A deep CNN based approach for liveness detection in maritime digital KYC processes

Narayanan Arvind[a], Saravanan Mugund[b], Dr. Avinash Kumar Singh[b]

[a,b]Intain AI Pvt. Ltd.

Abstract

Maritime digital KYC processes are susceptible to various face spoofing attacks. When any unauthorized person tries to enter in the authentication system by presenting a fraud image and/or video, it is termed as a spoofing attack. Face anti-spoofing attacks have been typically approached from texture based models (e.g. Local Binary patterns) combined with machine learning (e.g. KNN) approaches. The aim of this study is to build a robust face anti-spoofing system using deep convolutional neural networks for maritime digital KYC processes. The research is based on analyzing the features of genuine and fake images. We use the freely available NUAA photograph imposter database for our face anti-spoofing study. The database has respectively 7500 and 5100 labelled imposter and client face images. We split the dataset into train and test sets with an 80%-20% split ratio using stratified sampling. 2D convolutional layers combined with 2D MaxPooling layers followed by Flattening and Dense layers are employed for our deep network architecture. The research is carried out using scikit-learn and keras open-source libraries for python. The training accuracy of the reported model is 100% and the testing accuracy is 99.92%. The accuracy of our present deep learning approach surpasses the accuracy of all the models available in literature.

Key words: CNN, Liveness detection, Maritime KYC, digital KYC, face anti-spoofing, Local binary patterns, KNN, NUAA, stratified sampling, scikit-learn, keras, python

[a] Corresponding author, Email: arvind.narayanan@in-d.ai Tel: +91-8349232657

B.Tech. / M.Tech. IIT Kharagpur (Dept. of Ocean Engineering and Naval Architecture)

1. Introduction

Maritime digital KYC processes are susceptible to various face-spoofing attacks. Unauthorized agents may try to enter the system by presenting fraudulent images and/or videos. Typical attacks include image/video presentation attacks and masking attacks. Masking attacks involve the use of a 3D mask by a fraudster and is beyond the scope of this study. We focus on presentation attacks, where an image of the client image/video is presented for fraudulent purposes. The textural features of this 2D image-of-an-image are significantly different from the 3D human face textures captured by the original image. Parveen et.al. [3] study face liveness detection from a complete local binary patterns perspective. Local Binary patterns extract textural features from an image which can then be used to classify images using k-nearest neighbors or other machine learning algorithms. Parveen et.al. [2] study dynamic local ternary patterns to replace local binary patterns and carry our similar studies as [3]. Benlamoudi et.al. study face anti-spoofing using local binary pattern descriptors and fisher score. Tan et.al. [1] study a Lambertian model to represent the client and imposter images in a vector space. The binary classification problem thus posed is solved using a sparse logistic regression model. Most of the studies available in the literature for face anti-spoofing focus on extracting features from the input images and then classifying them according to a suitable technique. To our knowledge, this is the first complete end-to-end trainable deep convolutional network model available for this task.

2. CNN network for face anti-spoofing

2.1 Preprocessing

We start by resizing all the face images in the NUAA dataset to a size of 224 x 224 x 3. The dataset is then split into train and test sets with 80%-20% split ratio using stratified sampling to preserve the original ratio of samples in both the classes. Label encoding followed by one hot encoding of the target variables is carried out for classification using the CNN network.

