IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FACE SPOOF DETECTION USING IMAGE PROCESSING

[1]Sagar M S, [2] Saravanan C

[1]Student, [2]Assistant Professor

[1,2]Master of Computer Application

[1,2] RV College of Engineering®, Bengaluru, India

Abstract: Face recognition is a difficult field within the scope of biometric authentication since it is reliant on the uniqueness of biological qualities or qualities of an individual. Face recognition systems are subject to a variety of threats and hence their security is critical. Face spoofing is a way of gaining unauthorized access to a system by impersonating a legitimate user using a photo, video clip, or 3D mask as a replacement for another person's face. 2D and 3D spoof attacks are the two types of spoof attacks. To prevent all of these scams, there is a need for security solution that can combined with current using Biometric technology. This paper helps to detects fraud by using the image of the user's identity as a form of authentication. For training 72% and for testing 28% of total dataset are used. Tools used for this application are sypder, keras, Numpy and Tensorflow.

I. INTRODUCTION

There has been a growth in interest in human automatic secure identification in the previous decade, which is mostly based on unique personal biometric data. Biometrics is using physiological factors like as fingerprints, faces, and iris, as well as behavioral characteristics such as typing rhythm and stride, to uniquely identify or authenticate a person. As biometric systems are widely used in real-world applications such as mobile phone authentication and access control, biometric samples are supplied to the biometric system and sought to be authenticated.

Facial spoofing is a method for a fraudulent user to manipulate or attack a facial recognition system by imitating a registered user and gaining unauthorized entry and take benefits.

Face recognition systems are becoming increasingly important in today's world because they have a wide range of applications, including surveillance, forensic investigations, and access control. Face recognition systems employ facial traits to validate the user's identification. Face recognition system security has become one of the most important priorities. Face spoofing detection has been concentrated on assessing the luminance of face photos, ignoring the chrominance information that can help distinguish fraudulent faces from real ones. Spoofing attacks such as pictures, masks, and video attacks make face recognition systems vulnerable.[1]

Selfies have been a significant component of photography in recent years, and they are now regarded as a powerful and reliable communication medium. Today's technology has progressed to the point that anyone may change an image using available image editing tools. As a result, determining whether or not the image is faked has become challenging. To detect false faces in biometrics systems, many spoof detection algorithms are being developed. Face spoofing recognition, however, continues to be a problem in online social media. Face images are the most widely used biometric modality for highly accurate face recognition systems, but they are vulnerable to a variety of presentation attacks.

II. LITERATURE SURVEY

Spoofing attacks on pictures, movies, and 3D masks are common in face verification systems. Face spoofing detection, also known as face anti-spoofing, face liveness detection, or face presentation attack detection, is a difficult issue in practice for protecting face verification systems.[1]

The Fully Convolutional Network with Domain Adaptation and Lossless Size Adaptation (FCN-DA-LSA) is a suggested face spoofing detection system. The FCN-DA-LSA contains a lossless size adaptation pre-processor followed by an FCN-based pixel-level classifier with a domain adaptation layer [2]

The spoofing assault is still a difficult challenge to solve. To protect the face recognition system against spoofing assaults, robust solutions are required. This paper [3] gives an overview of modern face spoofing detection approaches that can be used to protect against various types of assaults.

Selfies have been a significant component of photography in recent years, and they are now regarded as a powerful and reliable communication medium. Today's technology has progressed to the point that anyone with access to picture editing tools may change images. [4]

Face images are the most widely used biometric modality for highly accurate face recognition systems, but they are prone to a variety of presentation attacks. Before providing the face image to biometric systems, face anti-spoofing is a crucial step. [5]

Various forms of attacks can readily spoof face recognition-based authentication systems. Consistent countermeasures must fulfill a number of criteria, the most important of which being reliable robustness and modest complexity. Researchers, developers, and retailers from the entire biometric community have collaborated on difficult jobs to produce a more accurate protection mechanism against spoofing attacks. [6]

