International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

The Classification Method for the Identification of Face Spoof in Convolutional Neural Networks

Anish Krishnan Ganesh

International Baccalaureate Diploma Programme, M.Ct.M Chidambaram Chettyar International School, Chennai, Tamil Nadu, India

Article Info
Volume 7, Issue 4
Page Number: 423-433

Publication Issue :
July-August-2021

Article History
Accepted : 20 July 2021
Published : 30 July 2021

ABSTRACT

Automatic facial recognition is currently extensively utilised in a variety of applications, ranging from identity deduplication to mobile payment verification. Face recognition has grown in popularity, raising worries about face spoof attacks (also known as biometric sensor presentation assaults), in which a picture or video of an authorised person's face may be used to obtain access to facilities or services without the person's knowledge. Even though a lot of face spoof detection methods have been suggested, their capacity to generalise has not been well investigated. On the basis of Image Distortion Analysis(IDA), we present an efficient and somewhat robust face spoof detection method . A new paradigm for each stage of a face recognition system is introduced in this article. In the phase of face identification, we present a hybrid model that combines AdaBoost and Convolutional Neural Network (ABCNN) to effectively handle the procedure. A multilayer perceptron and an active shape model will be used in conjunction with an ABANN to align the labelled faces identified in the previous phase. A mixture of Dense and Convolutional neural network layers was used to achieve binary classification of false recognition. The accuracy of categorial cross entropy prediction in Adam was found to be 91 percent, while the accuracy of SGD (stochastic gradient descent) was found to be 88 percent. In binary cross entropy, 90 percent accuracy was seen in Adam and 86 percent accuracy was observed in SGD, while in mean square, 86 percent accuracy was observed in Adam and 80 percent accuracy was observed in SGD.

Keywords : AdaBoost and Convolutional Neural Network, Multi-Layer Perceptron, stochastic gradient descent, Image Distortion Analysis, Spoof Detection.

I. INTRODUCTION

Due to its high simplicity and convenience of use for consumers, biometric-based access control is becoming more popular in today's world. It lowers the amount of human labour involved in identity identification and makes automatic processing more efficient. The face is one of the most significant biometric visual information sources, and it may be readily collected in an uncontrolled setting without

the need for user participation. Accurate detection of faked faces should be given top attention in order to make face-based identity recognition and access control systems more resilient against potential assaults. It has been shown that the newly developed CNN-based deep learning approach is a very efficient way of interacting with visual information. The input is sent into the CNN, which automatically learns the hierarchical characteristics at intermediate levels. Several CNN-based techniques, such as Inception and ResNet, have shown exceptional performance when applied to the picture classification task. The purpose of this study is to evaluate the performance of CNNs for face anti-spoofing[1]. Face The topic of anti-spoofing has lately gotten more attention, both in academic and industry circles. With the introduction of different CNN-based solutions, it was discovered that multi-modal (RGB, depth, and IR) methods-based CNNs outperformed single-modal classifiers in terms of performance. Improvements in performance and reductions in complexity, on the other hand, are urgently required[2]. As a result, an extreme light network design (FeatherNet A/B) with a streaming module is presented, which addresses the shortcomings of Global Average Pooling while requiring fewer parameters overall. Our single FeatherNet, which was trained only on depth images, offers a higher baseline with 0.00168 ACER, 0.35M parameters, and 83M FLOPS[3], compared to other networks.

Since then, deep Convolutional Neural Networks have been effectively used to a variety of computer vision applications, yielding promising results in several cases. As a result, several researchers have used deep learning to the field of face anti-spoofing. Most methods, on the other hand, rely only on the final fully-connected layer to differentiate between genuine and artificial faces. We are motivated by the notion that each convolutional kernel may be seen as a part filter, and we extract deep partial features from the convolutional neural network (CNN) in order to differentiate between genuine and fake faces to make this distinction. In our proposed method, the CNN is fine-tuned first on the face spoofing datasets before being applied to other datasets. Once this has been accomplished, the block principle component analysis (PCA) technique is used to decrease the dimensionality of features, thus avoiding the overfitting issue. At the end of the day, the support vector machine (SVM) is used to differentiate between genuine and artificial faces[4]. Biometric identification methods such as fingerprinting, iris scanning, finger vein analysis, and other similar techniques have advanced significantly over the last several decades, and associated applications have grown more widespread. The advancement of GPU[5] acceleration methods, as well as the influence of deep neural networks, has increased not just the accuracy of face recognition systems, but also the popularity of these systems. Even while facial recognition systems reduce the difficulty of identifying people, their use would expose a new difficult task: face spoofing and presentation assaults, both of which are becoming more common. Face spoofing assaults, which may take the form of photographs, films, or 3D masks, can not only limit the applicability of a face recognition system, but they can also raise its susceptibility in terms of security issues[6].

