IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 5, Ser. III (Sep. – Oct. 2020), PP 16-20
www.iosrjournals.org

Deep Transfer Learning for Face Spoofing Detection

Dr. Yogesh Kumar Sharma[1]
Associate Professor & Head, Department of Computer Science and Engineering,
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India.

Ms. Sujata Pandurang Patil[2]
Research Scholar, Department of Computer Science and Engineering,
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India.

Dr. Ranjit D. Patil[3]
Vice-Principal and Head, Department of Computer Science, Dr. D.Y. Patil ACS College, Pimpri, Pune, Maharashtra, India.

Abstract:
In recent years, the biometrics systems gained more popularity in the identification of the individual. In the biometric systems, the face is a widely used biometric trait in the authentication and surveillance systems. As the usage of face biometric traits getting increased in face recognition, the system becomes more vulnerable to spoofing attacks. In computer vision, the new techniques, algorithms, and advanced approaches are used for better accuracy and performance to develop the models that can be used in the anti-spoofing to tackle any kind of spoofing attack.

In this paper, we have has implemented the module to detect face anti-spoofing attacks that may possible through printed or mobile photos by the imposter. To implement this module the deep neural network and transfer learning approach is used. The pre-trained models are used to train the anti-spoofing module for detecting spoofing attacks. The different models are trained and tested on the NUAA dataset and the model with the highest accuracy is used in the anti-spoofing module. In this research paper, we have used the VGG16 model to detect spoofing attacks. The highest validation accuracy was achieved for VGG 16 model 100% on the NUAA dataset.

Keywords: *Face Recognition, Biometric, Face Spoofing, NUAA dataset, Transfer Learning.*

Date of Submission: 10-10-2020 Date of Acceptance: 26-10-2020

I. Introduction

In the recent era due to the advancement in technology, the usage of biometric systems like face, fingerprint, and vein pattern gets increased in the number of applications such as image database and forensic investigation, airport, border control, health care, education sector, and in surveillance systems [1]. In the surveillance systems, face recognition is used for identification and authentication purpose. In the authentication system mainly, the face is used as a biometric trait. The face biometric trait becomes more popular because as compared to the other biometric systems such as fingerprint, vein, or palm the face is the non-invasive biometric trait used for the identification of a particular individual. Nowadays the advanced face recognition algorithms are used for obtaining the accuracy in the authentication process. The face recognition system identifies and authenticates the individual but the system cannot find out the difference between the fake user and real user identity. Although the face recognition system is used for authentication purpose the system is more vulnerable to face a spoofing attack. Hence, there is a need to train the system which can recognize the individual and it should also able to detect liveness when the user submits the identity for authentication and authorization to gain access.

❖ Face Spoofing

A facial spoof attack is a process in which a fraudulent user attacks the face recognition system by disguising as an original or authorized user and thereby gaining unauthorized access and benefits [2].The face spoofing attack can be done by the unauthorized user by collecting the original user's data such as photographs, videos through social media or by capturing photos on Mobile. The fake evidence can be used by an illegal user to gain access. The face spoofing attacks are categorized in 2D and 3D spoof attacks. The 2D spoof consists of a photo and Video attack and in a 3D spoof; the fraudulent user can do the attack by using a mask [3]. The attacker can use the 3D mask of the authorized user's made up of either plastic or paper to access the system. In this research work the 2D photo and mobile attack considered during anti-spoofing model creation. The deep learning and transfer learning approach is used to develop the model. This paper is organized in the following sections. The literature review described in section II, Section III, describes the proposed methodology and dataset used in the model training process, Section IV explains VGG 16 model, Section V presents the experimental evaluation of VGG 16 model and Section VI concludes with the conclusion and future scope.

II. Literature Review

In this research field, to detect the face spoofing attack many researchers have already given their contribution to detecting the various types of spoofing attacks. But still, there is a chance to improve the accuracy and performance of the systems. The researcher has reviewed the previous work done under this field. In this section, some of the work revealed that uses different algorithms and techniques against spoofing attacks. Abdulkadir Sengur et al. [4] presented a paper on Deep feature extraction using liveness detection. This paper describes the CNN model used to detect the face spoofing. The model trained on publicly available two datasets NUAA and CASIA-FASD. The experimental results obtained are good and presented in the result section. Sandeep Kumar et al. [5] have discussed different spoofing attacks such as photo, video, and mask attack. To detect the spoofing attack the different anti-spoofing techniques and databases used for training the model are studied and compared by the author. M. Killiogluet al. [6] has focused on Liveness detection using pupil tracking in the research paper. The eye region extracted using Haar-Cascade Classifier and feature points are extracted using the Kanade-Lucas-Tomasi (KLT) algorithm. The author has developed an algorithm and tested successfully for liveness detection.

