Indian Institute of Information Technology
Allahabad

DEPARTMENT OF INFORMATION TECHNOLOGY(IT)

Sixth Semester Project Report on

Face Spoofing Detection using Convolutional Neural Networks(CNN)

Under the supervision of
Dr. Triloki Pant (Asst. Professor)

Submitted by:
Sourabh, (IIT2017139)
Pratham Singh, (IRM2017006)
Joel Swapnil Singh, (ITM2017002)

Contents

1 Certificate from the Supervisor

I hereby declare that the project work entitled **"Face Spoofing Detection using Convolutional neural networks"** submitted at Indian Institute of Information Technology, Allahabad, is the bonafide work of **Sourabh (IIT2017139), Pratham Singh (IRM2017006) and Joel Swapnil Singh (ITM2017002)**. It is an authentic record of our study carried out from January 2020 till May 2020 under my guidance. Due acknowledgments have been made in the text to all the materials used. The project was done in full compliance with the requirements and constraints of the prescribed curriculum.

Dr. Triloki Pant
(Assistant Professor)
Department of Information Technology
Indian Institute of Information Technology Allahabad

2 Abstract

For face recognition systems, impostors can obtain legal identity authentication by presenting the printed images, the downloaded images or candid videos to the sensor. Since, the face is a unique biometric of the individual and face recognition is the superior identification method. This paper proposes a novel method for face spoofing detection by using binary classification. Binary classification on the basis of liveness which gives a good estimate of whether the face is real or brought in by any of the spoof techniques.

3 Introduction

Biometric systems are widely used for identifying or recognizing people on the basis of their physical features but these can be spoofed too using various traits. Biometric spoof attacks are becoming a larger threat, where a spoofed biometric sample is presented to the biometric system and attempted to be authenticated. Most recognition algorithms on the internet and research papers suffer from spoof attacks and these methods work really well. These can't distinguish between faces as fake or real as most of them work on 2D frames.

4 Motivation

It's no surprise that cybercrime is on the rise in our increasingly digital world. Many companies are now exploring biometric face recognition as a viable security solution based on machine learning. This innovative technology shows a lot of promise and could revolutionize how we access sensitive information.But as promising as facial recognition is, it does have flaws.

5 Problem Definition

Fraudulent users can subvert or attack a face recognition system by masquerading as a registered user and thereby gaining illegitimate access and advantages. Here we will be devising a methodology for creation of a face spoofing detector in order to distinguish fake and real faces in real time as much as possible.

6 Literature Review

Table 1: A summary of published methods on 2D face spoof detection.

Serial Number	Method	Strength(s)	Limitation(s)
1	Face motion analysis	Effective for print attack	Requires multiple frames, Slow response.
2	Face texture analysis	Relatively low computational cost and fast response	Poor generalizability, Requires face and/or landmark detection.
3	Face 3D shape or depth analysis	Effective for 2D attacks	Requires multiple frames or additional devices.
4	Image quality analysis	Good generalizability, Low computational Cost, Fast response time, Face and/or landmark detection not required	Image quality measures can be device dependent.
5	Frequency domain analysis	Good generalization ability, Low computational cost	Spectral features can be device dependent.
6	Active approach	Good generalizability	Requires additional devices.

Since our focus is 2D face spoof attack detection (on smartphones), we provide a brief summary and analysis of published 2D face spoof detection methods. Table 1 groups the published methods into six categories:
1. Face motion analysis
2. Face texture analysis
3. Face 3D depth analysis
4. Image quality analysis
5. Frequency domain analysis
6. Active methods.

Spoofing detection methods based on face motion analysis extract behavioral characteristics of the face, such as eye blink, and lip or head movement. These methods require accurate face and landmark detection to localize the facial components. Additionally, multiple frames must be used in order to estimate the facial motions. These methods are designed to detect print attacks, and thus are not able to handle video replay attacks with facial motions.

Spoofing detection methods based on face texture analysis capture the texture differences (due to

different reflection properties of live face and spoof material) between face images captured from live faces and face images captured from various spoof mediums (e.g., paper and digital screen). These methods can perform spoof detection based on a single face image, and thus have relatively fast response. However, face texture analysis based methods may have poor generalizability when using small training sets with a limited number of subjects and spoofing scenarios.