Face recognition systems are gaining popularity as a result of recent advancements in computer vision technology. At the same time, the methods used to deceive these systems are becoming more sophisticated, necessitating the development of countermeasure measures. To keep up with the current advances made with convolutional neural networks (CNN) in classification tasks, we propose a method based on transfer learning that uses a pre-trained CNN[7] model that only uses static characteristics to detect picture, video, and mask assaults in classification tasks. We put our method through its paces on the public datasets REPLAY-ATTACK and 3DMAD. According to our accuracy on

the REPLAY-ATTACK database, we have a half total error rate (HTER) of 1.20 percent and a half total error rate (ACR) of 99.04 percent. Our accuracy for the 3DMAD was 100.00 percent, while our accuracy for the HTER was 0.00 percent [8].

II. RELATED WORKS

Face recognition has progressed to become a commonly used biometric technology. However, it is vulnerable to presentation assaults, which presents a major security danger to the system. Although presentation attack detection (PAD) techniques attempt to solve this problem, they often fail to generalise to assaults that have not yet been seen. In this paper, we offer a novel framework for PAD that makes use of a one-class classifier and a multi-channel convolutional neural network to train the representation that will be utilised (MCCNN)[9]. A new loss function is proposed, which pushes the network to learn a compact embedding for the genuine class while remaining far away from the representation of assaults, thus improving performance. A one-class Gaussian Mixture Model is used on top of these embeddings in order to complete the PAD challenge. The suggested framework offers a new method to learning a resilient PAD system from legitimate and accessible (known) attack classes[10], which is described in more detail below. Deep learning-based techniques for detecting face presentation attacks have shown promising results in recent years. Although effective against conventional attacks, such techniques have a tendency to over-emphasize a certain geographic region, which leaves the system susceptible to adversarial example assaults and restricts their effectiveness against them. This paper proposes multi-regional convolutional neural networks and introduces the concept of local classification loss to local patches in order to utilise more information from the input and improve the robustness of face presentation attack detection methods against adversarial examples. This allows the input information to be utilised across the entire face region and avoid over-emphasizing certain local areas[11,12].

Current state-of-the-art dual camera-based face liveness detection techniques identify a live face and a face Presentation Attack using either hand-crafted features, such as disparity, or deep texture features, which are either hand-crafted or deep texture characteristics (PA). When used to unknown face PA under unfavourable circumstances, deep Convolutional Neural Networks (CNN) are less successful than other classifiers, especially deep Convolutional Neural Networks (CNN)[13]. We demonstrate, in contrast to previous methods, that supervising a deep CNN classifier by learning disparity features using the current CNN layers increases the performance and resilience of the CNN to unknown kinds of face PA in this article. [14]. When it comes to reducing the risk of traffic accidents, driver behaviour monitoring systems, also known as Intelligent Transportation Systems (ITS), have been extensively used. The majority of prior approaches of monitoring driver behaviour have relied on computer vision techniques. Such techniques are subject to invasion of privacy and the potential of spoofing, among other drawbacks. This article offers a new and efficient deep learning technique for evaluating the driving behaviour of commercial truck drivers. In order to distinguish between five different driving styles[15,16], we utilised driving signals such as acceleration, gravity, throttle, speed, and Revolutions Per Minute (RPM) to identify five different driving styles. These were classified as normal, aggressive, distracted, sleepy, and intoxicated driving[17,18].

Facial anti-spoofing (FAS) is a critical component of face recognition systems, which are becoming more popular. For example, the majority of current FAS methods 1) rely on stacked convolutions and expert-designed networks, which are weak in describing

detailed fine-grained information and easily become ineffective when the environment changes (for example, when illumination changes), and 2) prefer to use long sequences as input to extract dynamic features, which makes them difficult to deploy in scenarios where rapid response is required. Specifically, we present a new frame level FAS technique based on Central Difference Convolution (CDC), which is capable of capturing inherent detailed patterns by aggregating both intensity and gradient information[19,20] and can be used to any image type.

