International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Face Liveness Detection using Machine Learning and Neural Network -Literature Survey

Shambhavi Mokadam[1], Madhura Bhange[2], Yash Hulsurkar[3], Babita Sonare[4]

[1]*Shambhavi Mokadam, Dept. of Information Technology, PCCOE, Maharashtra, India*
[2]*Madhura Bhange, Dept. of Information Technology, PCCOE, Maharashtra, India*
[3]*Yash Hulsurkar, Dept. of Information Technology, PCCOE, Maharashtra, India*
[4]*Prof. Babita Sonare, Dept. of Information Technology, PCCOE, Maharashtra, India*

Abstract - *As the world becomes more and more digitized, the threat to security grows at an alarming rate. The mass usage of technology has garnered the attention and curiosity of people with foul intentions, whose aim is to exploit this use of technology to commit theft and other heinous crimes. One such technology used for security purposes is "Facial Recognition". And there are external forces who take advantage of the vulnerabilities of this technology by "Face Spoofing". This paper aims to elaborate the various techniques in face liveness detection. These techniques will enable the creation of a system which will be able to properly distinguish between a real and a fake face and thus limit the vulnerabilities of the face recognition system leading to a better level of security wherever face recognition is used.*

Key Words: Face liveness Detection System, Machine Learning, Deep learning, Face Detection, Face spoofing

1. INTRODUCTION

People are increasingly relying upon technology for the completion of their daily tasks. As the usage of smart devices increases, there is a need for securing these devices against people with malicious intentions. The threat to security is high and the consequences are dire if unauthorized access is gained to such systems. Personal data, organizational sensitive information, high risk information is secured in such systems. Hence, properly securing these systems is essential. Face verification has become the most popular method employed for this task; however, it is vulnerable to diverse spoofing attacks. Face liveness detection, which is also referred to as face spoofing detection, has been devised to defend against spoofing attack.

The emergence of machine learning, deep learning, and computer vision tools have made face liveness detection efficient and feasible for general purpose use. Here we have mentioned few approaches which have helped us in solving this security problem.

2. Approaches based on feature(s) extracted from image captured:

The first step of face liveness detection is feature extraction. Depending on the feature(s) extracted, the accuracy and efficiency of the liveness detection system varies. The different approaches are elaborated further.

2.1 Texture Analysis approach:

A. Face Liveness Detection Using a Flash Against 2D Spoofing Attack [1]:

This paper makes use of flash for detection of 2D face spoofing attack. Flash is used to emphasize the difference between legitimate and illegitimate users, as well as lessen the impact of other external environment based factors. The paper states a method which consists of capturing two images of the subject, one with flash and one without. This model makes use of four texture and 2D structure descriptors having low computational complexity, to gather information about the two images. The main advantages of this method are that it does not require the user to co-operate and the cost of installation of flash is very low. The proposed method in this paper is evaluated using a dataset made up of 50 subjects, captured under varying situations. The results of the experiment show that the method proposed in this paper gives better performance when tested under varying scenarios. The paper states that accuracy, running time as well as robustness improves when flash is used.

B. Deep Feature Extraction for Face Liveness Detection [2]:

This paper establishes that in recent times, the use of deep learning based models has shown impressive results in face liveness detection systems. Despite this, very few works have made the use of convolutional neural network (CNN) for working on face liveness detection systems. And those which have used CNN have used various fine-tuning approaches as well as different dataset for the purpose of training. The approach used in this paper is based on transfer learning, making use of some pre-trained CNNs architectures which are well-known, for the purpose. Various deep features are studied and compared on the common ground for face liveness detection in videos. After performing experimental analysis on well-known, publicly available databases such as

NUAA and CASIA-FASD, it is observed that the methodology proposed gives satisfying results which can be compared with the same of other methods.

2.2 Color and Texture Analysis approach:

Face Spoofing Detection using Color Texture Analysis [3]:

Analysis of luminance data from images of face has been a major focus of research about non-intrusive software based face liveness detection systems, and this disregards the color component which can give vital information when detecting face liveness. This paper introduces a unique and fresh approach in face spoofing detection methodologies by making use of color texture analysis. The method proposed in this text focuses on obtaining complementary low level feature data from various color spaces. This information is then utilized in the form of joint color and texture data from the luminance and chrominance channels. To be more precise, feature histograms are calculated for each image band, differently. The paper states that the result of varied experiments performed on three standard datasets, specifically the CASIA Face Anti-Spoofing Database, the Replay-Attack Database and MSU Mobile Face Spoof Database have been excellent. The paper states that the method proposed produces stable performance over all three datasets. The encouraging results imply that under unfamiliar circumstances, facial color texture representation is more reliable than the gray scale one.

