**IJARCCE** ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

**Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022**

DOI: 10.17148/IJARCCE.2022.114141

# LIVENESS OF FACE

**Pratyush Agrawal[1], Shivendra Shukla[2] , Shreya Rawat[3] , Prince Dogra[4] and Neha Gupta[5]**

[1–4]Student, Department of Information Technology, Inderprastha Engineering College,

Sahibabad Site IV, Ghaziabad 201010, Uttar Pradesh, India

[5]Assitant Professor, Department of Information Technology,

Inderprastha Engineering College, Sahibabad Site IV, Ghaziabad 201010, Uttar Pradesh, India

**Abstract:** This research paper aims at exploiting efficient ways of tackling face spoofing problem. Face recognition is one of the most prevalent bio metric approaches used. This technology has expeditiously advanced in recent years, due to it being more in-line, user-friendly and easy to use than other methods. Liveness detection creates a secured system which helps in protecting the system against spoof attacks using non real or fake faces like photographs. The approach used by us in our work are classified according to the various procedures used for liveness detection which helps to understand the solutions developed for different spoof attack scenarios. The primary goal is to provide a well-developed and impenetrable face liveness detection approach.

## INTRODUCTION

Biometrics are the fastest growing segment of such security industry. This technology formulates individual identity based on physical and behavioral features of the individual. Some popular techniques used for biometric are facial recognition, hand geometry, fingerprint recognition, retinal as well as iris scanner. Among these techniques, face recognition technology has developed the most in recent years due to it being user friendly, easy to use and more direct than other approaches. Therefore, it has been applied to various security systems. However, face recognition algorithms generally fail to distinguish between 'live' face from 'not live'(spoofed) face which can cause a major security issue.

Liveness is the process or art of distinguishing the feature space into live (real) and non-living (spoofed). Imposters will try to insert as many spoofed biometrics into system as possible. This can be prevented using the concept of face liveness which will in turn improve the performance of the biometric system. This ability to differentiate between live and non-live faces plays an important factor in determining the reliability of biometric system security against such spoof attacks. In recent years, Liveness detection has gained attention of researchers mainly to be used in fingerprint recognition and iris recognition while face recognition technology is very limited to deal with this problem. For face recognition to be applied in our daily life, this anti-spoofing issue must be resolved. As the social networking websites (YouTube, Facebook, Instagram and others), gain popularity, it has become very easy for the imposters to gather content that can be used to spoof a face authentication system. To counter this vulnerability of face authentication systems, several active measures have been taken against face spoofing, one of which is Micro-texture analysis which has been effectively extended in the field of facial recognition and authentication, recently.

## LITERATURE SURVEY

There are many approaches implemented in Face Liveness Detection. In this section, some of the most interesting liveness detection methods are presented.

### *A. Frequency and Texture based analysis*

Frequency and Texture based analysis This approach is used by Gahyun Kim et al. In this approach, the real and spoofed faces are differentiated on the basis of shape and detailedness which differentiates between the real face and 2-D masks based on frequency and texture analysis. To analyze the texture of the facial image a description method based on Local Binary Pattern (LPB) is used. This approach relies on the fact that the texture information extracted from 2-D objects loses details as compared to when extracted from 3-D objects. Facial images are transformed into the frequency domain with help of 2-D discrete Fourier transform for extracting frequency information which is then divided into several groups of concentric rings where each ring represents a corresponding region in the frequency band after which a 1-D feature vector is acquired by combining the average energy values of all the concentric rings.

For fusion-based feature extraction, Support Vector Machine (SVM) classifier are used for learning liveness detectors with the feature vectors generated by power spectrum based and LBP-based methods. This method extracts a feature vector by the combination of the decision value of SVM classifier trained by power spectrum-based feature vectors and SVM classifier trained by LBP-based feature vectors. Three different illumination condition were used to capture the real faces dataset and printed paper, magazine and caricature were used to create the fake faces dataset. Overall, the fusion-

DOI: 10.17148/IJARCCE.2022.114141

based method proved to be the best with error rate of 4.42% compared to frequency based with 5.43% and LBP-based method with 12.46%. Similar technique was proposed by Jukka et al with the key idea to emphasize the differences of micro texture in the feature space.

