# INTEL AI HACKATHON

# Neural Ninjas

## Problem Statement

## Deepfake Detection Shield

Deep-Fake encompasses various technologies employed to create audio, image, and video hoaxes. The widespread accessibility of these tools has led to an unprecedented surge in AI-driven content generation. However, the unauthorized use of individuals' information to create such hoaxes raises significant concerns. In this track, participants are tasked with devising techniques to detect Deep-Fakes, addressing the need to safeguard against the misuse of personal data in fabricated media content


| Team members Names | Email IDs | Institution Name |
|---|---|---|
| • Ayush P | cb.en.u4cse22406@cb.students.amrita.edu | Amrita Vishwa Vidhyapeetham |
| • Vaibhav Shekar | cb.en.u4cse22452@cb.students.amrita.edu | Amrita Vishwa Vidhyapeetham |
| • Eniyan M K | cb.en.u4cse21435@cb.students.amrita.edu | Amrita Vishwa Vidhyapeetham |
| • Ramya Tadepalli | cb.en.u4cse21263@cb.students.amrita.edu | Amrita Vishwa Vidhyapeetham |

# Solution

**Overview:** Deepfakes are a type of synthetic media that can be used to create realistic but fake videos or images of people. They are created using AI techniques, and can be used for malicious purposes such as spreading misinformation or damaging someone's reputation.

- **Proposed solution:** We propose a deep learning-based solution to detect deepfakes. Our system will use a convolutional neural network (CNN) to extract features from videos and images, and then use a recurrent neural network (RNN) to classify the features as real or fake.
- **Expected benefits:** Our solution will help to protect people from the harmful effects of deepfakes. It will also help to ensure the integrity of online content.

# Method

- **Approach:** We will leverage the strengths of the frame-by-frame classification approach using EfficientNet B7 encoders and MTCNN face detection, while incorporating our own innovative techniques to enhance accuracy and robustness.
- **Model architecture:** The model used will be a convolutional neural network (CNN) with EfficientNet B7 encoders. EfficientNet B7 is a pre-trained model that has been shown to be effective for image classification tasks. We will fine-tune the EfficientNet B7 model with our enhanced data and experiment with different hyperparameters, architectures, and ensemble learning strategies.
- **Face detection:** The MTCNN detector will be used to detect faces in each frame of the video. This is important because deepfakes are often focused on manipulating facial features.
- **Heavy augmentations:** Data augmentation is a technique that is used to artificially increase the size and diversity of a training dataset. This may involve incorporating temporal augmentations, adversarial training, and domain-specific augmentations
- **Custom heuristic for averaging predictions:** To design a heuristic to average the predictions of the model for each frame, considering factors like confidence scores, temporal consistency, and neighboring frame predictions.
- **Ensemble Learning:** We will investigate the potential of combining multiple models trained with different configurations and data augmentations. This ensemble approach can leverage the strengths of diverse models to achieve better overall performance and generalization.

# OneAPI toolkit:

## AI Tools

## End-to-End AI and Machine Learning Acceleration

- Intel® Distribution for Python* with highly optimized scikit-learn*
- Intel® Extension for PyTorch*
- Intel® Extension for TensorFlow*
- Intel® Optimization for XGBoost*

- Intel® Optimization of Modin* (available through Anaconda* only)
- Intel® Neural Compressor
- Intel® AI Reference Models

## Intel® Distribution of OpenVINO™ Toolkit

## Deep Learning Inference Deployment

- Model Optimizer
- Deep Learning Workbench
- Inference Engine
- Deployment Manager
- OpenCV*
- DL Streamer
- Post Training Optimization Tool