Deepfake video detection using CNN

Shameena M K
Reg.No: KTE21MCA-2046

Guided By
Dr. Vineetha S
Department of Computer Applications
Rajiv Gandhi Institute Of Technology, Kottayam

March 1, 2023

Contents

Introduction

- Image and video forgery are posing a threat to society in today's world. People can artificially create any audio or video clip.
- In a deepfake video, a person's face, emotion, or speech is replaced by someone else's face, different emotion, or speech, using deep learning technology.
- Deepfake videos are often visually indistinguishable from real ones.
- They can have a heavy social, political, and emotional impact on individuals, as well as on society.

Current state of art

- Deepfake technology is rapidly advancing and becoming more difficult to detect.
- Current methods for detecting Deepfakes involve analyzing artifacts and inconsistencies in the video.
- However, Deepfake creators are becoming more skilled at avoiding these artifacts and making their videos appear more realistic.
- Advanced machine learning techniques, such as GANs, are being used to create more convincing Deepfakes.
- To stay up with the developing technologies, there is a need for more advanced and precise detecting techniques.

Motivation

- The increasing number of deepfake videos is a growing concern
- Advancements in technology have made it easier to create deepfake videos
- Deepfake videos have harmful impacts on people
- The project aims to detect deepfake videos to reduce their impact
- Developing a deepfake video detector is a proposed solution
- The detector will be able to identify and reduce the spread of deepfake videos

Objectives

- To study the existing models for detecting deepfake videos.
- To develop an optimal solution for deepfake detection with improved accuracy.
- To compare the impact of different feature extractors on the model and choose the best among them for implementation
- To develop a model with low computational complexity and memory requirements so it could be used in edge devices.
- To prevent the propagation of false information through deepfake media

Literature Review

- M. S. Rana and A. H. Sung, "DeepfakeStack: A Deep Ensemble-based Learning Technique for Deepfake Detection," 2020, doi: 10.1109/CSCloud-EdgeCom49738.2020.00021.
- S. Suratkar, E. Johnson, K. Variyambat, M. Panchal, and F. Kazi, "Employing Transfer-Learning based CNN architectures to Enhance the Generalizability of Deepfake Detection," 2020, doi: 10.1109/IC-CCNT49239.2020.9225400.
- M. C. El Rai, H. Al Ahmad, O. Gouda, D. Jamal, M. A. Talib, and Q. Nasir, "Fighting Deepfake by Residual Noise Using Convolutional Neural Networks," 2020, doi: 10.1109/ICSPIS51252.2020.9340138.
- G. Jaiswal, "Hybrid Recurrent Deep Learning Model for DeepFake Video Detection," in 2021 IEEE 8th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2021, pp. 1–5, doi: 10.1109/UPCON52273.2021.9667632

Proposed Methodology

The proposed solution for deepfake detection consists of five steps:

- Frame Extraction Facial Landmarks Detection
- Temporal Facial Feature Analysis
- Data preprocessing
- Data split: Training, validation and Testing
- Customized Convolutional Neural Network (CNN)