PROPOSED METHODOLOGY

Modern state-of-the-art Face Recognition systems make use of graphics processing technology, often known as GPUs, which have seen significant advancements over the years. It was Nvidia, in particular, who introduced the CUDA programming environment, which enabled C and C++ programmes to make use of the GPU for large parallel processing. It makes use of Deep Learning (also known as Neural Networks), which necessitates the use of GPU capability in order to execute large computing operations in parallel. Instead of encoding the logic rules and decision trees in software, Deep Learning is an approach to Artificial Intelligence that simulates how the brain functions by teaching software through examples, several examples (big data), rather than hardcoding the logic rules and decision trees in the software. (The development of the ImageNet dataset was a significant contribution to the field of Deep Learning. With the production of millions of pictures, it pioneered the gathering of large quantities of images that were tagged and categorised in order to train computers for image classifications. Neural networks are composed of layers of nodes, with each node being linked to nodes in the following layer, which is where the information is fed. Deepnets are very deep neural networks with many layers that are made feasible by the computing power of GPUs. In the field of computer vision, there are many different neural network topologies to choose from, such as the Convolutional Neural Networks (CNN) architecture, which is particularly useful for image categorization and face recognition.

Image-based Presentation Attack Detection (PAD) systems in two distinct domains are the focus of this repository. The first is cork PAD and the second is face PAD systems. In order to differentiate between a genuine picture and an image attack, the suggested PAD system makes use of the combination of two distinct colour spaces and just one frame, as shown in Fig. 1.

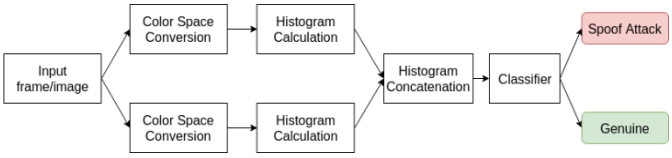

Figure 1. General flowchart for Proposed System

A face recognition system is a technology that may be used to identify or authenticate a person based on a digital picture or a video frame from a video source. It is also known as facial recognition software. A simple real-time face recognition system, at its most basic level, is comprised of the following pipeline components:

1. **Face Enrolment.** Registering faces to a database which includes pre-computing the face embeddings and training a classifier on top of the face embeddings of registered individuals.
2. **Face Capture.** Reading a frame image from a camera source.
3. **Face Detection.** Detecting faces in a frame image.
4. **Face Encoding/Embedding.** Generating a mathematical representation of each face (coined as embedding) in the frame image.

5. **Face Identification.** Inferring each face embedding in an image with face embeddings of known people in a database.

Face Liveness Detection (to prevent spoofing attempts using a picture, video, or 3D mask), face alignment, face augmentation (to enhance the amount of photos in the dataset), and face verification are some of the more sophisticated features available in more complex systems (to confirm prediction by comparing cosine similarity or Euclidean distance with each database embedding).

An artificial neural network consisting of neurons that are not completely linked to the next layer is known as a convolutional neural network. Specifically, the neurons are linked according to the filters that have been employed; for example, if the filter is a 3x3 filter, nine neurons in the nth layer control the output of one neuron in the (n+1)th layer. The convolution process is performed on the image's normalised pixels, which are then combined. The convolution process multiplies filter values and pixels, and then adds the values, resulting in the extraction of features via the convolution operation. After applying the fxf filter on a picture with dimensions of:, the resultant output has the following dimensions as given in equation 1:

$$nout = [nin+2p-k\ ] + 1 \qquad (1)$$

nin: number of input features nout: number of output features k: convolution kernel size p: convolution padding size s: convolution stride size

As a result, the convolution process lowers the size of the picture extracting characteristics that are extracted. Another process, known as Max pooling, is performed on pixels in which the pixel with the highest value in the surrounding pixels is chosen in order to minimise the spatial representation of the picture and, as a result, the number of parameters in the network.

