Deepfake detection system

CONTENTS OF THIS TEMPLATE

1. Topic of the Project
2. Problem Statement / Objective / Scope of the Project
3. Hardware / Software Requirement
4: Architecture Diagram / Process flow / Timeline
5. Usability / Application

Topic of the project

WHAT IS A DEEPFAKE?

Have you seen Barack Obama call Donald Trump a “complete dipshit”, or Mark Zuckerberg brag about having “total control of billions of people’s stolen data”, or witnessed Jon Snow’s moving apology for the dismal ending to Game of Thrones? Answer yes and you’ve seen a deepfake. The 21st century’s answer to Photoshopping, deepfakes use a form of artificial intelligence called deep learning to make images of fake events, hence the name deepfake.

Problem statement

Deepfakes that harass, intimidate, demean, undermine and destabilise. Deepfakes may spark major international incidents. A deepfake of a world leader pressing the big red button may cause armageddon. A deepfake satellite images of troops massing on a border can cause much trouble.

There can be many other calamities when there is a ample room for mischief-making. Last year, Tesla stock crashed when Elon Musk smoked a joint on a live web show. In December, Donald Trump flew home early from a Nato meeting when genuine footage emerged of other world leaders apparently mocking him. Will plausible deepfakes shift stock prices, influence voters and provoke religious tension? It seems a safe bet.

Deepfakes undermine trust. The more insidious impact of deepfakes, along with other synthetic media and fake news, is to create a zero-trust society, where people cannot, or no longer bother to, distinguish truth from falsehood. And when trust is eroded, it is easier to raise doubts about specific events.

objective/ scope of the project

Artificial intelligence already helps to spot fake videos, but many existing detection systems have a serious weakness: they work best for celebrities, because they can train on hours of freely available footage. Tech firms are now working on detection systems that aim to flag up fakes whenever they appear.

The main objective of this project is develop a deepfake detection system using deep learning that will cater to the above problems caused.

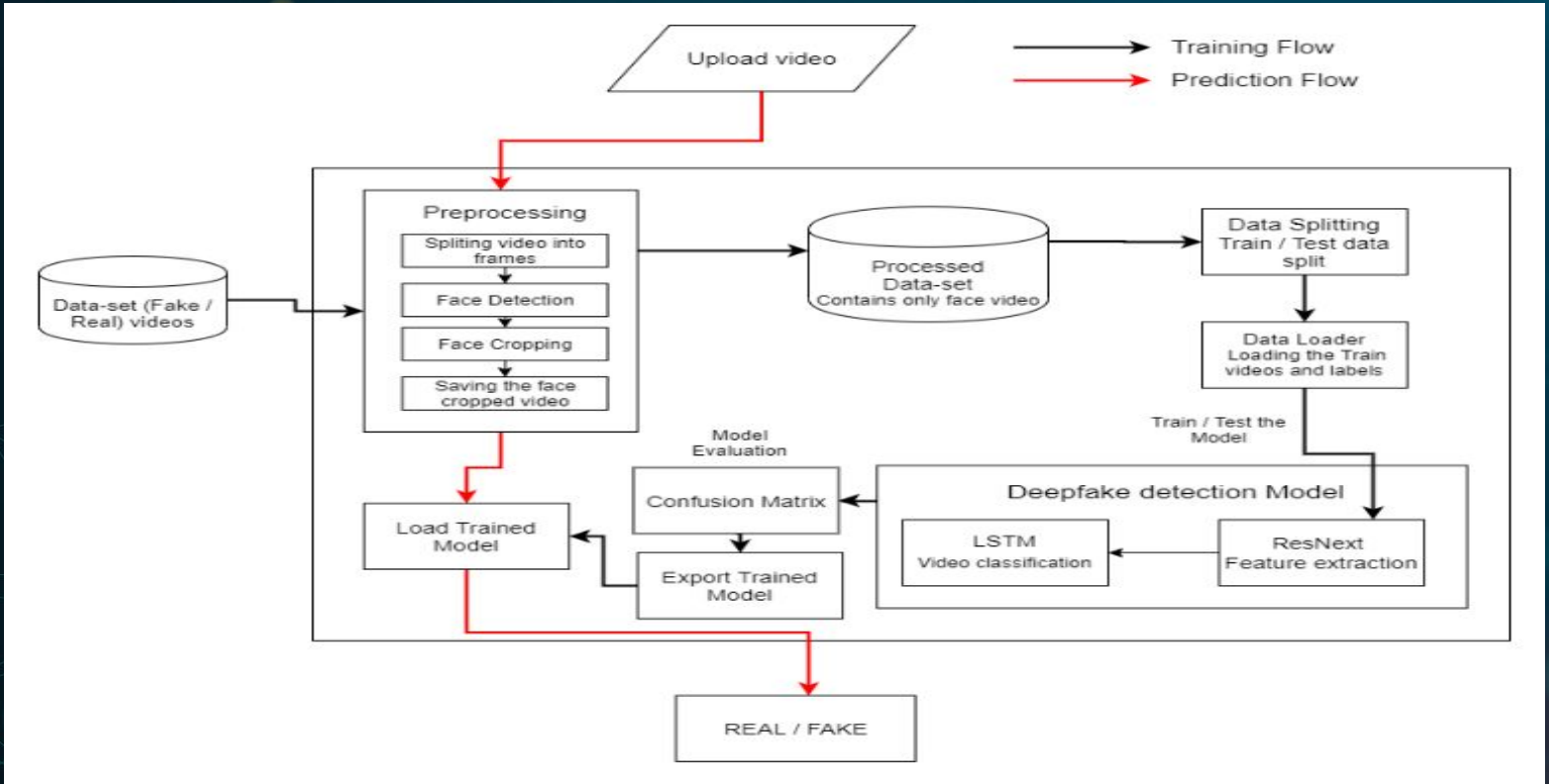
DeepFakes involves videos, often obscene, in which a face can be swapped with someone else's using neural networks. DeepFakes are a general public concern, thus it's important to develop methods to detect them. Deepfake detection system is a program to detect if a video or image is a deep fake or not.

