Jyothi Engineering College
NAAC Accredited College with NBA Accredited Programmes*
Approved by AICTE & affiliated to APJ Abdul Kalam Technological University
A CENTRE OF EXCELLENCE IN SCIENCE & TECHNOLOGY BY THE CATHOLIC ARCHDIOCESE OF TRICHUR
JYOTHI HILLS, VETTIKATTIRI P.O, CHERUTHURUTHY, THRISSUR. PIN-679531 PH : +91- 4884-259000, 274423 FAX : 04884-274777
NBA accredited B.Tech Programmes in Computer Science & Engineering, Electronics & Communication Engineering, Electrical & Electronics Engineering and Mechanical Engineering valid for the academic years 2016-2022. NBA accredited B.Tech Programme in Civil Engineering valid for the academic years 2019-2022.

Deep Fake Detection Using Machine Learning

Group no : 14

Department of CSE

Jyothi Engineering College

Thrissur

January 21, 2021

Group Members :

- Karthik PC : JEC17CS061
- M P Adithya Vijayan : JEC17CS069
- Sanjana S : JEC17CS088
- Thushara P : JEC17CS103

Guide : Ms. Aswathy Wilson

Vision of the Department

- Creating eminent and ethical leaders in the domain of Computational Sciences through quality professional education with a focus on holistic learning and excellence.

Mission of the Department

- To create technically competent and ethically conscious graduates in the field of Computer Science and Engineering by encouraging holistic learning and excellence.
- To prepare students for careers in Industry, Academia and the Government.
- To instill Entrepreneurial Orientation and research motivation among the students of the department.
- To emerge as a leader in education in the region by encouraging teaching, learning, industry and societal connect.

Course Outcomes

C410.1 The students will be able to analyse a current topic of professional interest and present it before an audience.

C410.2 Students will be able to identify an engineering problem, analyse it and propose a work plan to solve it.

C410.3 Students will have gained thorough knowledge in design, implementations and execution of Computer science related projects.

C410.4 Students will have attained the practical knowledge of what they learned in theory subjects.

C410.5 Students will become familiar with usage of modern tools.

C410.6 Students will have ability to plan and work in a team

CO Mapping to POs

	POs											
COs	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
C410.1	3	2	3	2	3	3	2	3	3	2	3	3
C410.2	2	3	3	3	3	3	2	3	2	3	3	3
C410.3	3	2	3	3	3	2	3	3	2	3	3	3
C410.4	3	3	3	2	3	3	3	2	3	3	3	3
C410.5	2	3	2	3	2	3	2	3	2	3	2	2
C410.6	3	3	3	2	2	3	2	3	2	3	2	2
Average	2.67	2.67	2.83	2.5	2.67	2.83	2.33	2.83	2.33	2.83	2.67	2.67

Contents

- Introduction
- Literature Survey
- Proposed System
- Software & Hardware Requirements
- Modules
- Data Flow Diagram
- Applications of Proposed System
- Conclusions
- References

Introduction

- Deep Fake videos are AI generated videos that look real but are actually fake
- Smartphone and desktop applications like FaceApp and FakeApp are built upon this process
- Deep fake videos can have an adverse effect on a society
- These videos can challenge a person's integrity

Literature Survey

DeepFake Video Detection Using Recurrent Neural Network

- Machine learning based free software tool has made it easy to create deepfakes that leave few traces of manipulation
- These realistic fake videos are used to create political distress, fake terrorism,etc.
- The proposed system uses a convolutional neural network to extract features.
- These features are then used to train a RNN that learns to classify whether a video has been manipulated or not.

- LSTM is used to process sequence generated by CNN
- Using convolutional LSTM we can measure whether video is manipulated or not
- 92 % accuracy has been obtained

Effective & Fast DeepFake Detection Method Based on Haar Wavelet Transform

- Deepfakes are generally created using GAN. By using GAN it became easier to create deepfakes in much realistic manner.
- Proposed method takes advantage of the fact that current algorithms can only generate deepfakes with a certain resolution
- A further distortion and blur is needed to fit the fake face with the background

- A blur inconsistency detection scheme relied on the type of edge and sharpness analysis using Haar Wavelet is used
- This can determine whether a video has been subjected to manipulation or not
- 90.5 % accuracy has been obtained

Classification of Real & Fake Images Using One-Class Variational Encoder

- Deepfakes are AI generated videos that look real but are actually fake.
- It requires only real images for training so data scarcity limitation can be solved.
- One class variational encoder consist of encoder and decoder
- At encoder side image is given as input and scaling is done using convolutional layer and mean and variance is calculated.This is given as input into decoder.
- RMSE value is calculated and it will be low for real image and high for fake images
- Eventhough it has 97.5% accuracy, better performance is only on NT and DFD dataset.