III. Methodology

The researcher has used deep learning and transfer learning approach to build the face anti-spoofing module to detect the face spoofing attack. The pre-trained model VGG 16 is used that is already trained on a large ImageNet dataset. The model is customized by modifying the last layers and again re-trained on the NUAA photo imposter dataset [7]. The trained model is used to solve the binary classification problem to classify or predict the fake and real class of users. To detect the face from the image we have used the MTCNN algorithm [8] and to extract the feature embeddings the FaceNet model is used from the transfer learning [9]. To build the model Keras library and TensorFlow are used. The Keras used as the front end and TensorFlow used as backend in the model building process. The proposed model of face anti-spoofing is shown in Figure 1. The steps used to build the anti-spoofing model are as follows:

1. Initially, the NUAA photo imposter dataset is loaded and different data pre-processing steps are applied on the dataset.
2. In the data preprocessing step, the normalization and label encoding process used to bring the data in a numerical format, and appropriate encodings are assigned to the data.
3. After applying the pre-processing steps, the data split into a training set and testing set in the 80:20 ratio respectively.
4. The transfer learning VGG 16 model is created by customizing the last dense layer and the two classes are added fake and real at the output layer.
5. The model is trained on the NUAA photo imposter dataset and then evaluated for training accuracy.
6. The trained model again validated on test dataset to evaluate the validation accuracy of the model.
7. The developed model is saved and loaded to evaluate the fake and real class of users.

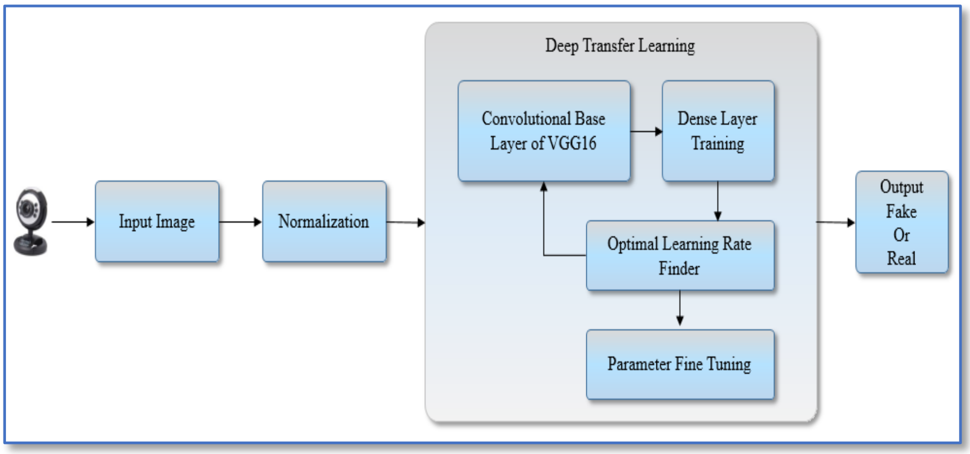
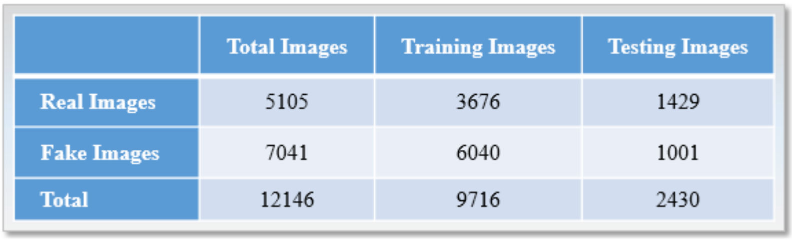


Figure 1: Face Anti-Spoofing with VGG 16 Model Using Transfer Learning

- **Dataset Formulation**

In the training and validation process of the anti-spoofing module, we used the NUAA photo imposter dataset. The training and validation samples used in training and validation of the process of model distributed as shown in Figure 2. The dataset consists of a total of 12146 images out of that 5105 from real class and 7041 images from fake class. In this research work, the printed photo and mobile photo spoof attack are considered. To train and test the model fake and real images are used from the dataset. The data preprocessing applied to the data to deal with missing data from the dataset. After checking the missing data, the next step used data labeling and encoding for categorical data. This step ensures that the dependent variable is converted into binary form 0 and 1. The data preprocessing and label encoding step completed, then the dataset is divided into two sets. The 80% of data used for training the model and 20% data used for validation purposes. The model used for face anti-spoofing is the VGG 16 model that is trained on the total number of 9716 samples out of those 3676 real images and 6040 fake images. The testing phase contains 2430 total images used in the validation phase. Out of that 1429 real images and 1001 fake images.