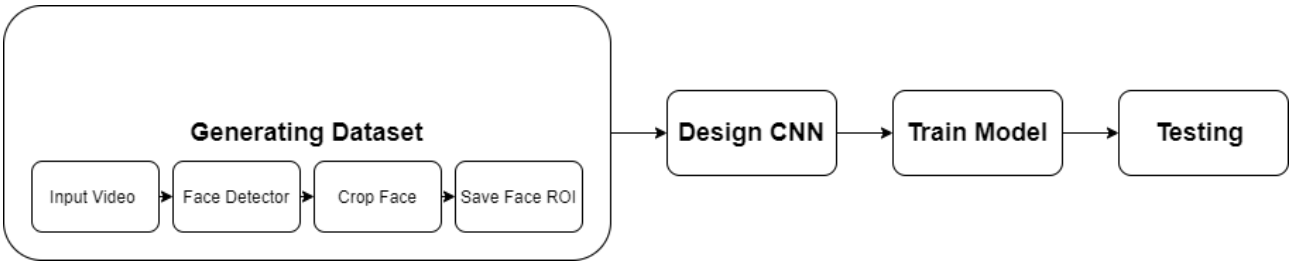
Spoofing detection methods based on 3D depth analysis estimate the 3D depth of a face to discriminate between 3D live face and 2D spoof face. While live faces 2Cross-database testing involves, training on database A and testing on a different database B, collected in a different setting from database A and with different subjects. This is in contrast to the easier, but, not realistic protocol of intra-database testing where, cross-validation is used on a specific database. are 3D objects, spoof faces presented on 2D planar medium are 2D. Thus, these methods can be quite effective to identify 2D face spoof attacks if the 3D depth information of a face can be reliably estimated. Face 3D depth analysis based methods usually rely on multiple frames to estimate the depth or 3D shape information of a face.

Spoofing detection methods based on image quality analysis utilize the image quality differences between live face images and spoof face images. Since the spoof face images and videos are generated by recapturing live face images and videos in photographs or screens, there will be degradations of color, reflection, and blurriness in the spoof face images compared to the live face images and videos. These methods have been found to have good generalization ability to different scenarios. However, studies on face spoofing detection based on image quality analysis are limited.

Frequency domain based anti-spoofing methods analyze noise signals in recaptured video to distinguish between live and spoof face access. During the recapture of printed photos or video replays, there is a decrease in low frequency components, and an increase of high frequency components. In order to quantize these changes, the input is usually transformed into the frequency domain.

Active methods utilize additional sensors, such as nearinfrared (NIR) and 3D depth to capture a face besides the 2D visual face image. While these methods provide better robustness against illumination and pose variations of the face, the use of additional sensors also limit their application scope, particularly in smartphone scenarios.

7 Proposed Methodology



7.1 Generating Dataset

The process of dataset creation can be done using online pictures but as our dataset will play a major role in training classifiers, we will require all input images of the same size. Hence to gain it we will create our own dataset of real and fake images using mobile camera and finally extracting the ROIs as per our interest.

7.2 Design CNN

We begin by designing a model with 2D convolution masking with matrix size of 3x3. Padding is set as the same to keep the dimension of output the same. Further activation used here is 'relu' to ensure the non-linearity of sample throughout the layers and avoiding the dimensional problems.To ensure that program works faster on huge sample using dropout to unset random values creating noisy values to overfitting and using batch normalization to reduce training dataset. Max pooling is used further by sliding feature maps and allowing assumptions to be made about features.

7.3 Train Model

While training our model will perform functions like splitting dataset for training and testing purposes separately normalizing pixels of dataset, dataset expansion for better results. Now we will run classifier to train sample dataset using CNN created.

7.4 Testing

After training our CNN classifier with the training dataset of images we will test the model with testing dataset in order to analyze the current performance. Analysis of time taken and accuracy can be done later.

8 Problem Faced

8.1 Creation of Dataset

1. Model will work for the person with skin tones near the trained model images of the person's skin tone. It requires training with multiple skin tone personalities under various lighting conditions to gain more accuracy.
2. It is assumed that videos used for dataset creation have one face throughout for better feature gathering.
3. Creation of self dataset using a video results in many duplicate sample images.

8.2 Designing CNN

1. Using lots of parameters for perfection will make implementation slow.
2. Overfitting can be a problem with more parameters.

8.3 Training and Testing

1. Dataset was quite small for plotting and accuracy calculations.

9 Results

Our Face Spoofing Detector was successful in distinguishing between fake and real faces, which utilize CNN that shows the same qualities as VGGNet-esque with only a few learned filters.

Accuracy	Misclassification Rate	Recall	Precision
0.95	0.05	0.98	0.95

10 Conclusion

Biometric spoof attacks are a larger threat, where a spoofed biometric sample is presented to the biometric system and attempted to be authenticated. Hereby, we conclude the methodology for face spoofing detection using CNN discussed here works amazingly with good accuracy results upto 95% on testing dataset. Our task of detecting faces being real or fake via webcam can be made more accurate with a wide dataset with various skin tones.

11 References

1. Saptarshi Chakraborty and Dhrubajyoti Das, "AN OVERVIEW OF FACE LIVENESS DETECTION" in International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014.

2. Keyurkumar Patel, Student Member, IEEE, Hu Han, Member, IEEE, and Anil K. Jain, Life Fellow, IEEE, "Secure Face Unlock: Spoof Detection on Smartphones", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 10, October 2016.