DeepFake Source Detection via Interpreting Residuals with Biological Signals

- Deepfakes are AI generated videos that look real but are actually fake.
- At first DeepFake are made using CNN in which the classification took place between real and fake.
- Source Detection is used in which PPG(Photoplethysmogram) which is present in human which can be identified by using computational methods
- The PPG signals depend on the surroundings lightning,skin tone,opacity etc.
- ROI(Region of Interest) is used for classification of fake and real images
- The main advantage is biological signal is used with an accuracy of 93%.

Classification of DeepFake Using Mouth Features

- Deepfakes are AI generated videos that look real but are actually fake.
- To build DeepFake two GAN algorithms are used which are encoder and decoder
- Encoder is for dimensional reduction by encoding data from input layer this reduces number of variables
- Decoder reduces variables to create a new output
- CNN is used to export videos and image is used for comparison
- Advantage DeepFake classification using this take less compared to other only take 2 second

Proposed System

- Here we are using Artificial Neural Networks for Deepfake Detection
- As we are using more than one indicator for checking, it has more accuracy
- The system compare headpose,eyes and mouth features.
- If all the comparisons are true the video will be classified as real
- Else it will be classified as fake

Software and Hardware Requirements

Operating System : Windows

Programming Platform : VS Code / Jupyter Notebook / Google Colab

Programming Technologies : Python, Tensorflow

CPU : Intel Core I5 or above (or its equivalent alternatives)

RAM : 4 GB or above

Hard disk : 500 GB

Functional Requirements

- Detection of deepfake images
- Detection of deepfake images with varied resolution

