Fingerprint and Face Spoof Detection Using Deep Learning

Chiranshu Adik[1], Amey Waze[2], Samruddhi Tendulkar[3], Akansha Agarwal[4], Prof. Nikhil Dhavase[5]
[1,2,3,4] Student, MMCOE, Savitribai Phule Pune University, Pune, Mahrashtra, India
[2]Assistant Professor, MMCOE, Savitribai Phule Pune University, Pune, Mahrashtra, India

Abstract- **Fingerprint and Face recognition systems are widely used in various applications like Smartphone unlock, School attendance, Defense applications, Banks, etc. However these systems can be spoofed easily using various methods like fake fingerprints can be created using various materials like Fevicol, Silicon gel, Hot glue, rubber, paper-printed fingerprints, etc and fake face can be created using paper-printed faces or a smartphone device can be used as a fake image. While a number of face and fingerprint spoof detection techniques have been proposed, current solutions often rely on domain knowledge, specific biometric reading systems, and attack types. This paper proposes using convolutional neural networks for detecting a spoofed fingerprint or face.**

Since, CNNs currently outperform almost all other models for image recognition and classification. This paper proposes to use Google's Inception v3 model which was trained on a huge dataset (ImageNet dataset) and has better acuracy than most other models.

Index Terms- Deep Learning, Face recognition, Spoofing detection, Convolutional Neural Networks.

INTRODUCTION

Biometrics are currently widely used in various applications like authentication in smartphones, attendance management systems, access control system, banks, surveillance, and also in national and global security systems. Biometrics provide a very easy and fast authentication process speeding up the process of verification. It is also consider safe as it is rare for two people to have the same fingerprint or face.

1.1. Biometric Spoofing Techniques

In the last few years, various techniques have been found out to spoof or defeat these biometric systems. Attacks on biometric systems can be direct or indirect. Direct methods involve creating synthetic biometric samples acting at sensor level. While, Indirect methods involve methods like using matching algorithm, feature extraction procedures, accessing database and finding vulnerabilities in the network, etc refer

[1]. Generally, Direct methods are mostly use by hackers to spoof the biometric systems. This can be easily done as fingerprints of a person can be easily extracted with or without his permission.

The fingerprint traces can be found from the objects a person has touched and similar fake fingerprint can be generated and be used. These fake fingerprints can be created using the mould of the fingerprint and these moulds are then used to create fake fingerprints using materials like gelatin, silicon gel, fevicol, hot glue, rubber, play-doh, etc.

In the context of faces, a person's fake face can be easily generated using photographs or smartphones/tablets. There are methods that can be used to create face masks of a person using his photographs.

1.2. Other Anti-Spoofing Techniques

Traditional anti-spoof techniques have been developed which require expert-knowledge and are mostly dependant on modality for which they were developed. If a slight change is made in spoofing technique the system needs to be redesigned completely. Various techniques involve using sensors like sweat detection, temperature detection, etc. that will sense if the applied fingerprint is live.

For detecting a fake face, recently apple introduced a new method in their iphone X's face recognition system. It uses techniques like number of data points, uses of infrared scanning and attention awareness, refer [2].

1.3. Deep Learning for Spoof Detection

This paper suggests using Deep Neural networks for detecting a spoofed fingerprint or face. Deep learning has proven to be successful in various AI applications. This is mainly because in the past few years huge amount of data has been collected. This data can then be used to train machine learning models. Neural networks give very high accuracy if they are trained with huge data. Convolutional Neural Networks are inspired from human visual cortex and are usually used for image recognition and classification. CNNs have layers of Convolution and pooling operations that are used for feature learning. The next part is a fully connected layer of neurons responsible for classification.

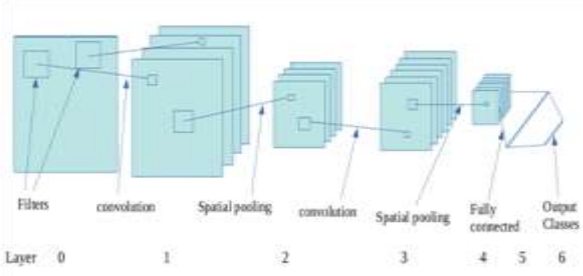

Fig. 1 Convolutional Neural Network.

1. CONVOLUTIONAL LAYERS

They are responsible for learning features from the image. Convolution layers are unique as they do not connect all neurons together [3].

2. FULLY CONNECTED LAYERS

Fully connected layers are responsible for actual classification process. In these layers all the nodes of a layer are connected to all the nodes of its previous layer [3].

3. SOFTMAX FUNCTION

A softmax function is usually used in the final layer of a NN. It is generalization of logistic function that squashes the K dimensional vectors to values in range of 0 to 1 that add up to 1. It gives a categorical distribution among the categories and we get the probability of a certain category [3].