Hardware/software requirements

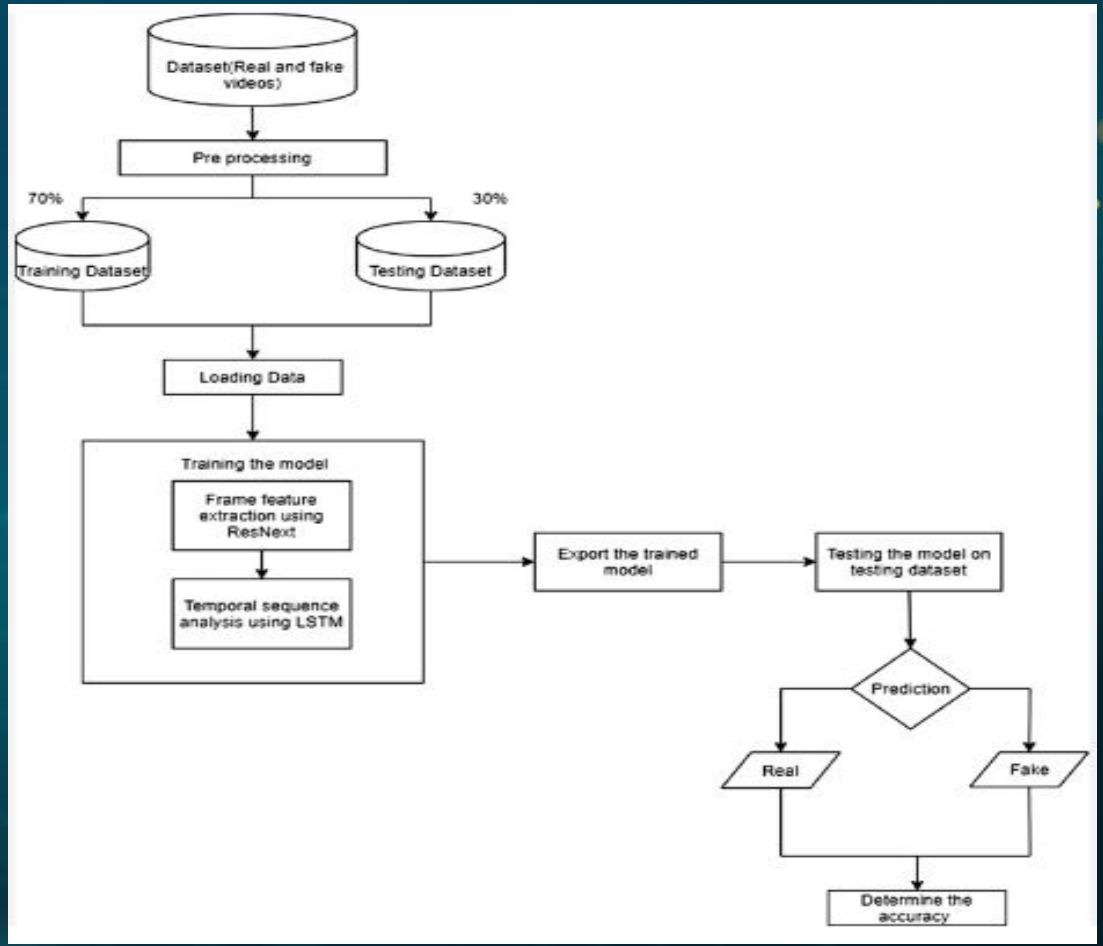
Software Requirements: python 3.x
CV2
Neural networks
Matplotlib
Tensorflow
OS
Pandas
Numpy

Hardware Requirements: camera
laptop (8 RAM , Quad core processor)

Architecture diagrams



Process flow/timeline



Modules used

- Glob
- Face recognition
- Torch
- Torch vision
- OS
- Numpy
- CV2
- Matplotlib
- Json
- Random
- Sklearn
- Seaborn

Usability

- Deepfake algorithms can create fake images and videos that humans cannot distinguish them from authentic ones.
- Even if a video is genuine and a viewer would acquire true beliefs, distrust born of deepfakes would prevent a person from actually believing what they saw. The epistemic threat is that deepfakes will interfere with our ability to acquire knowledge about the world by watching media.
- Video deepfakes have the potential to modify our memories and implant false memories. They can also modify a person's attitude toward the target of the deepfake. One study found that exposure to deepfake depicting a political figure significantly worsened participants' attitudes toward that politician.
- Therefore, a deepfake detection system can be used to tackle these issues and prevents in causing outrage in possible situations.

Application

The technology of the deep fake detection system can be applied in below situations to detect :-

1) Child sexual abuse material
2) rape sexual content
3) fake news
4) Hoaxes
5) Bullying
6) Financial fraud
7) cybercrime
8) identity theft

→From traditional entertainment to gaming, deepfake technology has evolved to be increasingly convincing and available to the public, allowing the disruption of the entertainment and media industries

→A bank in Hong Kong was duped by an artificial intelligence-powered “deep-voice” attack that cloned a trusted director’s voice seeking huge amount of money.

→A classic deepfake example is when a person of influence asks for some type of monetary donation. An executive may seemingly send a voicemail over email to an employee asking for a donation to her charity only to find out the recording was a fake and the money was given to an offshore account.