Non functional Requirements

- The system should be scalable
- The system should be reliable

Modules

- Data acquisition module
- Image enhancement module
- Deepfake detection module

Data Acquisition Modules

- DeepFake dataset collection
- Set sample size

Image Enhancement Modules

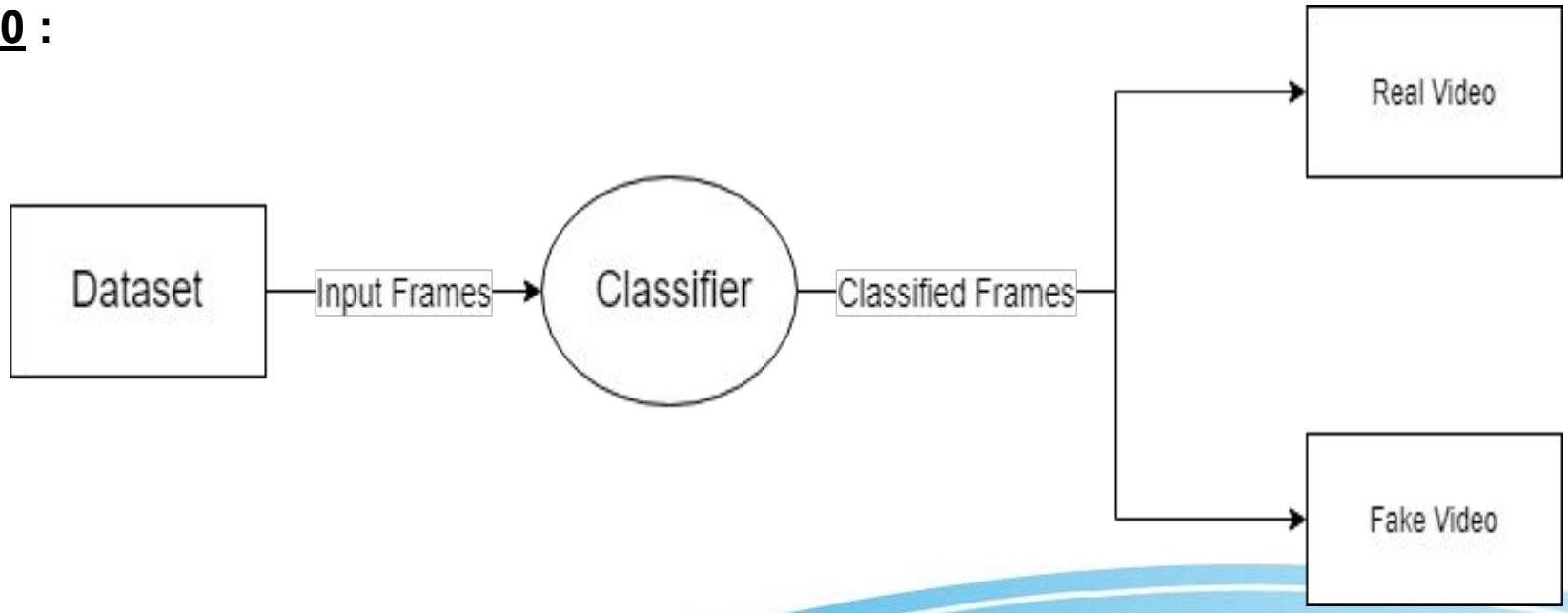
- Noise reduction
- Size correction

Deepfake Detection Modules

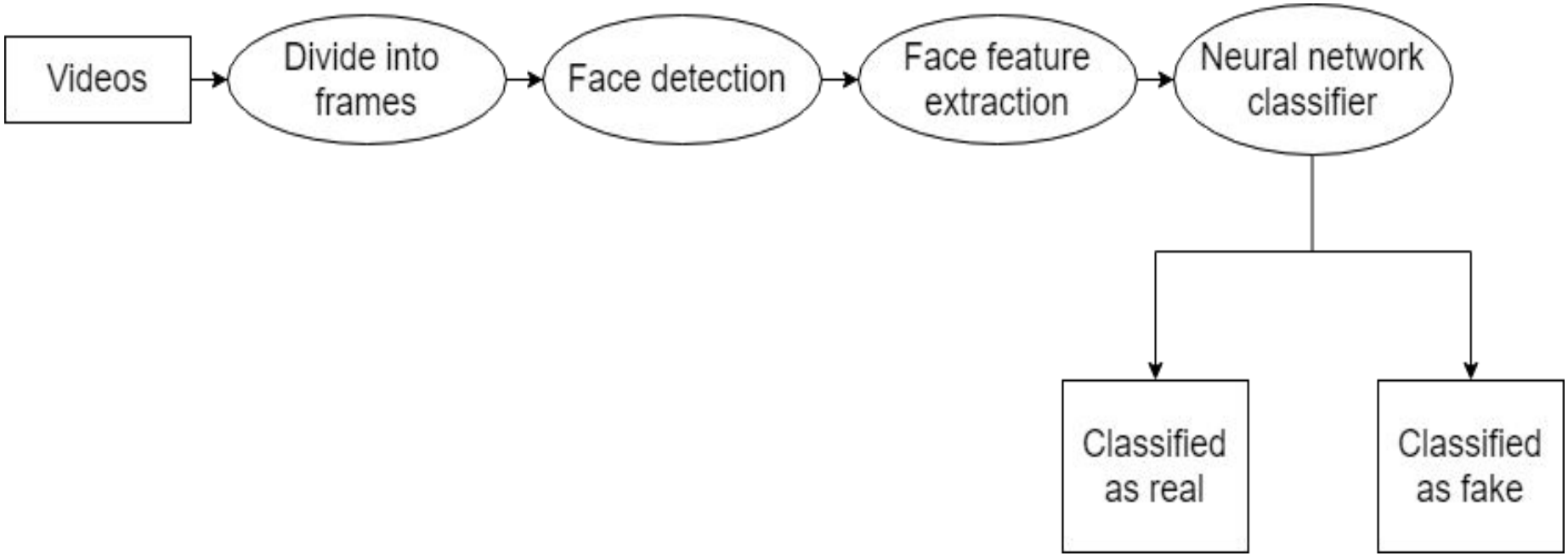
- Artificial Neural Network is used
- Facial features are extracted
- Images are classified as real or fake