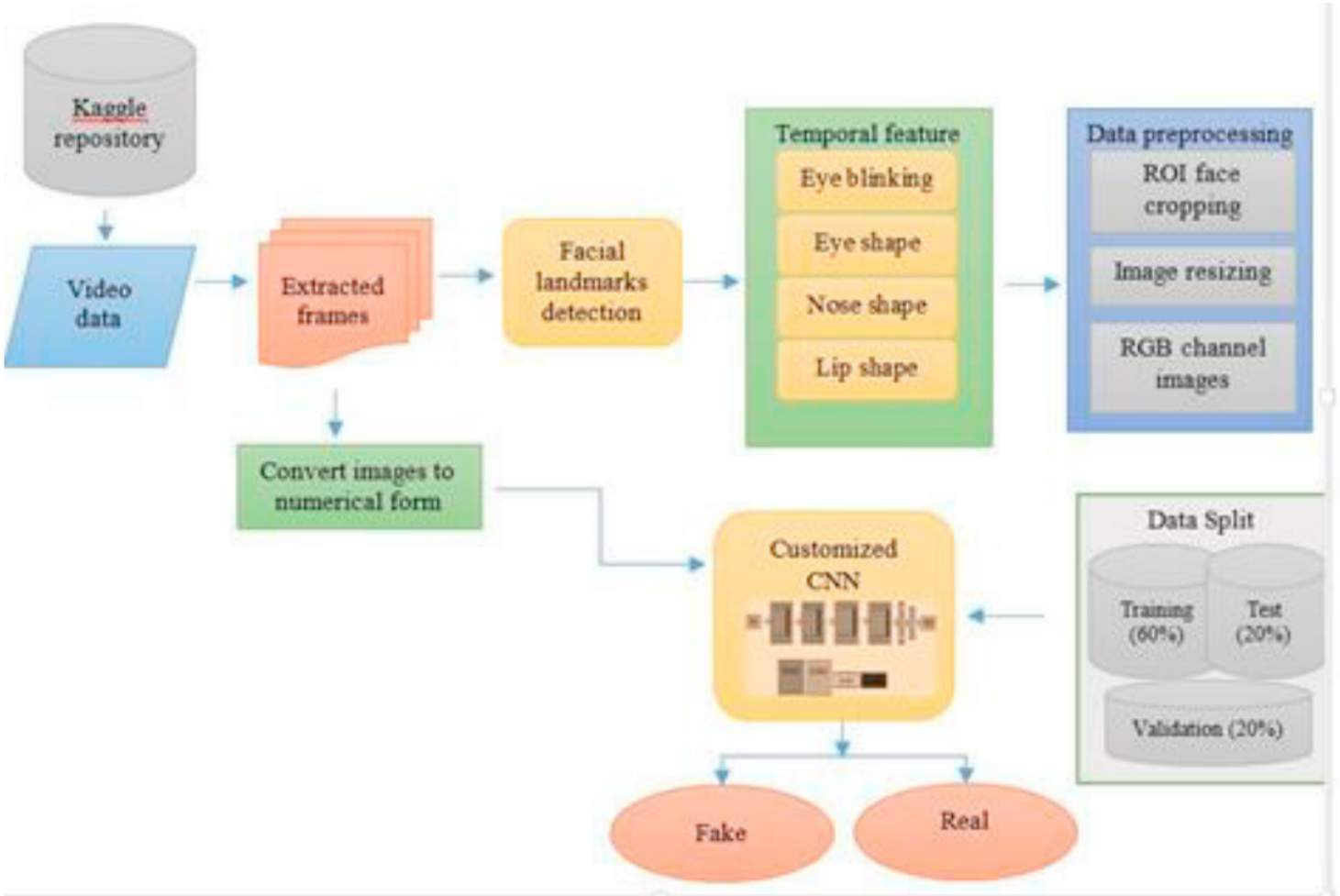

Fig.1. Block diagram of proposed model

Algorithm:

Input: Deepfake video dataset
Output: Good classification results

Strategy:

Step 1. Input video dataset from Kaggle
Step 2. Frames extraction from videos
Step 3. Detection of the all-face features using Facial landmark predictor model
  a. Eyes blink detection
  b. Eyes shape detection
  c. Lips shape detection
  d. Nose shape detection
Step 4. Perform data preprocessing on frames
  a. Crop the face region of interest
  b. Image resize into 224 x 224
  c. Ensure all images in the RGB channel
Step 5. Data splitting into three parts
  a. Training set (60%)
  b. Validation set (20%)
  c. Testing test (20%)
Step 6. Hyper Parameters setting
Step 7. Apply Customized CNN model by adding some layer for training
  a. conv2d layer
  b. Batch normalization
  c. Max pooling layer
  d. Drop out layer
  e. Flatten
  f. Dense layer
Step 8. Perform testing on a test set
Step 9. Calculate performance metrics
Step 10. Classification results whether it is fake or real

Implementation Status and Plan

- Proposed method has been implemented and tested on a dataset of both real and deepfake videos.
- Increase the accuracy of the system.
- Future plans include further refinement of the model by incorporating more advanced techniques and increasing the size of the dataset for training.
- Evaluate the effectiveness of the model on a larger and more diverse dataset in the future.

Thank you!