	Total Images	Training Images	Testing Images
Real Images	5105	3676	1429
Fake Images	7041	6040	1001
Total	12146	9716	2430

Figure 2: Training and Validation Samples Distribution in NUAA Dataset

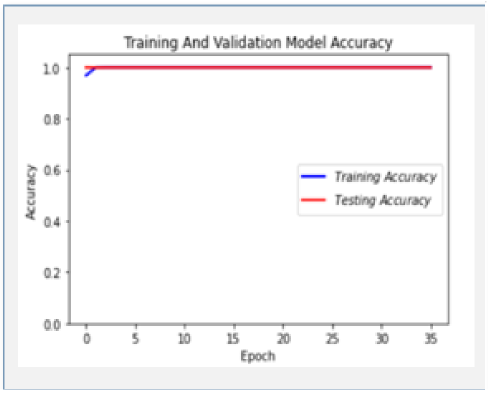
IV. Building VGG 16 Architecture For Face Anti-Spoofing

The Visual Graphics Group (VGG) 16 networks are pre-trained network trained on ImageNet Dataset [10]. The VGG 16 model is 16 layers deep and used for the extraction of features, and prediction of classes. This model was presented in 2014 in the research paper, Very DNN for Large Scale Image Recognition [11]. In this research work, to develop the model to detect the spoofing attack, the transfer learning approach is used. The last layers of the VGG 16 model are modified and again the model re-trained on the NUAA photo imposter dataset to detect the spoofing attack and to predict the classification of the user. The model is already trained on a large dataset with different categories of images so even on a small dataset this model achieves good accuracy. To extract the features from the input image this neural network model is used. In this research paper, this VGG 16 model is used to predict the fake and real user by detecting the printed or mobile photo spoof attack during authentication.

V. Experimental Result Evaluation Of VGG Model

The VGG 16 model is developed by using Keras and TensorFlow as backend. The various libraries are used from python and Keras library to build the model. In this section, the experimental results are explored related to the anti-spoofing model. This VGG 16 model is trained by using the NUAA dataset through 35 epochs with batch size 64. The by default learning rate is set to 0.0001. The value of the cost function is optimized by using the adam optimizer. The SoftMax classifier is used for the classification of a fake and real class of users.

The result of the experimental evaluation is discussed below. The training and validation accuracy obtained for VGG 16 model is 100% is shown in Figure 3.The training and validation loss of the model is shown in Figure 4.



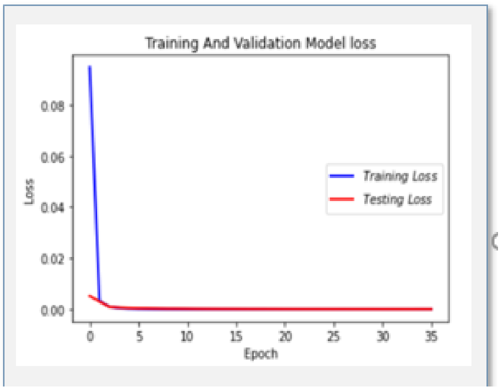


Figure 3: VGG 16 Model Training and

Figure 4: VGG 16 Model Training and

- **Validation Accuracy Plot Testing Loss Plot**

The training and testing validation loss value of the VGG 16 model is zero. In the anti-spoofing module, the researcher has passed the real-time input image captured through the camera. In the transfer learning model, the input image size required 224 × 224 pixels. Initially, the captured image is passed to the MTCNN algorithm to detect face boundaries and after cropping that face region the facial region passed to the FaceNet model to extract the features.

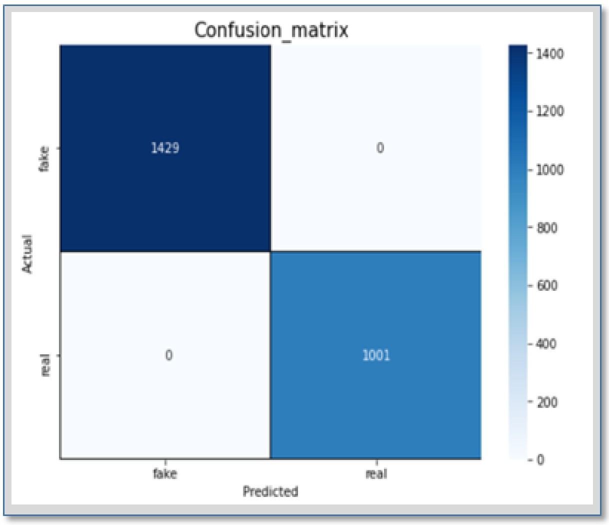


Figure 5: VGG 16 Model Confusion Matrix for Anti-Spoofing

After feature extraction, depending upon two classes passed at the output layer the model classifies between fake and a real class of user. The transfer learning VGG 16 model is evaluated by using the different performance metrics such as validation accuracy and confusion matrix. As we have seen the training and testing accuracy obtained after training and testing the model is highest. The confusion matrix for VGG 16 model is shown in Figure 5. To solve the binary classification problem the researcher has used a two-class confusion matrix to calculate the precision, recall value, and misclassification rate of the model. In the confusion matrix it has been observed that out of total numbers of 2430 images used in the testing phase, all the images are correctly predicted by the model. The false-positive and false-negative values are not present in the confusion matrix. The model correctly predicts the fake and real class of users.