Data Flow Diagram

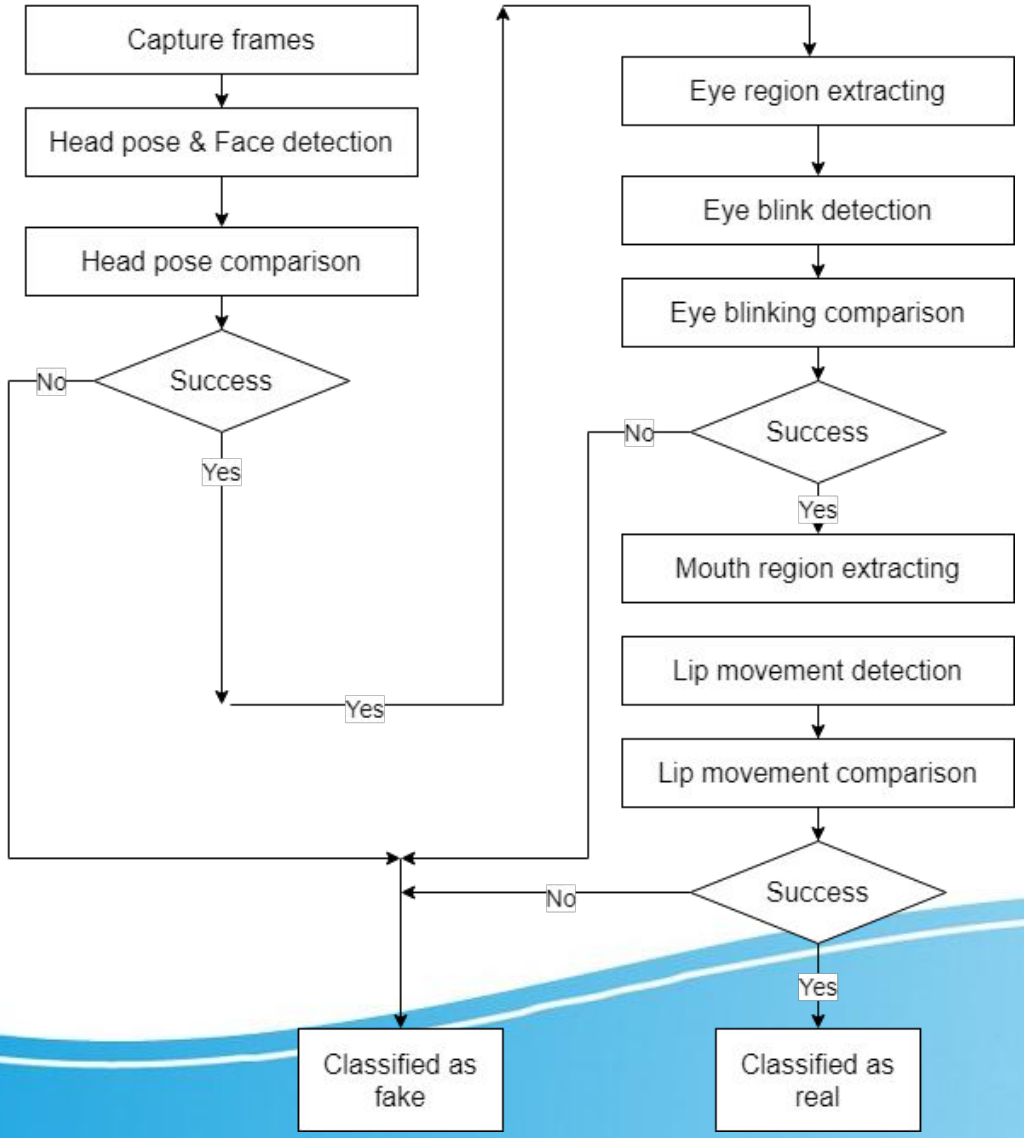
Level 0 :



