#### P.K.M Educational Trust®

#### R.R. INSTITUTE OF TECHNOLOGY

(Affiliated to VTU, Belagavi | Approved by AICTE, New Delhi & Government of Karnataka) Accredited by NAAC with B+



#### Department of Computer Science and Engineering



## Deepfake Creation and Detection Using Cycle GANs

Under the guidance of Prof. SHRUTHI S Asst Prof, Dept of CSE, RRIT



**Project Synopsis Presentation** 







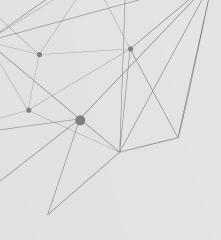
NIKITH KUMAR N
1RI17CS028

O4 SHANKAR R A
1RI17CS043

#### CONTENTS OF THIS TEMPLATE

- 1. Abstract
- 2. Scope / Objectives
- 3. Problem Identification
- 4. Proposed system
  - Approach / Methodology
  - DFD / Flowchart
- 5. Hardware Software Requirements
- 6. Expected Outcomes
- 7. Gantt charts





# O1 ABSTRACT

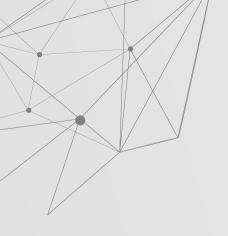
- Deepfakes is a popular image synthesis technique based on artificial intelligence. It is more powerful than traditional image-to-image translation as it can generate images without given paired training data.
- Our approach takes as input the suspect image/video as well as the target identity information (a reference image or video).
- Our motivation is to prevent the most common and harmful deepfakes that spread false information of a targeted person.



#### The aim of this project is to provide the reader with a deeper understanding of the creation and detection of deepfakes, the current trends and advances in this field, the weaknesses of current defense solutions, and the areas that require further research and attention.

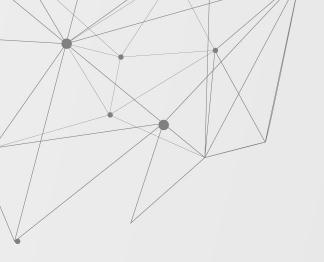
 One of the important objectives is to evaluate its performance and acceptability in terms of security, user friendliness, accuracy and reliability.

## OZ OBJECTIVE



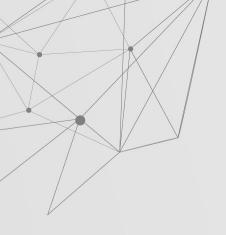
# O3 PROBLEM IDENTIFICATION

- Most of the current research aimed at combating the impact of deepfakes have focused on automated deepfake detection: using algorithms to determine whether a specific image, audio clip, or video has been significantly modified from an original.
- The goal is to train the CycleGAN model to learn how to map between images
  of two domains, and then use the trained models to generate deepfakes for the
  given input image.

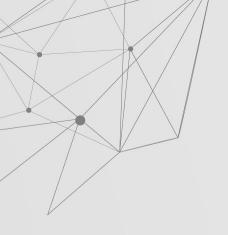


## 04 PROPOSED SYSTEM

- There are many tools available for creating the deepfake, but for deepfake detection there is hardly any tool available.
- Our approach for creating and detecting the deepfake will be great contribution in avoiding the percolation of the deepfake over the world wide web.
- The project can be scaled up from developing a web based platform to a browser plugin for automatic deepfake detections.



- Dataset: There are some sources such as YouTube, Face Forensics++, Deep fake detection challenge dataset etc, to train the mixed datasets, consisting of equal numbers of images/videos. our newly preparing dataset contains 50% of the original video and 50% of the manipulated deepfake videos. The dataset is split into 70% train and 30% test set.
- Preprocessing: Dataset preprocessing includes the splitting the video into frames.
  Followed by the face detection and cropping the frame with detected face. To
  maintain the uniformly in the number of frames the mean of the dataset video is
  calculated and the new processed face cropped dataset is created containing the
  frames equal to the mean. The frames that doesn't have faces in it are ignored
  during preprocessing.
- Model: The Data Loader loads the preprocessed face cropped video and split the
  videos into train and test set. Further the frames from the processed videos are
  passed to the model for training and testing in mini batches.



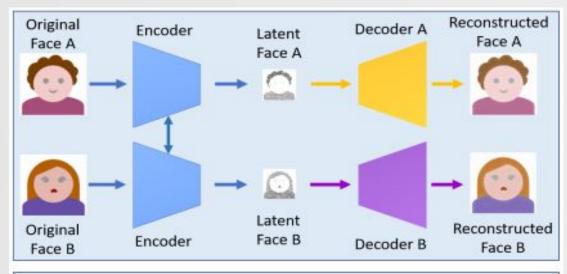
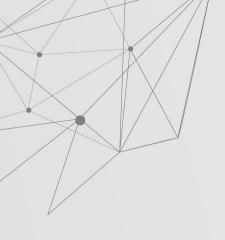
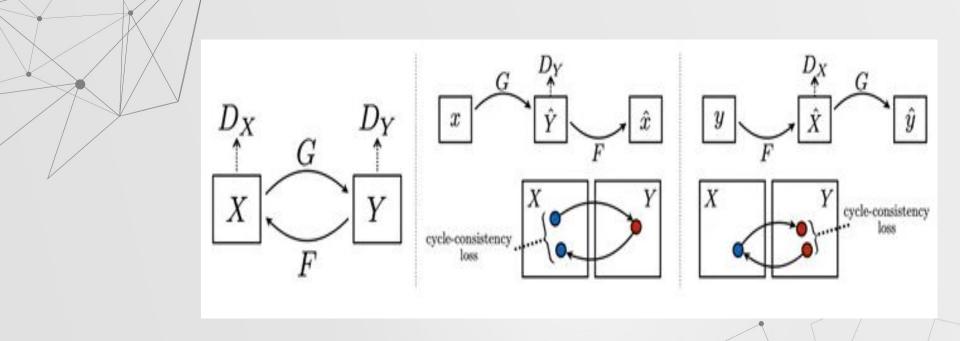