2. INCEPTION MODEL

Inception-v3 is a convolutional neural network model consisting of 48 layers. It was developed at Google to provide state of the art performance on Image Net Large-Scale Visual Recognition Challenge. It is computationally more efficient than its competitor architectures [4]. This paper proposes to use Transfer Learning for training the CNN. The inception-v3 model was trained on 1.2 million images from thousands of categories. Training inception-v3 took about 2 weeks on a fast desktop with 8 GPUs. Transfer Learning allows use to reuse the parameters inception has previously learned. Hence, we can create high accuracy classifier with far less training data. Also, training time required using Transfer learning is much less as compared to training CNN from scratch.

3. EXPERIMENTAL RESULTS

3.1. DATASETS

3.1.1. FINGERPRINT DATASET

The inception model was trained with ATVS-FakeFingerprint database (ATVS-FFp DB) [5]. It contains fingerprint samples of the index and and middle fingers of both hands of 17 users (17 × 4 = 68 different fingers). These images were taken from three different sensors (flat optical sensor Biometrika Fx2000, sweeping thermal sensor Yubee and capacitive sensor Precise 100 SC). These images were taken with and without cooperation of the user. The whole dataset comprises of 1632 and 1536 images taken with and without cooperation respectively.

3.1.2. FACE DATASET

The face dataset was created using faces of 10 different people. Short videos of 10 seconds were captured in three different light conditions (Dark room, well lit room, room with too much light). These videos were then split to 100 images each.

Fake images were created by taking pictures of the picture in a smartphone.

This dataset contains 3000 real and 3000 fake face images.

3.2. RESULTS

The below results were obtained after training the inception model using the datasets mentioned above.

Table 1. Training Accuracy of Face and Fingerprint on Inception-v3 model

Model	Training Accuracy
Fingerprint Spoof Detection	99.2%
Face Spoof Detection	99.6%

3.3. EQUIPMENT USED

Fingerprint sensor used for testing the Fingerprint spoof detection was Nitgen eNBioScan-C1.

The face images were captured using a laptop camera (1.3MP) and a smartphone camera (5MP).

4. CONCLUSION

Face and Fingerprint authentication systems are widely used in various applications. Since there are various simple techniques with which we can easily spoof or fake the system, there is a need to develop anti-spoofing technologies to secure our systems. There are methods which we can detect the livelinessof a fingerprint or face. But these are very condition and problem specific. They may not give accurate output if some new type of input is given. We may then need to change our whole system to adapt new conditions. Using CNNs, accurate results can be obtained even in different conditions. On training the Inception-v3 model with face and fingerprint datasets, training accuracy of 99.6% and 99.2% was achieved. Also, CNNs currently outperform almost all other Machine Learning models for object classification and recognition. Hence, CNNs can provide very good results if trained with enough amount of data.

5. ACKNOWLEDGMENT

The authors would like to thank Prof. Nikhil Dhavase for his support and guidance throughout the project.
They are also grateful to The Autonomous University of Madrid for providing the fake fingerprint dataset (ATVS-Ffp DB) needed for the experiments.

REFERENCES

[1] D. Menotti, G. Chiachia, A. Pinto, W. Schwartz, H. Pedrini, A. Falcao, A Rocha “Deep Representations for Iris, Face, and Fingerprint Spoofing Detection” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 4, APRIL 2015.

[2] ‘Face ID on the iPhone X: Everything you need to know about Apple’s facial recognition’. Available:https://www.macworld.com/article/3225406/iphoneipad/face-id-iphone-x-faq.html
‘Learning AI if You Suck at Math’. Available: https://hackernoon.com/learning-ai-if-you-suck-at-math-p5deep-learning-and-convolutional-neural-nets-in-plainenglish-cda79679bbe3

[3] ‘ImageNet: VGGNet, ResNet, Inception, and Xception with Keras’. Available: https://www.pyimagesearch.com/2017/03/20/imagenetvggnet-resnet-inception-xception-keras/

[4] ATVS-FakeFingerprint database (ATVS-FFp DB), Universidad Autonoma de Madrid, SPAIN.

[5] E. Marasco, P. Wild, B. Cokic “Robust and Interoperable Fingerprint Spoof Detection via Convolutional Neural Networks.”

[6] D. Wen, H. Han, A.Jain “Face Spoof Detection with Image Distortion Analysis,” in IEEE Transactions on Information Forensics and Security, 2015.

[7] M. Sharma, “Detection and Prevention of Fingerprint Altering /Spoofing Based on Pores (Level-3) with the Help of Multimodal Biometrics” in IJSR 2012.

[8] 'Convolutional Neural Network'. Available: https://github.com/llSourcell/Convolutional_neural_network/blob/master/convolutional_network_tutorial.ipynb