Jordan University of Science and Technology
Faculty of Computer and Information Technology
Department of Network Engineering and Security

Graduation Project 1 Report

Project Title

Liveliness Detection Using Deep Learning

BY

Shahed Al-Rweidan, 126159
Tasneem Al-Barqat, 125572
Ahmad Bazar, 101862
Mohammad Kayed, 126292
Amin Al-Tawiel, 101598

Supervisor
Dr. Raed Bani-Hani

Wednesday, January 19, 2022

Introduction

Face recognition is a biometric system that automatically identifies or verifies a person's identity using his/her facial features and expressions. Face recognition software has many applications in the modern world such as logging in to a computer using facial verification as a password, gaming, people tagging, security and so on [1]. Face recognition systems have become the target of spoofing threats and the face biometric systems are highly vulnerable to presentation attacks that can be carried out by presenting video, where an impostor can gain access to the system by presenting a video of a valid user to the sensor, so face liveness detection is a necessary step before granting authentication to the user.

We started thinking of developing deep architectures for face liveness detection that uses a combination of texture analysis and a convolutional neural network (CNN) to classify the captured image as real or fake.

Background

Liveliness detection in biometrics is the system's ability to detect face is real from a live person present at the capture point or is fake, and it consists of a set of technical features to counter biometric spoofing attacks, in which a person's biometrics are used [4].

In recent years, various algorithmic development for face liveness detection systems has been reported. These developments can be broadly classified into two domains: fixed features-based face anti-spoofing systems and deep features-based face anti-spoofing systems. Fixed features-based face anti-spoofing systems exploit hand-crafted features to perform classification between live face and spoof. On the other hand, deep features-based face anti-spoofing systems utilize deep neural networks such as convolutional neural networks (CNN) to classify a live face and spoof. Since features learned by deep neural networks are dynamic, and they are currently the most preferred choice for most face anti-spoofing systems [3].

Convolutional neural networks (CNN) are specifically designed to work with problems involving images as inputs where these inputs can be represented by an image or a set of images and take the image raw pixel data , trains the model, then extracts the features automatically for better accuracy classification if spoof or real [5]. The experimental results showed that the CNN model achieves an accuracy of 99.5% [2].

Design Requirements

Due to covid-19, it is better to avoid using any recognition systems that need touching. Face recognition became more popular to be used today and more vulnerable to being hacked too, so we thought to develop liveliness detection as a solution to spoofing the face.

Our system requires a face detection algorithm that captures a face from a video that could be real/spoofed then we divide data into three-part: 60% of the images are for training data to feed the model, 20% are for test data to test the model and the rest 20% development set to optimize hyper-parameters.[6]

Engineering Standards

To implement liveliness detection in face recognition, we have used Python programming which has a rich library to build solutions faster. For deep learning model design and training we used the Tensor-flow framework and Keras, building and training models in Keras is much easier. For images reading we used the OpenCV library and Numpy library for array operations like re-scaling images, extracting an image from videos.[7]

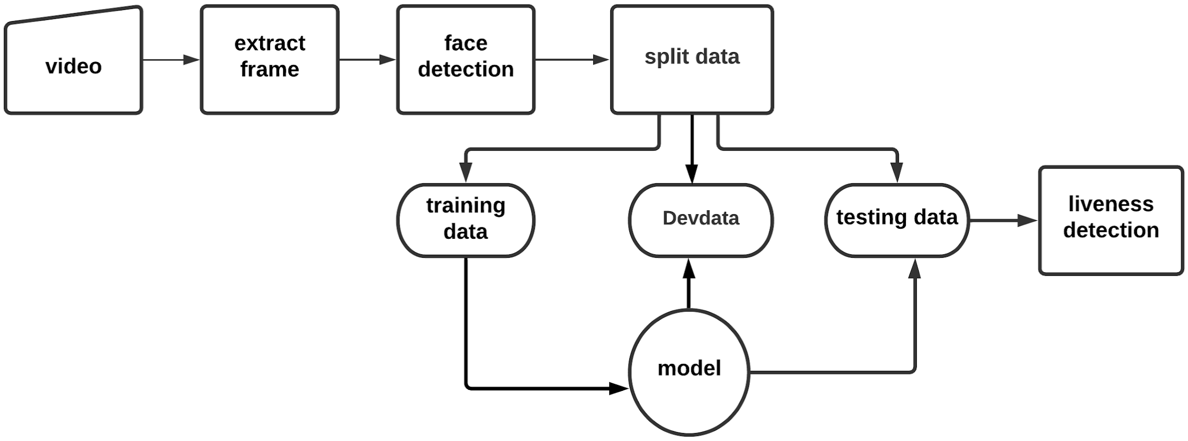
Realistic Constraints

Data used for the feed model need a month to be collected and can occupy near 2 GB.
The resolution of the video could affect the model performance. The resolution has the potential for further increasing neural network performance.[8]

Dataset requires more preparation extract frames, resize and crop .etc [9]

Proposed System Model/Design

The framework for project face liveliness detection is as shown in Fig below :



1- preparing dataset

The dataset consists of two classes, namely real face images and spoofed face images. Spoofed face images are created by capturing face images displayed in a video or camera screen by using another camera.

We collected videos from eight people each person recording one real video of the 20s and one spoofed video of the 20s. We expect to extract 30-60 frames per second from each video . Total dataset real/spoofed between 4800-9600 frames.

In future work, we need face detection[10] to extract faces from videos that are used for building the dataset of live face images and spoofed face images. Building a convolutional neural network model and trained to detect real and spoofed videos.

Completed Tasks

- Collected that dataset real and spoofed videos.
- Learned python programming language.

References

[1] Suad Haji and Asaf varol “real-time face recognition system “, in turkey25-27 April-2016.https://www.researchgate.net/publication/303393659_Real_time_face_recognition_system_RTFRS

[2] Syafeeza, A. R., Khalil-Hani, M., Liew, S. S., & Bakhteri, R. "Convolutional neural network for face recognition with pose and illumination variation". International Journal of Engineering & Technology, 6(1), 0975-4024,2014.

[3]Yasar Abbas Ur Rehman, Lai-Man Po, Mengyang Liu, Zijie Zou, Weifeng Ou, Yuzhi ZhaO. “Face liveness detection using convolutional-features fusion of real and deep network generated face images”.Department of Electronic Engineering, City University of Hong Kong, Hong Kong Special Administrative Region,p.1,2019

https://www.sciencedirect.com/science/article/pii/S1047320319300641

[4]https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/liveness-detection.

[5]https://towardsdatascience.com/understanding-cnn-convolutional-neural-network-69fd626ee7d4

[6]https://towardsdatascience.com/data-splitting-technique-to-fit-any-machine-learning-model-c0d7f3f1c790

[7] Bali Shankar Khurana,”liveness detection in face recognition using deep learning “.Turkish Journal of Computer and Mathematics Education.p(2),2021.

https://www.turcomat.org/index.php/turkbilmat/article/view/8096/6334

[8] “image resolution” https://pubs.rsna.org/doi/full/10.1148/ryai.2019190015

[9]https://machinelearningmastery.com/best-practices-for-preparing-and-augmenting-image-data-for-convolutional-neural-networks/

[10]”face-detection”https://www.analyticsvidhya.com/blog/2021/07/facial-landmark-detection-simplified-with-opencv/

Project path :

January **1\1-30\1**	**Collect data (video)**
February **1\2-30\2**	**Preparing data for training (extract image)** **Split data** **Build model CNN**
March **1\3-30\3**	**Training model and test** **solve any problem in model**
April 1\4-30\4	**Test project**
May 1\5-30\5	**Final result in project**