Face recognition systems can be fooled by spoofing attacks. Face anti-spoofing with excellent accuracy is addressed using an optical flow vector on two sorts of attacks: photographs and videos displayed on high-resolution electronic screens. Face recognition systems are becoming increasingly important in today's world because they have a wide range of applications, including surveillance, forensic investigations, and access control. Face recognition systems employ facial traits to validate the user's identification. [7]

Based on the outcome of Literature survey, it has been observed that Face verification systems are vulnerable to photo, video, and 3D mask spoofing attacks. The spoofing assault is still a difficult challenge to solve. To protect the face recognition system against spoofing assaults, robust solutions are required. The analysis of the brightness of the facial photos has been the main focus of face spoofing detection. Information about chrominance that can be used to distinguish between fake and real faces. Face spoofing detection, also known as face anti-spoofing, face liveness detection, or face presentation attack detection.

III. PROPOSED SYSTEM

This section demonstrate the methodology and the principle adopted in the work.

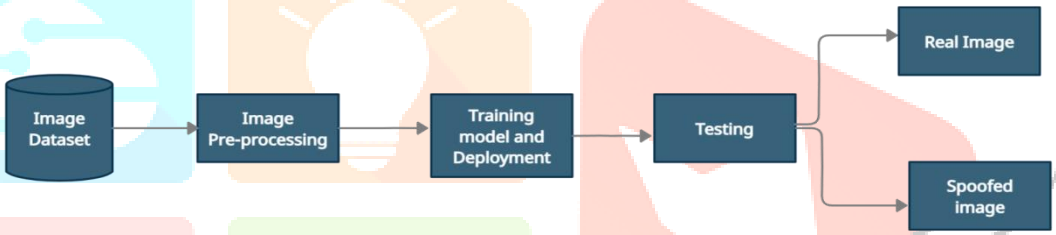

Figure 1: Block diagram of the proposed system
This figure represents the block diagram of steps for face spoofing detection

Dataset: Dataset: The data was gathered via kaggle. A total of 17332 photos were used for training, with another 6686 images used for testing and validation. To begin, the data for the software is loaded.

Image pre-processing: The keras ImageDataGenerator is used to label data from directories and to enhance the data with shifts, rotations, zooms, and mirroring. Mirroring will help ensure that the data is not biassed toward one handedness or the other.[8]

Training the Model and Deployment: The CNN model is defined to train and deploy within the application after the data has been pre-processed. Finally, various Keras auxiliary functions were used to train the model. Separate testing and validation datasets were defined because hyper-parameter optimization was not performed. Within the application, the model can be further assessed in real-time.[9]

Testing the model: After the model had been trained, some real photographs were utilized alongside some modified photos to assess the model's prediction.

IV. RESULTS

This application is primarily concerned with strengthening the security of web users who may be targets of spoofing attacks, and installing this system rather than manually looking for data saves time. This application aims to provide a facial image spoofing detection system using the algorithm called Depth feature fusion that can detect manipulation and photo-print attacks on internet users' faces. This system can be used to detect criminal individuals as well as for security.