III. METHODS AND MATERIAL

3.1 DESIGN

The word (libfaceid) refers to a library function that is intended to be simple to use, modular, and resilient in its construction. Model selection is accomplished via the constructors, and the expose function is as simple as detect() or estimate(), making use very simple. The files are structured into modules, which makes it extremely easy to comprehend and debug what is going on. Because of the sturdy architecture, it will be extremely simple to support additional models in the future.

Neurons, the computing units of neural networks, are connected in a network to form the network. In order to operate, neurons must have a number (either as an initial input or as an output from a previous layer) and an activation function. A neuron's output is determined by the activation functions, which are nonlinear functions that are utilised to determine the output of the neuron. The activation functions that are most frequently employed include the ReLU (Rectified Linear Unit), tanh, sigmoid, and so forth. Weights are present in the connections between layers, and bias is present in every layer. Backpropagation is a technique used in neural networks to change the weights and biases of the network based on the label of the training data. As a result, the weights and biases of the actual and deepfake modified frames are different from one another. Similarly shaped features in pictures induce comparable neurons to fire, and as a result, their weights and biases are similar in value as well.

Algorithm for Pre-processing

First step is to train SVM classifier with different fake and live faces. Once the features are extracted from those image, test image is given as input to determine whether it belongs to live

user or non-live user.

Step 1: Go to cd .. and give the test image name which has to be checked for classification.

Step 2: Read image with .jpg format.

Step 3: Detect a face within an image using bunding box. Liveness detection procedure can be proceeded if and only if face is detected within the box.

Step 4: Convert RGB format to HSV format.

Step 5: Calculate the Means and standard deviation of H,S,V

Step 6: Determine the skewness factor using Mean and standard deviation. And find minimum and maximum value of H,S,V

Step 7: Calculate the motion blur using PSF function

Step 8: Find the edge of the normalized image e1 and edge of the blur region e2. Remove blur= sum(e1-e2)/RxC

Step 9: Store the skewness values of normalized image and concatenate. Find out the histogram values of normalized image (H)

Step 10: Compare the histogram values of normalized image, if the feature is same increment out else increment out1. Out is considered as positive features belongs to live face out1 is considered as negative features.

Step 11: Store all the values in QF.

Step 12: Compare stored values with trained image values, if the outfuse is -1 then it is live face else fake face.

Algorithm: CNN Model for Fake Spoof Identification

Procedure

Routing ($\mathbf{u}^{(i)}$, $W^{(i,j)}$, r)

$\widehat{W}^{(i,j)} \leftarrow W^{(i,j)} + rand\left(size\left(W^{(i,j)}\right)\right)$

$\widehat{\boldsymbol{u}}^{(i)} \leftarrow \widehat{W}^{(i,j)}\, square\left(\boldsymbol{u}^{(i)}\right)$

$\widehat{\boldsymbol{u}}^{(i)} \leftarrow dropout\left(\hat{u}^{(i)}\right)$

for all input capsule i and all output capsules j **do** $b_{i,j} \leftarrow 0$

for r iterations **do**

for all input capsules i **do** $c_i \leftarrow$ softmax ($\mathbf{b}_i$)

for all output capsules j **do** $s_j \leftarrow \sum_i c_{i,j}\, \widehat{\boldsymbol{u}}^{(i)}$

for all input capsules j **do** $v^{(j)} \leftarrow$ squash ($\mathbf{s}_j$)

for all input capsules i and output capsules j **do**

$b_{(i,j)} = \leftarrow b_{i,j} + \widehat{\boldsymbol{u}}^{(i)\mathrm{T}} \boldsymbol{v}^{(j)}$

return $v^{(j)}$

Only models that have been pre-trained will be supported. It is the technique of applying a pretrained model (that has been trained on a big dataset) to a fresh dataset to improve accuracy and efficiency. Basic definition: When a machine learning algorithm has been trained on a big dataset, it has gained enough "experience" to be able to generalise the learnings to a new environment or new dataset, this is referred to as generalisation capability. It is one of the most important elements contributing to the growth in popularity of Computer Vision, not just for face recognition but also and especially for object identification, during the last several decades. And, more recently, in the middle of this year, transfer learning has made significant progress in the field of Natural Language Processing (BERT by Google and ELMo by Allen Institute). This kind of transfer learning is very beneficial, and it is the primary objective that the group working on Reinforcement Learning for robots is striving to accomplish.