2.3 Frequency and Texture Analysis approach:

Face Liveness Detection Based on Perceptual Image Quality Assessment Features with Multi scale Analysis [4]:

In biometrics domain, recognition system is still vulnerable to spoofing attacks (presentation attacks). Among all the biometrics, face has the most threat as it is easily available and accessible. In this paper, an effective approach against face spoofing attacks based on perceptual image quality assessment features with multi-scale analysis was presented. First, it was demonstrated that the blind image quality evaluator (BIQE) was effective. Next, BIQE was combined with the image quality assessment model called Effective Pixel Similarity Deviation (EPSD) which was used to obtain the standard deviation of the gradient magnitude similarity map by selecting effective pixels in the image. A total number of 21 features acquired from the BIQE and EPSD constitute the multi-scale descriptor for classification. Extensive experiments based on both intra-dataset and cross-dataset protocols were performed using three existing benchmarks, namely, Replay-Attack, CASIA and UVAD. The proposed algorithm demonstrated its superiority in detecting face spoofing attacks over many state of the art methods. It is believed that the incorporation of the image quality assessment knowledge into face liveness detection is promising to improve the overall accuracy.

2.4 Feature Fusion approach:

A. Integration of image quality and motion cues for face anti spoofing [5]:

Face recognition has become quite popular mainly due to the fact that it does not inconvenience the user too much. Despite this there is an absence of a single face liveness detection technique that can deal with all manners of spoofing attacks in different environmental factors. This paper proposes a multiple cues based framework to better the generalizability of face liveness detection systems. In order to improve the ability for face anti-spoofing, an extendable multi-cues integration framework for face anti-spoofing using hierarchical neural networks was proposed. It can fuse image quality cues and motion cues for liveness detection. Shearlet was used to develop an image quality-based liveness features. A bottleneck feature fusion strategy can integrate various liveness features effectively. The proposed approach was evaluated on three public face anti-spoofing databases. A half total error rate (HTER) of 0% and an equal error rate (EER) of 0% were achieved on both REPLAY-ATTACK database and 3D-MAD database. An EER of 5.83% was achieved on CASIA-FASD database.

B. Face Liveness Detection Using Defocus [6]:

This paper states that the major problems associated with Face Recognition (FR) systems is their vulnerability when faced with spoofing attacks. The paper proposes a method to withstand such attacks by making the use of defocus technique. Two images are captured of the user, with varying focuses. From these, three features get extracted, which are

A. gradient location and orientation histogram (GLOH),
B. focus and
C. power histogram.

After feature extraction, feature fusion technique is utilized for identification of fake faces. This paper makes use of two different databases to provide better performance assessment, using once a digital camera and once a webcam. The method that this paper proposes can be used in equipment consisting of a camera.

2.5 Feature re-capture approach:

Face Liveness Detection with Recaptured Feature Extraction [7]:

This paper focuses on distinguishing between real images which it classifies as images of a real scenario and fake images which are classified as retaken images of previously captured videos or photos. The method proposed aims to extract three types of features, which are
1. Specular reflection ration,
2. Hue channel distribution,
3. Blurriness

This method is effective because of the differences that exist between the two types of images under consideration in this paper. These are,

1. Real images have smaller reflection ratio when compared with fake images.
2. Image color distribution proportions might change according to the display screen and print.
3. Images of real faces have high frequency information when in comparison with fake images.

3. CONCLUSIONS

In this paper we discussed the various approaches a face liveness detection system can be based on, by focusing on the types features extracted from the image or video. We found that using feature fusion when extracting features and opting for a deep learning model which consists of CNN and SoftMax classifier proved to be most useful. Also by selecting color texture feature extraction model and making use of both the luminance and chrominance data, admirable results can be obtained. Thus, among many types of features to be extracted, we found feature fusion approach using CNN most useful.

REFERENCES

[1] Patrick P. K. Chan, Weiwen Liu, Danni Chen, Daniel S. Yeung, Fei Zhang, Xizhao Wang and Chien-Chang Hsu, "Face Liveness Detection Using a Flash Against 2D Spoofing Attack" IEEE Transactions On Information Forensics And Security, Vol. 13, No. 2, February 2018

[2] Abdulkadir Şengür, Zahid Akhtar, Yaman Akbulut, Sami Ekici, Ümit Budak "Deep Feature Extraction for Face Liveness Detection" Firat University Elazig, Turkey, INRS-EMT, University of Quebec, Canada, Bitlis Eren University, Turkey

[3] Zinelabidine Boulkenafet, Jukka Komulainen and Abdenour Hadid "Face Spoofing Detection Using Colour Texture Analysis" IEEE Transactions On Information Forensics And Security

[4] Chun-Hsiao Yeh Herng-Hua Chang, Computational Biomedical Engineering Lab, Department of Engineering Science and Ocean Engineering, National Taiwan University, Taiwan "Face Liveness Detection Based on Perceptual Image Quality Assessment Features with Multi-scale Analysis" 2018 IEEE Winter Conference on Applications of Computer Vision

[5] Litong Feng, Lai-Man Po, Yuming Li, Xuyuan Xu, Fang Yuan, Terence Chun-Ho Cheung, Kwok-Wai Cheung "Integration of image quality and motion cues for face anti-spoofing: A neural network approach" J. Vis. Commun. Image R. 38 (2016) 451–460

[6] Sooyeon Kim, Yuseok Ban and Sangyoun Lee "Face Liveness Detection Using Defocus" Sensors 2015, 15, 1537-1563; doi:10.3390/s150101537

[7] Xiao Luan, Huaming Wang, Weihua Ou and Linghui Liu "Face Liveness Detection with Recaptured Feature Extraction" 2017 International Conference on SPAC Security, Pattern Analysis, and Cybernetics ()