V. SCREEN SHOTS

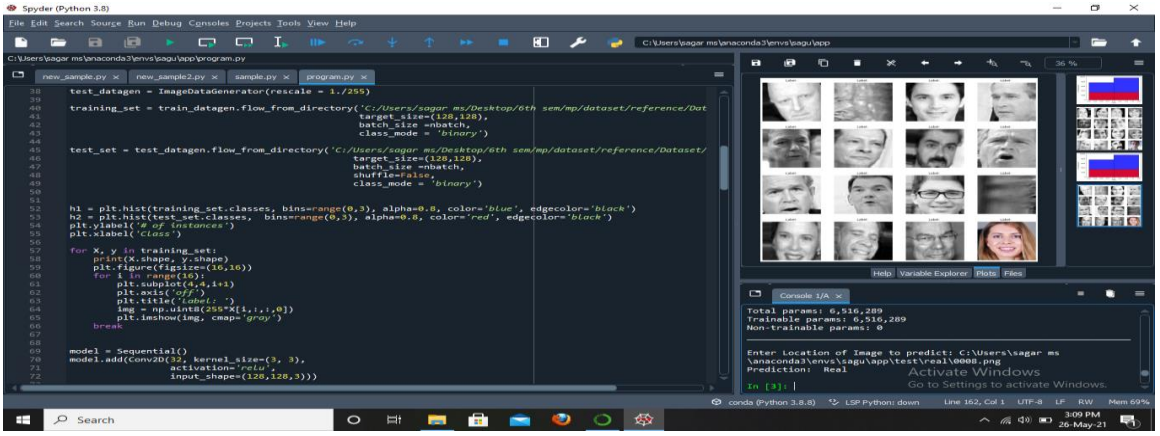

Figure 2: Prediction of real image
This figure represents the prediction of real image based on input image

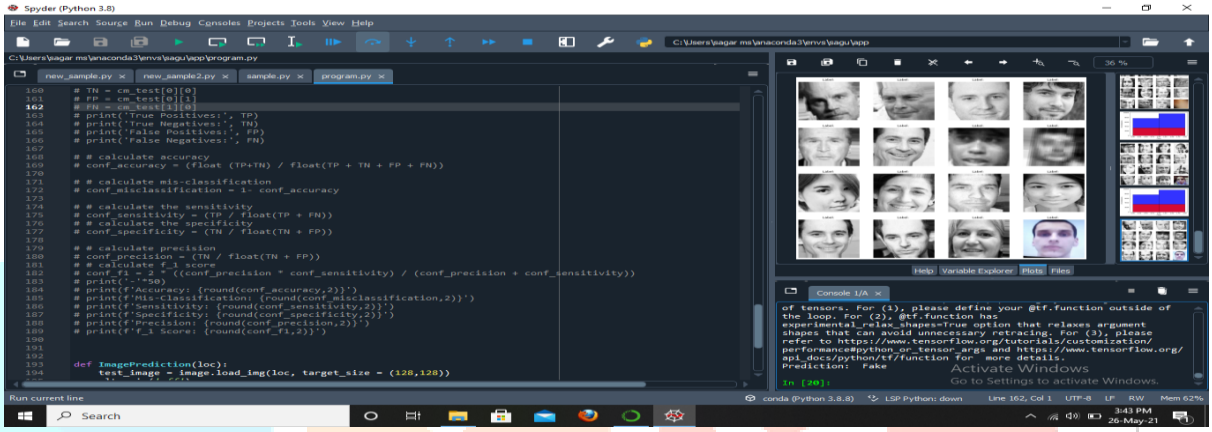

Figure 3: Prediction of fake image
This figure represents the prediction of fake image based on input image

