Turkish Journal of Computer and Mathematics Education Vol.12 No.12 (2021), 3534-3537

Research Article

Liveness detection in Face Recognition using Deep Learning

Bali Shankar Khurana
Assistant Professor, MCA Department, PCCoE, Pune

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract: In the last few years face recognition has received a lot of attention. Recently face authentication has become very popular since it is easy to use and face recognition technologies have achieved good performance. Face biometric systems are widely used for recognizing the true identity of enrolled person on the basis of physiological appearances and behavioural patterns. However, this can be spoofed by nefarious users trying purposely to by-pass face recognition on system using various traits like photo or video of the person held in front of the camera may be accountable for performing face recognition. Using anti-face spoofing methods in our facial recognition framework, we tried to detect "real" or "fake" faces. By detecting possible spoofing attacks like placing 3D printed photo, eye & mouth photo imposter and video of a person in front of the camera, the proposed method improves liveness accuracy results.

Keywords: Liveness Detection, Face Spoofing Detection, Anti-face spoofing

1. Introduction

The main objective of our proposed work was to distinguish between "Actual" and "Non Real" faces by using anti-face spoofing algorithms. We have used Convolution Neural Network algorithm which is widely used for image processing work and implemented in the application using python programming with OpenCV, Keras and Tensorflow framework. We have studied various existing systems which generally involve image capture of users from the camera, Face detection, Feature Extraction, Matching features stored in the database and finally determine identity if there is a match or not. The problem with these systems is they are prone to the spoofing attacks. Facial data used in biometrics can easily be stolen from social platforms or online communities and used for device spoofing. Playing video or placing a 3D dummy mask of the user in front of the camera may also be used to spoof the user's face. Integrated liveness detection may be used to solve certain problems where physiological signs of life are present in the database. For a given image input, we trained a CNN for distinguishing real faces from unreal faces.

2. Review of Literature

Face Liveness detection is the term used to refer if the face has features of motion, texture and life signs. Liveness detection is a process to determine whether a detected face is real or not before a face recognition system identifies the face. It prevents the face recognition system from making a wrong decision. There are several types of spoofing faces, such as 2D printed photos, videos, high-definition (HD) tablets, 3D masks, and so on. Among them, 2D photos are used widely because they are easy and cheap to obtain. To minimize the vulnerability against 2D attacks, researchers have shown steady progress in developing anti-spoofing technologies based on features of 2D photos **[1].** There are some characteristics in recaptured 2D photos. First, detailed components and sharpness are lost. In this case, researchers analyze texture and frequency components in the input data. In order to represent the textural feature, local binary patterns (LBP) are often used over face regions and using an SVM to classify the faces as real or spoofed. **[2, 3].** Bai et al**. [4]** calculate secularity components from the input data there are a number of approaches to liveness detection which includes

Komulainen et al. **[5]** suggest a countermeasure with the fusion of motion and micro-texture analysis methods. The last approach is based on 3D facial information. Based on type of liveness indicator face liveness detection can be separated into three main categories i.e. (a) Motion Analysis (b) Texture Analysis and (c) Life Sign Detection **[1].** Kant et al. **[6]** present a real-time solution using a thermal image and skin elasticity of a human face.

Most researchers utilized eyeblink as it is an essential function of eyes. For effective and more reliable face liveness detection combined biometric traits could be utilized instead of system based on capturing only eyeblink. **[7].** Convolutional neural networks are specifically designed to work with problems involving images as inputs. CNNs can be used to solve machine learning or data mining problems wherein inputs can be represented by an image or a set of images. CNNs can be visualized as a modified version of multi-perceptron neural network model **[9]**

3. Methodology

In order to implement liveliness in face recognition, we have used Python programming which has a rich library to build solutions much faster. For deep learning model design and training we used the Tensorflow framework and

Keras which provide high level API binding to Tensorflow. Building and training models in Keras is much easier. For image reading we used OpenCV library and Numpy library for array operations, like re-scaling image array, transforming array etc.
We have tested CNN and ResNet architecture for liveness, CNN gives better results than ResNet, so in the final solution we used CNN. CNN requires a lot of data to generalize the model. Model generalization reveals how a deep learning model behaves on unknown data, which necessitates a large amount of data for CNN.

