THESIS proposal
Deep Fake detection with ML techniques

Student Name:Muhammad Qasim, Roll No.: 19K1612, Supervisor:Dr. Noman Durani

1. **Abstract**

Manipulation of videos and images is not a new field. For many years graphics designers and video editors have been doing this thing with the latest graphics tools(photohso, after effect). Deep fake fields start from 2017 when some anonymous person has published a video on reddit plot form by using a famous actress's face in a pronology video[1]. There are three types of deep fake videos (Head puppetry:whole face and upper shoulder, Face Swapping:face with source expression, Lip syncing:) [2]
CCT photogs are the evidence for any event which happened anywhere. The DeepFake video is very dangerou for people (celebrities, politicians, army officers etc.) We have already achieved good accuracy for generating deep fake videos using novel Deep learning techniques GANs known as DeepFake[3]. There may application exist for creating deepfake Image/Video for example FaceApp, Zao and also online tools available deepfakesweb.com , https://www.synthesia.io/, https://www.cannyai.com/ we can generate deepfake videos and images using the above tools.

Deep Fake video use for reenact, lip sync, motion detection source to target videos, face swap, synthesis video which did not exist before or real there so many applications are here. audio and video generated. Due to deep learning this is really possible now we can generate all types of fake videos and audios now but not all perfectly. Some applications that have already achieved 100% accuracy look like real images/videos.

but we need to improve current existing techniques for detecting deep fake videos/images for forensic purposes. Many researchers have already started working on it. They also applied and tested machine learning techniques for this purpose. I'll share this in the next section. I'll try to find a gap with the help literature review (research).
J. Deng already applied CNN and RNN for deepfake detecting[4]. which i was thinking of using for this purpose but i'll also try to use some other combination like anomaly detection technique with this i still not found in literature which i have readed until now.

2. **Introduction including motivation and benefits of the research work**

Deep fake detection is one of the hottest research topics where many researchers are trying to find the way to identify if the digital content is real or deep fake generated content. Many researchers have already done work for this domain. That's why I think I'm goin on right direction. Researchers already have applied deep learning and ML techniques for this purpose [2]. Initially I have decided to work with LSTM and CNN combination for deep fake detection but after retrature review I found this work has already been done by p.korshunov [5].

I will try to combine LSTM, CNN or ML techniques (anomaly detection and others) for deep fake detection.

The Motivating factor is that I wanna contribute to the Artificial Intelligence community. Hopefully I'll do this or may be able to write some research papers or it will be published in good generals.

3. **Literature Review**
    a. DEEPFAKE DETECTION: CURRENT CHALLENGES AND NEXT STEPS
    b. deepfake generation and detection_aala survey_2021
    c. Deepfakes: Trick or treat?
    d. Deepfakes and beyond: A Survey of face manipulation and fake detection
    e. The Deepfake Detection Challenge (DFDC) Preview Dataset

4. **Research Gap and Research Question(s)**

    Q1: How will you get data for your research?
    Ans: There are many databases available with generated through deep fake or we can also generate fake videos or images using online tools or mobile applications.

    Q2: How will you implement this,do you have enough hardware/software resources for this experiment?
    Ans: I have an NVIDIA card in my office. I can run expensive process tasks in my office or home. as google colab is one of the other free platforms for deep learning experiments. Otherwise I also have an AWS account where I can use Sagemaker service for end to end ML pipeline.

    Q3: What will you do if you get stuck on any particular point? Do you have access to connect with these domain experts?
    Ans: I have connected with some deep learning experts which have huge experience in deep learning. like Dr. Nouman durani, Dr Noman Islam, Dr. Waseem and Sir Zia Khan

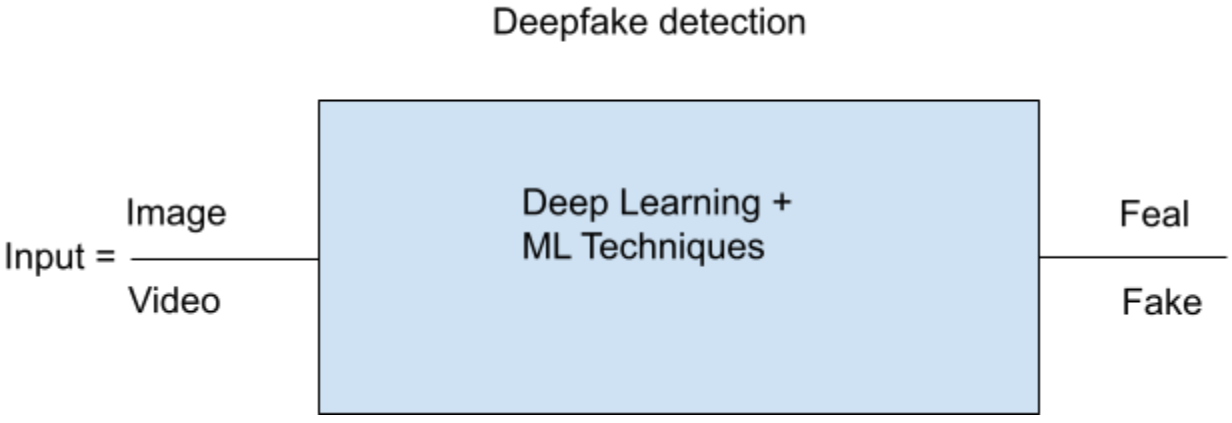
    Q4: work-flow or process diagram is this possible in the current area?

    Q5: How can you identify the gap and what will you do to fill this gap?
    After retrature review I'll try to find a gap plus how to fill this gap using my knowledge in this domain.

5. **Problem Statement**

    In the current era deep fake contents are frequently seen on social media and other platforms so we have to create some method which will help to identify the digital contents as fake or real or auto generated. We will focus only for deep fake generated contents detection using deep learning or ML techniques.

6. **Block diagram of proposed research methodology**



7. **Project Timeline**

   Retrature review try to read maximum papers, try to run some relevant paper code, and finally add some new techniques with previous researcher working or coding.

8.

9. References

[1] Bitesize, B. B. C. (2019). deepfakes: What are they and why would i make one?. *2019.[Online]*.

[2] Lyu, S. (2020, July). Deepfake detection: Current challenges and next steps. In *2020 IEEE international conference on multimedia & expo workshops (ICMEW)* (pp. 1-6). IEEE.

[3] https://github.com/deepfakes/faceswap .

[4] J. Deng , W. Dong , R. Socher , L. Li , K. Li , L. Fei-Fei , ImageNet: A Large-Scale Hier-archical Image Database, in: Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2009 .

[5] P. Korshunov , S. Marcel , Speaker Inconsistency Detection in Tampered Video, in: Proc. European Signal Processing Conference, 2018 .