CNN (for frame feature extraction) + **LSTM** (for temporal sequence analysis)

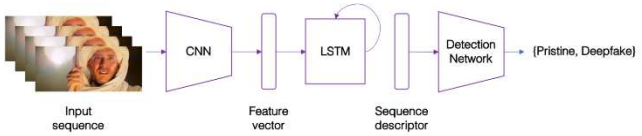

Figure 2. Overview of our detection system

There are 3 main categories of AI-synthesized media

1. face-swap: the face in a video is automatically replaced with another person's face.

2. lip-sync: a source video is modified so that the mouth region is consistent with an arbitrary audio recording
3. puppet-master: a target person is animated (head movements, eye movements, facial expressions) by a performer as shown in fig 3.

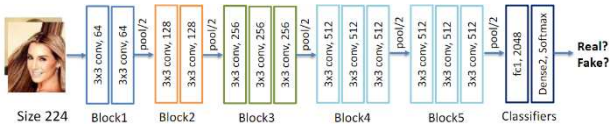

Figure 3. Blocks in Classifiers

Hypothesis

- As an individual speaks, they have **distinct (but probably not unique) facial expressions and movements.**
- that the creation of all three types of deep fakes tends to disrupt these patterns.

3.2 FEATURES

It is not feasible for certain Face Recognition applications to have several datasets of pictures per individual because of technical limitations. As a result, it is essential to identify a suitable model for the target hardware platform (CPU, GPU, embedded system) that strikes a compromise between accuracy and speed. The three pillars of artificial intelligence are data, algorithms, and computation. Each model or algorithm in the pipeline may be selected using the libfaceid library.

For each stage of the Face Recognition pipeline, the libfaceid library provides a variety of models to choose from. Some models are more accurate than others, and some models are quicker than others. You may mix and combine the models to meet the needs of your particular use case, hardware platform, and system specifications.

3.3 FACE ENROLMENT

- Should support dynamic enrolment of faces. Tied up with the maximum number of users the existing system supports.
- Should ask user to move/rotate face (in a circular motion) in order to capture different angles of the face. This gives the system enough flexibility to recognize you at different face angles.
- IPhone X Face ID face enrolment is done twice for some reason. It is possible that the first scan is for liveness detection only.
- How many images should be captured? We can store as much image as possible for better accuracy but memory footprint is the limiting factor. Estimate based on size of 1 picture and the maximum number of users.
- For security purposes and memory related efficiency, images used during enrolment should not be saved. Only the mathematical representations (128-dimensional vector) of the face should be used.

3.4 FACE DETECTION

- Only 1 face per frame is detected.
- Face is expected to be within a certain location (inside a fixed box or circular region).
- Detection of faces will be triggered by a user action - clicking some button. (Not automatic detection).
- Face alignment may not be helpful as users can be enforced or directed to have his face inside a fixed box or circular region so face is already expected to

be aligned for the most cases. But if adding this feature does not affect speed performance, then face alignment should be added if possible.

- Should verify if face is alive via anti-spoofing techniques against picture-based attacks, video-based attacks and 3D mask attacks. Two popular example of liveness detection is detecting eye blinking and mouth opening.

3.5 FACE IDENTIFICATION

- Recognize only when eyes are not closed and mouth is not open
- Images per person should at least be 50 images. Increase the number of images per person by cropping images with different face background margin, slight rotations, flipping and scaling.
- Classification model should consider the maximum number of users to support. For example, SVM is known to be good for less than 100k classes/persons only.
- Should support unknown identification by setting a threshold on the best prediction. If best prediction is too low, then consider as Unknown.
- Set the number of consecutive failed attempts allowed before disabling face recognition feature. Should fallback to passcode authentication if identification encounters trouble recognizing people.
- Images used for successful scan should be added to the existing dataset images during face enrolment making it adaptive and updated so that a person can be recognized with better accuracy in the future even with natural changes in the face appearance (hairstyle, mustache, pimples, etc.)