To generalize the model we collected, processed and trained our framework with 1.7 million images.
The data was split into two parts: 80 percent for training and 20% for validation.To minimize training time, we used the idea of transfer learning. For faster training and inference, we used a lightweight MobileNet model.
We have collected a large scale dataset from public release. Included Raw image size: 1.2 TB from LCC-FASD extended, NUAA Imposter, CASIA anti spoof, CelebA-Spoof. CelebA-Spoof contains over 0.6 million images, and covers various light conditions, environments, and illumination conditions. CelebA-Spoof is used to train and evaluate algorithms of face anti-spoofing. NUAA Photograph Imposter Database for face detection and geometric normalization. CASIA_faceAntispoof and LCC FASD datasets for false facial verification by using a photo, video. LCC-FASD extended dataset contains only live images captured using a mobile, we have generated spoof data from it.

Work flow of the proposed framework

We have divided the approach into two parts, first face detection and second one liveness detection.

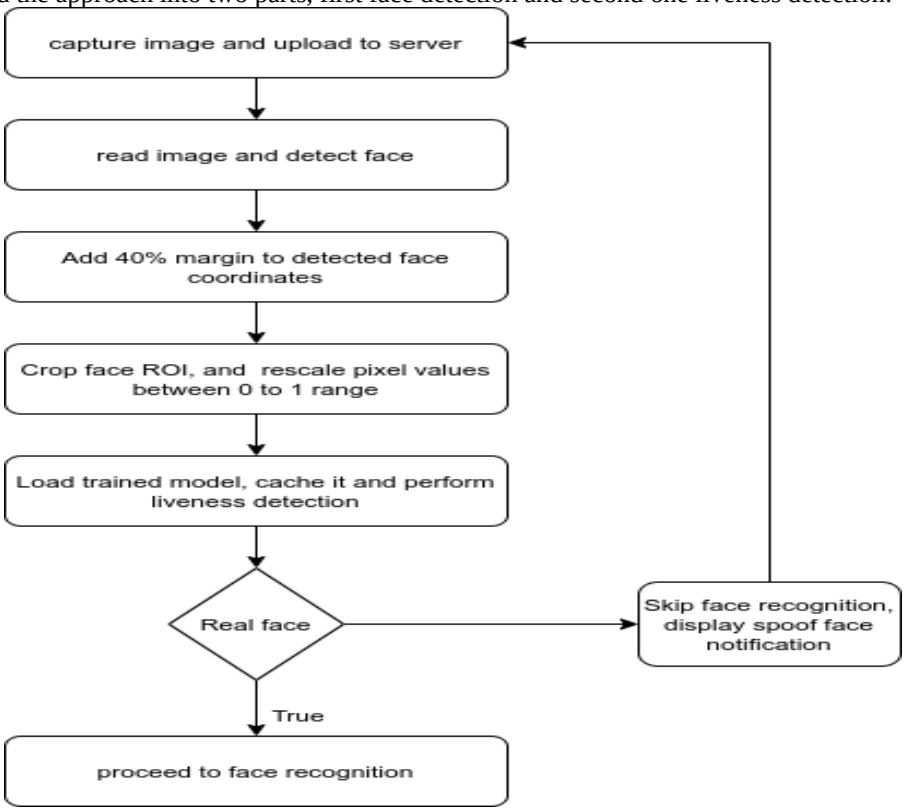

Figure 1: working model of Liveness detection

First face detection will be performed on the user photo. We tried different face detectors such as Opencv Haar cascade, dlib's hog and CNN based detector, SSD-ResNet, Multi-task CNN and retina-face detector. Retina-face detector given most accurate results among others, so we used retina-face. Retina face detects faces and returns a bounding box, after that the bounding box will be extended by a factor 0.4 to include the whole head, some background etc. based on extended bounding box coordinates face area will be cropped, resized to 300x300 and will be passed to CNN model as input for liveness detection.