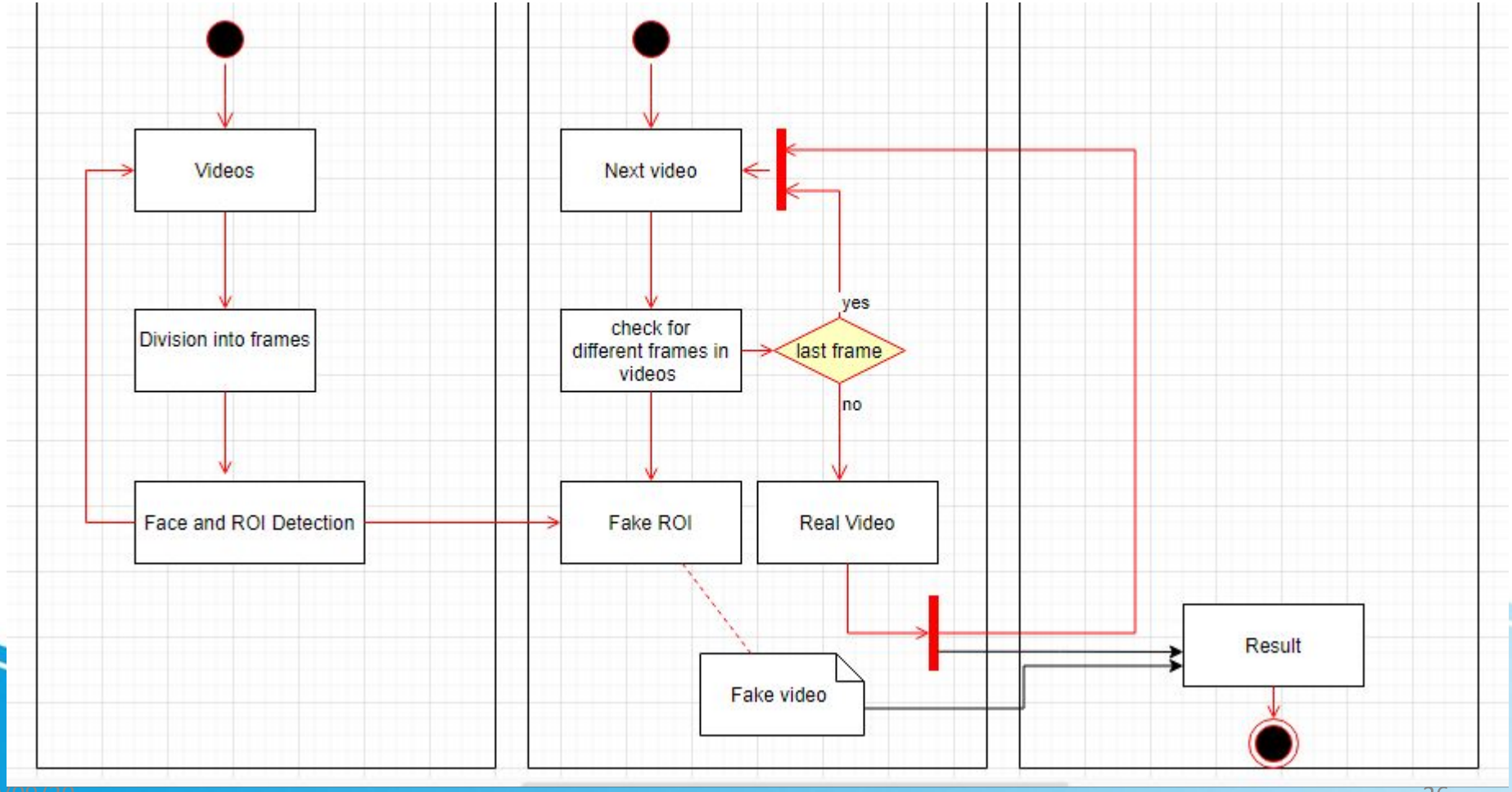
Level 1 :


Videos
Divide into frames
Face detection
Face feature extraction
Neural network classifier
Classified as real
Classified as fake

Level 2 :


Capture frames
Head pose & Face detection
Head pose comparison
Success
No
Yes
Yes
Eye region extracting
Eye blink detection
Eye blinking comparison
Success
No
Yes
Mouth region extracting
Lip movement detection
Lip movement comparison
Success
No
Yes
Classified as fake
Classified as real

UML Diagram


Videos
Division into frames
Face and ROI Detection
Next video
check for different frames in videos
yes
last frame
no
Fake ROI
Real Video
Fake video
Result

ADVANTAGES	DISADVANTAGES
• Time Efficient Time taken may vary to identify whether video is fake or not is less	• Require More data sets accuracy may become low due to less dataset
• More Accuracy comparing to other methods	• Lack of temporal awareness

Applications of Proposed System

- Decrease the spread of fake videos so that malicious abuser could not create fake news and mislead public
- Fake videos cannot be used for political distress and blackmailing
- Can be used in cyber crime detection centres
- Protection against fake celebrity pornographic videos

Conclusion

- In this we compare the features of head movement, mouth, eyes focusing on the variation from the original video
- Our system provides a method to detect these fake videos and thereby preventing the usage of these videos in creating political distress, blackmailing, fake terrorism events, etc.
- It has also increased the time taken to detect, making it more time efficient and resourceful

References

- .H. Khalid and S. S. Woo, **"OC-FakeDect: Classifying Deepfakes Using One-class Variational Autoencoder,"** 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Seattle, WA, USA, 2020, pp. 2794-2803, doi: 10.1109/CVPRW50498.2020.00336.
- .R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh and D. Batra, "**Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization**," 2017 IEEE International Conference on Computer Vision (ICCV), Venice, 2017, pp. 618-626, doi: 10.1109/ICCV.2017.74.
- D. Afchar, V. Nozick, J. Yamagishi and I. Echizen, "**MesoNet: a Compact Facial Video Forgery Detection Network**," 2018 IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, Hong Kong, 2018, pp. 1-7, doi: 10.1109/WIFS.2018.8630761.
- Z. Boulkenafet, J. Komulainen and A. Hadid, "**Face Spoofing Detection Using Colour Texture Analysis**," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1818-1830, Aug. 2016, doi: 10.1109/TIFS.2016.2555286.
-] D. Guera and E. J. Delp, "**Deepfake Video Detection Using Recurrent Neural Networks**," 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2018. [6] X. Yang, Y. Li, and S. Lyu, "Exposing Deep Fakes Using Inconsistent

Thank You