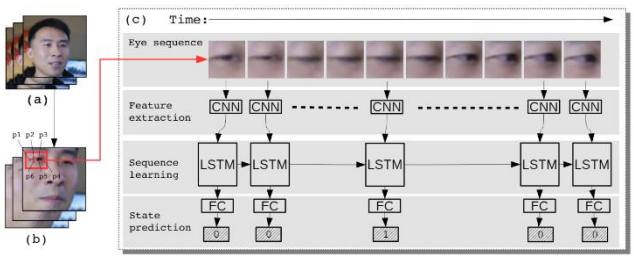

Figure 4. Feature Extraction using CNN and LSTM

In addition to these guidelines, the face recognition solution should provide a way to disable/enable this feature as well as resetting the stored datasets during face enrolment.

IV. PERFOMANCE OPTIMIZATIONS

The trade-off between speed and precision is common. Based on your particular use-case and system constraints, you may optimise performance to meet your needs. Speed is one of the primary considerations while designing models, while accuracy is another. Make careful to test all of the models given to discover which model is most suited to your particular use-case, target platform (CPU, GPU, or embedded), and special needs, before choosing one. Additional recommendations for improving performance are provided below.

4.1 SPEED

- Reduce the frame size for face detection.
- Perform face recognition every X frames only
- Use threading in reading camera source frames or in processing the camera frames.
- Update the library and configure the parameters directly.

4.2 ACCURACY

- Add more datasets if possible (ex. do data augmentation). More images per person will often result to higher accuracy.
- Add face alignment if faces in the datasets are not aligned or when faces may be unaligned in actual deployment.
- Update the library and configure the parameters directly.

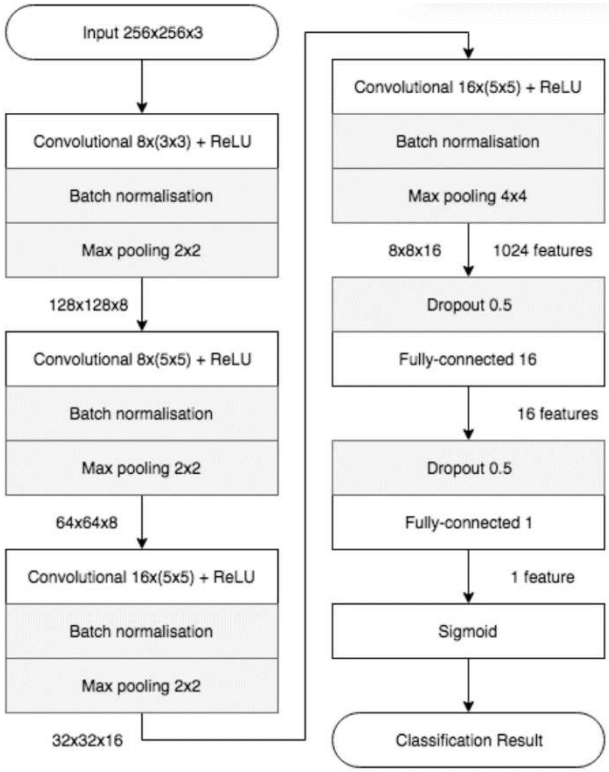

Figure 5. CNN Model with Classification Results

The real and fake images behave in noticeable different spectra **at high frequencies**, and therefore they can be easily classified.

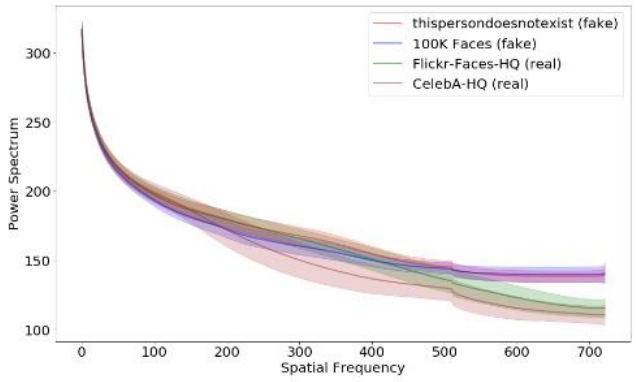

Figure 6. Spatial Frequency with Power Spectrum

The deepfake images have a noticeably different frequency characteristic.