Then liveness of the user is tested using CNN. If a person is live then the system will recognize the identity else reject it. Applying deep learning to automatically extract features, transfer learning and integrate domain generalization has resulted to improve spoofing detection.

Steps of Training Process

a) Collect dataset and clean it by removing noisy and wrong label images
b) Apply face detection on each image in the whole dataset and crop face and store cropped face in directory.
c) Load cropped face directory using Keras image data generator.
d) Split dataset into training and validation set.
e) Setup dataset augmentation pipeline using Keras
f) Build model, add models callback to save checkpoint on each epoch and start model training.
g) Visualize model accuracy and compute other accuracy metrics
h) Save model if checkpoint callback not enabled.

4. Result and Discussion:

We have used Keras framework to build and train liveness model. At training time we have used Horizontal flip, random scaling, random rotation, random brightness, and random contrast augmentations.

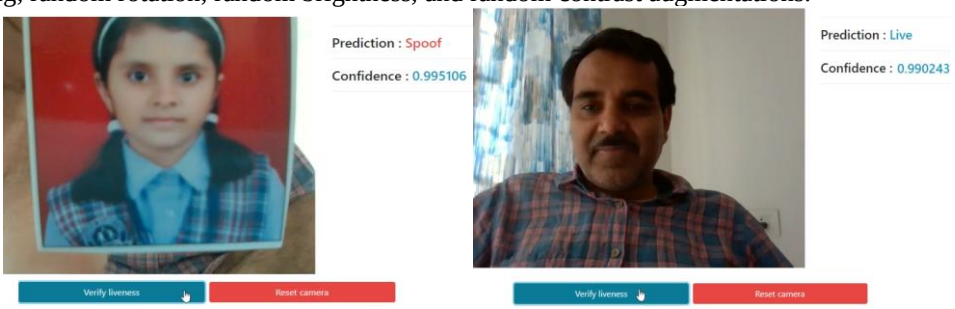

Figure 2: Liveness detection

Using this liveness detection we can not only spot live face or photo/video faces but also indicate the percentage of liveness features matching and identify live/spoof in face recognition systems. We have created our own dataset of 30 thousands images in size 300 x 300 to train our Neural Network to improve the performance of system and observed liveness detector was able to obtain overall 99% accuracy on validation set.

The results show that system can respond to the cross detection of more unknown databases to some degree, reduce over-fitting, and achieve successfully detect unseen spoofing attacks using domain generalization. However there are still some issues that domain generalization would preclude the training and impact on a single data set from achieving its optimum state, necessitating the enhancement of the network system.

Training and validation accuracy graph: Loss graph:

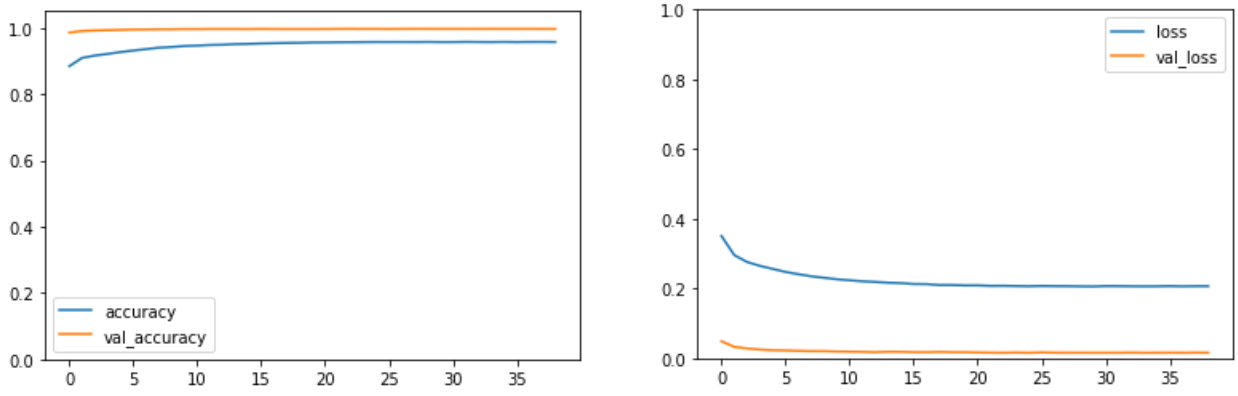

Figure 3: Training and validation graph:

5. Conclusion

We studied methods of spoofing face recognition used for authorization, with a focus on photo and video spoofing. Owing to the lack of normalization or self-quotient picture such as back tilting, slanted images and rotations, the hamming distance seems to tolerate further spoofs in these situations, resulting in a higher number of false positives. Other problems that have been observed are variation of brightness or electronic noise on images may costs the texture information. Eye glasses may cause reflection. In the proposed project we have used several liveness indicators which considerably improves the reliability of face recognition system and guard against spoofing.

The accuracy in Liveness detection may further help to develop models for detecting the emotions on faces. Our main aim is to provide a straightforward roadmap for the potential creation of more reliable, user-friendly, and effective methods for detecting face liveness.

References

1. Kähm, O.; Damer, N. 2D face liveness detection: An overview. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 6–7 September 2012; pp. 1–12.
2. Kim, G.; Eum, S.; Suhr, J.K.; Kim, D.I.; Park, K.R.; Kim, J. Face Liveness Detection Based on Texture and Frequency Analyses. In Proceedings of the 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 29 March–1 April 2012; pp. 67–72
3. Määttä, J.; Hadid, A.; Pietikäinen, M. Face Spoofing Detection from Single Images Using Micro-Texture Analysis. In Proceedings of the 2011 International Joint Conference on Biometrics, Washington, DC, USA, 11–13 October 2011.
4. Bai, J.; Ng, T.T.; Gao, X.; Shi, Y.Q. Is Physics-based Liveness Detection Truly Possible with a Single Image? In Proceedings of the 2010 IEEE International Symposium on Circuits and Systems (ISCAS), Paris, France, 30 May–2 June 2010; pp. 3425–3428.
5. Komulainen, J.; Hadid, A.; Pietikainen, M.; Anjos, A.; Marcel, S. Complementary countermeasures for detecting scenic face spoofing attacks. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–7.
6. Kant, C.; Sharma, N. Fake Face Recognition Using Fusion of Thermal Imaging and Skin Elasticity. IJCSC 2013, 4, 65–72.
7. Singh, M., Arora, A.S. A Novel Face Liveness Detection Algorithm with Multiple Liveness Indicators. Wireless Pers Commun 100, 1677–1687 (2018)
8. Khurana, B. S. (2018). IT initiatives in power distribution sector. International Journal of Advanced Science and Research, 15-18.
9. "CS231n Convolutional Neural Networks for Visual Recognition", Cs231n.github.io, 2017. [Online]. Available: http://cs231n.github.io/convolutional-networks/. [Accessed: 08- Apr- 2017].
10. Pan G, Wu Z, Sun L. Liveness detection for face recognition. Recent advances in face recognition. 2008 Dec 1:109-24.
11. Khurana, B. S. (2016). Research on Detecting Faults Based on Internet Control Message Protocol. The International journal of Science and Technoledge, 3.
12. X.Tan, Y.Li, J.Liu and L.Jiang. Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model, In: Proceedings of 11th European Conference on Computer Vision (ECCV'10), Crete, Greece. September 2010