From the confusion matrix, it has been observed that the precision value and recall value obtained is 100%. Both the values are the same means that there is the absence of Type I and Type II error. Hence, the model correctly predicts and classifies the real and fake class of user. The output of the VGG 16 model is tested by using a single image of the fake user and real user. The model correctly classifies the fake and real class of users.

To solve this binary classification problem the researcher has used deep learning and pre-trained model from transfer learning. The training time is reduced because the model is already trained on the ImageNet dataset. The researcher has observed by using a small anti-spoofing NUAA dataset in the experimental results 100% accuracy is obtained. The precision and recall value obtained is also highest.

VI. Conclusion and Future Scope

The experiment is performed to develop the anti-spoofing module by using Keras and TensorFlow. The model is trained by using Google Colab to get faster output during the training process. The VGG 16 model achieved 100% accuracy, precision, and recall value on the NUAA dataset to detect the spoofing attack. This developed VGG 16 model is used to detect the face anti-spoofing attack done by an intruder by using either photo print or mobile photo. In the authentication system, where the identification is done through face recognition, this customized model is capable to detect the spoofing attack during face recognition. This model works for photo print and mobile photo spoof attacks. In further research, the model can be extended to detect mask and video attack during face recognition.

References

[1]. Krishna Dharavath, F. A. Talukdar, R. H. Laskar (2013), “Study on Biometric Authentication Systems, Challenges, and Future Trends: A Review”, 2013 IEEE International Conference on Computational Intelligence and Computing Research, ISBN: 978-1-4799-1597-2, pp. 1 - 7

[2]. Anjos, A., Marcel, S.: ‘Counter-measures to photo attacks in face recognition: a public database and a baseline’. Int. Joint Conf. Biometrics (IJCB), 2011

[3]. Javier Galbally, Sébastien Marcel (member IEEE), and Julian Fierrez, “Biometric Anti-spoofing Methods: A Survey in Face Recognition”, In the Proceedings of the 2014 IEEE Access Publication, 10.1109/ACCESS.2014.2381273,2014.

[4]. Abdulkadir Sengur, Zahid Akhtar, Yaman Akbulut, Sami Ekici, Umit Budak (2018), “Deep Feature Extraction for Face Liveness Detection”, International Conference on Artificial Intelligence and Data Processing (IDAP), ISBN: 978-1-5386-6878-8, pp. 1- 4

[5]. Sandeep Kumar, Sukhwinder Singh, Jagdish Kumar (2017), “A Comparative Study on Face Spoofing Attacks”, International Conference on Computing, Communication and Automation (ICCCA2017), ISBN: 978-1-5090-6471-7, pp. 1104-1108

[6]. M. Killioglu, M. Taskiran, N. Kahraman (2017), “Anti-Spoofing in Face Recognition with Liveness Detection Using Pupil Tracking”, 15th International Symposium on Applied Machine Intelligence and Informatics, ISBN: 978-1-5090-5655-2, pp. 000087- 000092

[7]. X. Tan, Y. Li, J. Liu, L. Jiang, Face liveness detection from a single image with the sparse low-rank bilinear discriminative model, in Proc. ECCV, 2010, pp. 504–517.

[8]. Kaipeng Zhang, Zhanpeng Zhang, Zhifeng Li (2016), “Joint Face Detection and Alignment Using Multi-Task Cascaded Convolutional Networks”, IEEE Signal Processing Letters, Vol. 23, No. 10, ISSN: 1070-9908, pp. 1499-1503

[9]. FaceNet: A Unified Embedding for Face Recognition and Clustering Florian Schroff, Dmitry Kalenichenko, James Philbin

[10]. ImageNet http://www.image-net.org

[11]. Simonyan, K. and Zisserman, A. (2015). Very deep Convolutional networks for large-scale image recognition. arXiv:1409.1556 [cs.CV]

Dr.Yogesh Kumar Sharma, et. al. “Deep Transfer Learning for Face Spoofing Detection.” *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22(5), 2020, pp. 16-20.