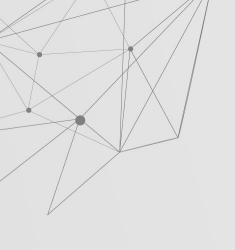
Fig. Creation procedure of Deepfakes



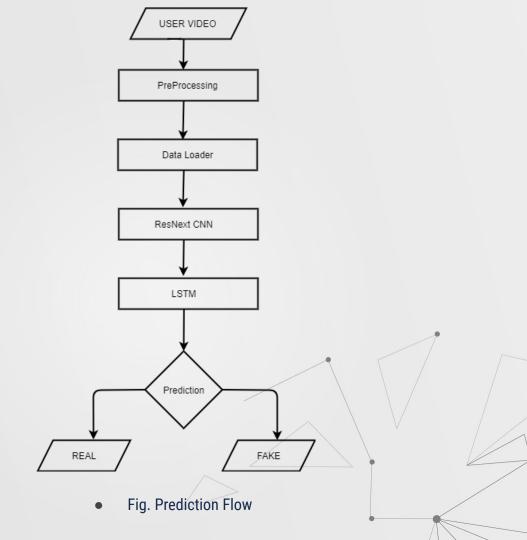
- A custom dataset will be created using helper functions to get images of the target and input faces.
- The network is trained using multiple losses. We use the losses of the two generator-discriminator pairs, just like a general GAN (adversarial loss), but we also add a cyclic loss and identity loss. The cyclic loss is used when the image is cycled back after passing through both generators.
- The need for this cyclic loss comes from our requirement that the image translated from one domain to another should retain the distinguishing features from the original domain. The identity loss helps the model to not make changes to the input image if its already in the required domain.

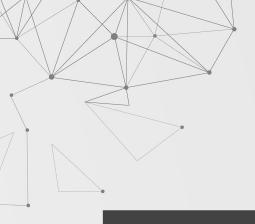


• Fig: The training procedure for CycleGAN.



#### DFD / FLOWCHART





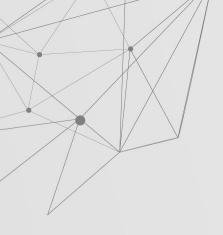
### SOFTWARE REQUIREMENTS

- Programming Language: Python 3
- Programming Framework: PyTorch
- Web Framework: Django (hosting)
- IDE: Google Colaboratory, Jupyter notebook, VSCode / Pycharm

# HARDWARE & SOFTWARE REQUIREMENTS

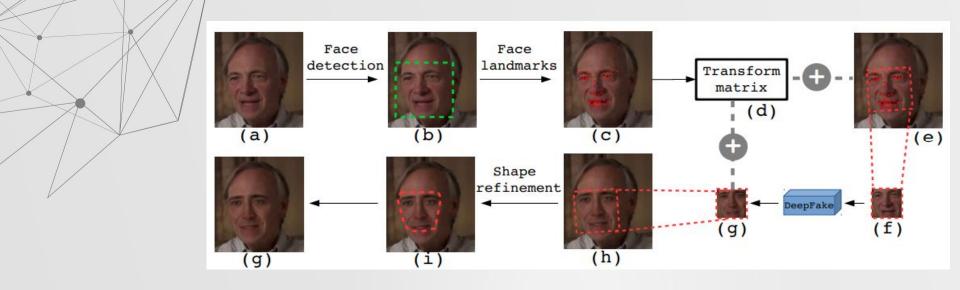
#### HARDWARE REQUIREMENTS

- GPU
- WEBCAM



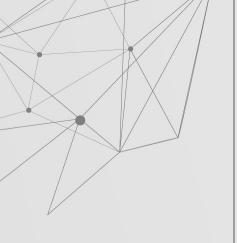
## 06 EXPECTED OUTCOMES

- The project is designed with a neural network-based approach to classifying the video as deep fake or real. The proposed method is inspired by the way in which deep fakes are created by GANs with the help of Autoencoders.
- Our method is used to detect frame level using ResNext CNN and to classify video using RNN along with LSTM. The proposed method is capable of detecting a video as a deep fake or real based on the parameters.



### 06 EXPECTED OUTCOMES

• Fig. Steps for detecting the deepfake in an image.



O7 GANTT CHART

	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Mar 2021	March-April 2021	April 2021	May 2021
Problem Identification								
Literature Review								
Abstract of Proposed Solution and its Advantges								
Architecture and High Level Design								
Code Implementation								
Low Level Desiign (Class Diagrams and Sequence Diagrams)								
Testing								
Project Deployment								
Thesis (Report Finalization)								

#### RESOURCES

#### **IEEE PAPERS & LINKS:**

- ★ Deep Learning for Deepfakes Creation and Detection: A Survey
- ★ A Convolutional LSTM based Residual Network for Deepfake Video Detection
- ★ The Creation and Detection of Deepfakes: A Survey
- ★ Generative Adversarial Networks
- ★ Github: deepfake / face swap