2.2 Architecture

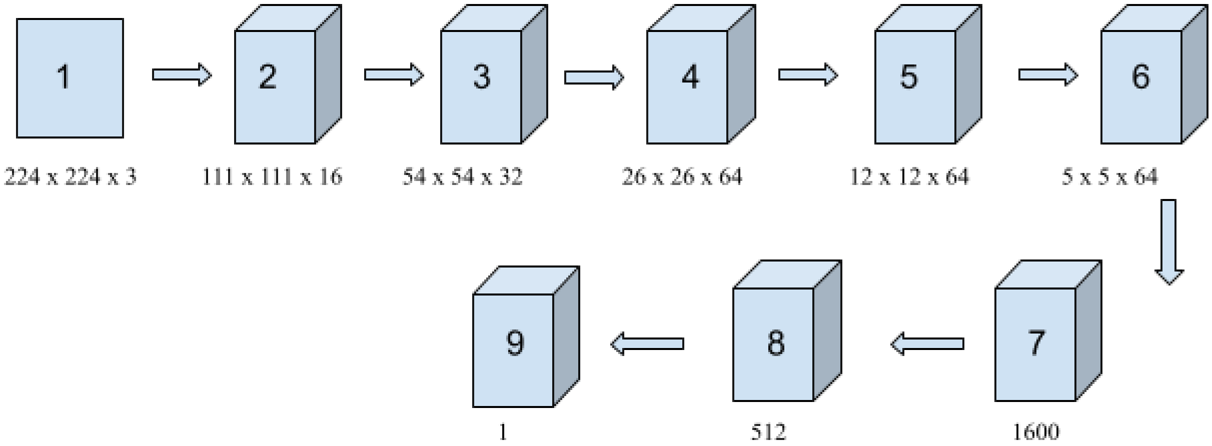

Figure 1. (1) The image of size 224 x 224 with 3 channels as input. (2) - (6) 5 blocks of 2D convolutional layers and 2D MaxPooling layers. Each block represents one pair of 2D Convolutional layer combined with a 2D MaxPooling layer. (7) Flattening layer. (8) - (9) Dense layers. The output dimensions of each block are mentioned in the figure.

Our model architecture is composed of 5 blocks of 2D Convolutional layers combined with 2D MaxPooling layers. The first block has a convolutional layer with 16 filters and 3 x 3 kernel size and a max pooling layer with 2 x 2 kernel size. The second block has a convolutional layer with 32 filters and 3 x 3 kernel size and a max pooling layer with 2 x 2 kernel size. The remaining three blocks have 64 filter-convolutional layers with 3x3 kernel size and max pooling layers with 2x2 kernel size. ReLU activation function is used for all the 2D convolutional layers. A flattening layer is added after the fifth block. A dense layer with 512 neurons and ReLU activation function is added next. Finally a prediction neuron with sigmoid activation function is added. This prediction neuron outputs a value between [0,1] and can be used to classify the input image based on a threshold.

3. Experiments

In this section we propose our methodology for carrying out our experimental studies. We use the NUAA photograph imposter database for our studies. Python is the chosen language for programming and scikit-learn and keras with tensorflow as backend are the major open source libraries used.

3.1 Dataset

The NUAA photograph imposter database is available in three different formats viz. A format without any processing, a format with face images output by a detector and a format undergone geometric normalization. We use the second format for our experiments. The dataset has around 5100 client face images and around 7500 imposter face images.

3.2 Experimental protocol

We compile our model architecture using the binary cross entropy loss function and use RMSprop with a learning rate of 0.001 as the optimizer. A batch size of 100 images is selected and the model is trained for 30 epochs. We use the keras ReduceLROnPlateau function and pass it as a callback while fitting the model.

3.3 Results and discussions

Our model achieves a training accuracy of 100% and a test accuracy of 99.92%. Results from other studies are also mentioned for comparison. Our model's accuracy surpasses all the other accuracy numbers mentioned in the literature. The final prediction neuron predicts results between [0,1] using the sigmoid activation function and we can set a threshold of 0.5 to classify our images. To predict the outcome for a new image, we run the haar cascade classifier [7] for face detection on the image and pass the resulting image to our trained model.

S/No	Author	Method	Accuracy
1	Parveen et.al. [3]	CLBP	96 %
2	Parveen et.al. [2]	DLTP	94.5 %
3	Narayanan et.al. [present]	CNN	99.92%

Table 1. Comparison of accuracy for different methods on the NUAA imposter dataset

Actual ↓ / Predicted →	Imposter	Cient
Imposter	1501	1
Client	1	1020

Table 2. Confusion matrix for our present model

4. Conclusions

A robust deep CNN based approach was presented for face anti-spoofing modeling in maritime digital KYC processes in this paper. The NUAA photograph imposter database was used for our experiments. Features were extracted from the client and imposter faces using a deep convolutional neural network which are then compared for classification. Our results surpass the previous accuracy numbers mentioned in the literature.

Acknowledgement

This work has been supported by the R&D labs at IN-D by Intain AI Pvt. Ltd. The training of the model was carried out using the Tesla T4 GPU provided by google colaboratory.

References

[1] 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

[2] Sajida Parveen et.al. Face Liveness Detection Using Dynamic Local Ternary Pattern (DLTP), Article, Computers, 24 May 2016

[3] Sajida Parveen et. al. Complete local binary pattern and spatial structure of live faces Sci.Int. (Lahore), 28(6), 5219-5222 , 2016 ISSN 1013-5316

[4] Azzeddine Benlamoudi et.al. Face spoofing detection using Local binary patterns and Fisher Score Conference Paper · May 2015 DOI: 10.1109/CEIT.2015.7233145

[5] Deep learning with python, machine learning mastery, ebook, Dr. Jason Brownlee

[6] Machine learning mastery with python, machine learning mastery, ebook, Dr. Jason Brownlee

[7] Paul Viola and Michael Jones, “Rapid Object Detection using a Boosted Cascade of Simple Features”, Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001