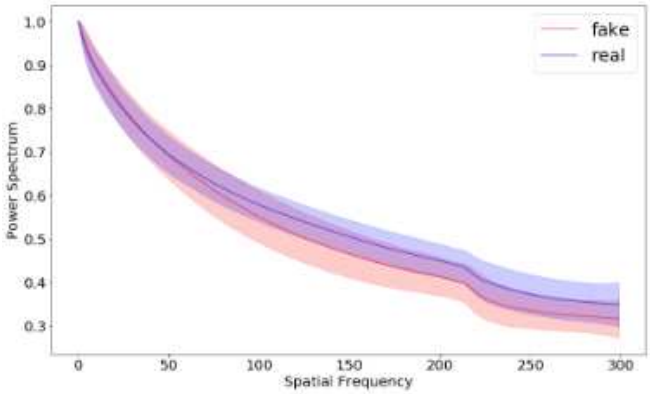

Figure 7. Prediction Results of Fake Vs Real

V. CONCLUSION

Face spoof detection is a challenging issue that we solve in this article, which is especially relevant in a cross-database setting. Instead of using motion or texture-based characteristics, as is the case with most published techniques, we propose to conduct face spoof detection using Image Distortion Analysis (IDA) (IDA). For the spoof face pictures, four different kinds of IDA features (specular reflection, blurriness, colour moments, and colour diversity) have been developed to capture the image distortion caused by the specular reflection. Each of the four distinct features is concatenated together, yielding an IDA feature vector with a 121-dimensional dimension. It is decided whether to utilise authentic or spoof faces by using an ensemble classifier composed of two component SVM classifiers that have been trained for distinct types of spoof assaults. The findings demonstrate that ABANN not only achieves an approximate detection rate and processing time comparable to that of the AdaBoost detector, but it significantly reduces the number of erroneous detections. The shortcomings of AdaBoost and the ANN detector have been addressed by ABANN. Images were then classified and labelled as a result of the Image Classification process. On the basis of the dataset, predictions were generated with the assistance of Machine Learning algorithms. As a result, this technique may be used to almost any video.

VI. ACKNOWLEDGEMENTS

The author would like to thank *Dr. K. S. Mohanasundaram,* Ph.D., Professor at SRM Institute of Science and Technology, Department of Computer Science, for his guidance and advice at various stages of this research. The author would also like to thank his family for their support throughout.

VII. REFERENCES

[1]. Nagpal, C., & Dubey, S. R. (2019, July). A performance evaluation of convolutional neural networks for face anti spoofing. In 2019 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE.

[2]. Zhang, P., Zou, F., Wu, Z., Dai, N., Mark, S., Fu, M., ... & Li, K. (2019). Feathernets: convolutional neural networks as light as feather for face anti-spoofing. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 0-0).

[3]. Li, L., Feng, X., Boulkenafet, Z., Xia, Z., Li, M., & Hadid, A. (2016, December). An original face anti-spoofing approach using partial convolutional neural network. In 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA) (pp. 1-6). IEEE.

[4]. Lin, H. Y. S., & Su, Y. W. (2019, November). Convolutional neural networks for face anti-spoofing and liveness detection. In 2019 6th International Conference on Systems and Informatics (ICSAI) (pp. 1233-1237). IEEE.

[5]. Lucena, O., Junior, A., Moia, V., Souza, R., Valle, E., & Lotufo, R. (2017, July). Transfer learning using convolutional neural networks for face anti-spoofing. In International conference image analysis and recognition (pp. 27-34). Springer, Cham.

[6]. George, A., & Marcel, S. (2020). Learning one class representations for face presentation attack detection using multi-channel convolutional neural networks. IEEE Transactions on Information Forensics and Security, 16, 361-375.

[7]. Ma, Y., Wu, L., & Li, Z. (2020). A novel face presentation attack detection scheme based on multi-regional convolutional neural networks. Pattern Recognition Letters, 131, 261-267.

[8]. Rehman, Y. A. U., Po, L. M., & Liu, M. (2020). SLNet: Stereo face liveness detection via dynamic disparity-maps and convolutional neural network. Expert Systems with Applications, 142, 113002.

[9]. Shahverdy, M., Fathy, M., Berangi, R., & Sabokrou, M. (2020). Driver behavior detection and classification using deep convolutional neural networks. Expert Systems with Applications, 149, 113240.

