





SJSU SAN JOSÉ STATE UNIVERSITY

CONCLUSION AND FUTURE WORK

- Deep fake technology continues to become a more sophisticated and critical tool in combating the spread of manipulated videos, images, and audio recordings.
- A deep fake detection system can help individuals, organizations, and governments to quickly identify and remove fake content, protecting individuals from the potential harm of false information. Help towards creating a more trustworthy and reliable digital landscape.
- Our work opens several avenues for future research. Firstly, we can explore the use of other deep learning models and compare their performance with the ones we used.
- Additionally, we can investigate the use of other features such as audio, text, and metadata to improve the accuracy of the deepfake detection system.
- Finally, we can explore the application of the deepfake detection system to various domains such as finance, politics, and entertainment, among others, to assess its effectiveness in detecting deepfakes in real-world scenarios


THANK YOU