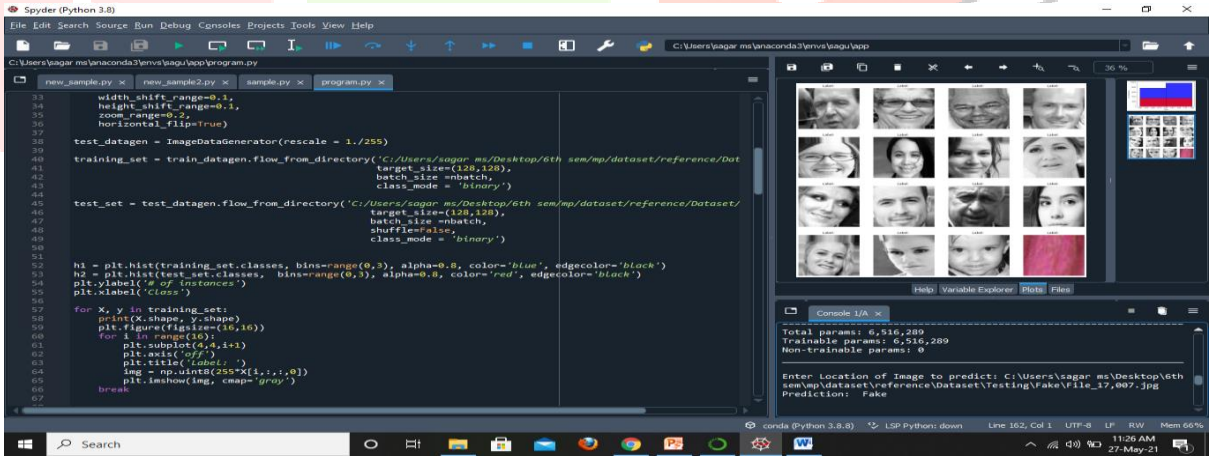

Figure 4: Image with No face will Predicts as fake image
This figure represents the prediction of fake image based on input image which has no face

Figure 5: Image with Blur face will Predicts as fake image
This figure represents the prediction of fake image based on input image which has blur face

V. CONCLUSION

This paper suggested with the rise in popularity of mobile technology in recent years, practically all applications now have access to private data in some form. This fact is particularly sensitive in the context of smart cities. Hackers frequently utilize profiles obtained through cyber-attacks on social media sites to steal personal information or even to expose the real user. Authenticating users using biometric attributes such as fingerprints, iris, or face features is one technique to prevent spoofing. The facial image spoofing detection system is intended to perform as predicted and to pass the various test circumstances. This paper is primarily focused on increasing the security of web users who are potential targets of spoofing attacks, and installing this system rather than manually looking for data saves time. This proposed work was successful in detecting facial image spoofing that can detect manipulation and photo-print attacks that are carried out on internet users' faces.

REFERENCES

[1] S. Kumar, S. Singh and J. Kumar, "A comparative study on face spoofing attacks," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 1104-1108, doi: 10.1109/CCAA.2017.8229961.

[2] N. Daniel and A. Anitha, "A Study on Recent Trends in Face Spoofing Detection Techniques," 2018 3rd International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2018, pp. 583-586, doi: 10.1109/ICICT43934.2018.9034361.

[3] W. Sun, Y. Song, H. Zhao and Z. Jin, "A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation," in IEEE Access, vol. 8, pp. 66553-66563, 2020, doi: 10.1109/ACCESS.2020.2985453.

[4] W. Sun, Y. Song, C. Chen, J. Huang and A. C. Kot, "Face Spoofing Detection Based on Local Ternary Label Supervision in Fully Convolutional Networks," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3181-3196, 2020, doi: 10.1109/TIFS.2020.2985530.

[5] Z. Boulkenafet, J. Komulainen and A. Hadid, "Face anti-spoofing based on color texture analysis," 2015 IEEE International Conference on Image Processing (ICIP), Quebec City, QC, Canada, 2015, pp. 2636-2640, doi: 10.1109/ICIP.2015.7351280.

[6] S. Bharadwaj, T. I. Dhamecha, M. Vatsa and R. Singh, "Computationally Efficient Face Spoofing Detection with Motion Magnification," 2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops, Portland, OR, USA, 2013, pp. 105-110, doi: 10.1109/CVPRW.2013.23.

[7] Y. Atoum, Y. Liu, A. Jourabloo and X. Liu, "Face anti-spoofing using patch and depth-based CNNs," 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, USA, 2017, pp. 319-328, doi: 10.1109/BTAS.2017.8272713.

[8] T. J. Jayan and R. P. Aneesh, "Image Quality Measures Based Face Spoofing Detection Algorithm for Online Social Media," 2018 International CET Conference on Control, Communication, and Computing (IC4), Thiruvananthapuram, India, 2018, pp. 245-249, doi: 10.1109/CETIC4.2018.8531037.

[9] N. Daniel and A. Anitha, "A Study on Recent Trends in Face Spoofing Detection Techniques," 2018 3rd International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2018, pp. 583-586, doi: 10.1109/ICICT43934.2018.9034361.

[10] E. Fourati, W. Elloumi and A. Chetouani, "Face anti-spoofing with image quality assessment," 2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART), Paris, France, 2017, pp. 1-4, doi: 10.1109/BIOSMART.2017.8095313.