[10]. Yu, Z., Zhao, C., Wang, Z., Qin, Y., Su, Z., Li, X., ... & Zhao, G. (2020). Searching central difference convolutional networks for face anti-spoofing. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5295-5305).

[11]. Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. IEEE Transactions on Information Forensics and Security, 10(4), 746-761.

[12]. Zhang, Y., Yin, Z., Li, Y., Yin, G., Yan, J., Shao, J., & Liu, Z. (2020, August). Celeba-spoof: Large-scale face anti-spoofing dataset with rich annotations. In European Conference on Computer Vision (pp. 70-85). Springer, Cham.

[13]. Farmanbar, M., & Toygar, Ö. (2017). Spoof detection on face and palmprint biometrics. Signal, Image and Video Processing, 11(7), 1253-1260.

[14]. Chinchu, S., Mohammed, A., & Mahesh, B. S. (2017, July). A novel method for real time face spoof recognition for single and multiple user authentication. In 2017 International Conference on Intelligent Computing, Instrumentation and

Control Technologies (ICICICT) (pp. 376-380). IEEE.

[15].Liang, Y., Hong, C., & Zhuang, W. (2021). Face Spoof Attack Detection with Hypergraph Capsule Convolutional Neural Networks. International Journal of Computational Intelligence Systems, 14(1), 1396-1402.

[16].Nixon, K. A., Aimale, V., & Rowe, R. K. (2008). Spoof detection schemes. In Handbook of biometrics (pp. 403-423). Springer, Boston, MA.

[17].Nasiri-Avanaki, M. R., Meadway, A., Bradu, A., Khoshki, R. M., Hojjatoleslami, A., & Podoleanu, A. G. (2011). Anti-spoof reliable biometry of fingerprints using en-face optical coherence tomography. Optics and Photonics Journal, 1(03), 91-96.

[18].Eskandari, M., & Toygar, Ö. (2015). Selection of optimized features and weights on face-iris fusion using distance images. Computer Vision and Image Understanding, 137, 63-75.

[19].Patel, K., Han, H., & Jain, A. K. (2016). Secure face unlock: Spoof detection on smartphones. IEEE transactions on information forensics and security, 11(10), 2268-2283.

[20].Patil, P. R., & Kulkarni, S. S. (2021). Survey of non-intrusive face spoof detection methods. Multimedia Tools and Applications, 80(10), 14693-14721.

AUTHOR PROFILE

Mr. Anish Krishnan Ganesh is an International Baccalaureate Program student and a Research Scholar at Lumiere Education (USA). He is the Founder and CEO of Conquerly (https://conquerly.io/), nationally recognized AI Educational platform completely free for students across the globe with a mission to educate the world on the unlimited possibilities of AI and make a positive impact on society through innovations. He was headlined in Edex, The New Indian Express, India's National Education paper along with his interviews at The Hindu, Dinamalar, Edex Live and few other media outlets for his educational innovations.

He has done extensive research on Artificial Intelligence under the guidance of Harvard University and New York University mentors to find out whether training conversational AI with sentiment-based rewards exhibit meaningful semantic variation. His research paper has been submitted to prestigious Springer Journal of Grid Computing. Currently working on two more research papers on "Environmental impact of consumer textiles and climate conscious recommendations" and "Projecting Eco-friendliness values of manufactured items to consumers using Deep Learning Algorithms".

He has worked as a Data Science Intern for 2+ years and has immense experience working with Machine Learning, Deep Learning using Python, TensorFlow, and PyTorch. He has solved real-world problems by developing AI products in the fields of healthcare, education, music, finance, and reducing waste. He has designed a framework, EcoShop which has been submitted for Copyright/Patent under Intellectual Property by Government of India.

He was the World Topper in IGCSE Mathematics, Grand Award Winner at IRIS National Fair and his project, Conscious Clothing is selected as Finalist at International Science and Engineering Fair (ISEF) 2021, received a Diploma by the Royal Swedish Academy of Engineering Sciences. He has completed a Java programming course from John Hopkins University, three IBM AI Engineering courses, and advanced Python programming courses from Datacamp. From a very young age, he has love for all things AI and lived his life with the words never giving up flowing through his very being.

Cite this article as :

Anish Krishnan Ganesh, "The Classification Method for the Identification of Face Spoof in Convolutional Neural Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7, Issue 4, pp.423-433, July-August-2021.