A local binary pattern (LBP) was adopted for microtexture analysis and spatial information. The feature space vectors are then given as an input to an SVM classifier which characterizes the face as a real or spoofed face on the basis of micro-texture patterns. The process initiates when a face is detected which is then cropped and normalized and then converted into a 64 × 64 pixel image. Then, a LPB operator is applied to this normalized image and then the resulting LPB face image divided into 3×3 overlapping regions. From each region, a local 59-bin histograms is obtained which are then computed and collected into a single 531-bin histogram. Using the LPB operator two other histograms are obtained of the whole face. Finally, to determine whether the faces are real or not, a nonlinear SVM classifier with radial basis function kernel is used.

B. *Variable Focusing based analysis*

Sooyeon Kim et al [3] implemented this technique of face liveness detection using variable focusing. This approach utilizes the variation of pixel values by focusing between two images sequentially taken in different focuses. Assuming that there is no big difference in movement, the authors have tried to find the difference in focus values between real and fake faces when two sequential images are collected from each subject. The focused regions in real faces are clear and others are blurred due to depth information. Whereas, the difference between the images taken in different focuses of a printed copy of a face (fake face) is minute since they are 2-D. This method relies on the degree of Depth of Field (DoF) which is a basic constraint for this approach. The DoF is the range between the nearest and farthest objects in a given focus. For improving the liveness detection performance, focusing effect for which the DoF should be narrow are increased.

Sum Modified Laplacian(SML) is used for focus value measurement. Firstly, two sequential pictures are taken by focusing the camera on facial components where one is focused on a nose and the other is on ears. This is done because the nose is the closest to the camera lens, while the ears are the farthest. It is this difference in the patterns between real and fake faces are used as features to detect face liveness. For testing, the two main parameter considered are False Acceptance Rate (FAR) and False Rejection Rate (FRR). It was observed that when Depth of Field (DoF) is very small, FAR is 2.86% and FRR is 0.00% but when DoF is large, the average FAR and FRR is increased. Thus, it was concluded that this approach is dependent on the DoF and it is very crucial to make the Dof small.

*C. Movement of the eyes-based analysis*

The technique built around the analysis of eyes' movement was initially introduced by Hyung-Keun Jee et al for integrated facial recognition system. This method proposed detecting eyes in sequential input images after which the the variation in each ocular area is calculated to determine whether the face is live or not. The key idea behind this approach is that due to blinking and other uncontrolled movements of the pupils, there should be big shape variations. This method detects the center point of both eyes in the input face image after which the facial area is normalized and the areas of the eye are then extracted. Then these extracted eye regions are binarized and of these each binarized eye regions are compared and calculation of variance takes place.

For an image to be categorized as a live face the result should be greater than the threshold otherwise it is identified as a photograph. Intensity of the eye region is lower than the rest of face region if the image is considered as a 3D curve. Gaussian filtering to the face image is performed to track down the eye region,so that the smoothened 3D curve is obtained. All the local minimums are extracted from the curve using the gradient descent method.Eye classifier, which is trained by Viloa's AdaBoost training methods, is used to reduce the invalid eye candidates. Then, the face region is normalized through the size and rotation by using center point of eyes as the input face can vary in size and orientation. Self Quotient Image (SQI) is applied to decrease the effect of illumination.

*D. Blinking based analysis*

Lin Sun et al's blinking-based approach for liveness detection using Conditional Random Fields (CRFs) is used to model blinking activities, for accommodating longrange dependencies on the observation sequence. A linear chain structure of CRFs is used by the authors since it has discrete eye state label data yt = 1, 2, . . . , c, t = 1. . .T, and observation xt.

Half-open state is challenging to characterize commonly over the various people, since the eye size of half open state relies upon the individual's eye appearance. The authors have employed two state labels, C used for closed state and NC used for non-close. Video database including blinking video clips and imposter video clips is used to test this approach.

They used a total of 80 clips which is in blinking video database for 20 individuals, 4 clips for each individual: the first clip includes video without glasses in frontal view, the second clip is with thin rim glasses in frontal view, the third clip contains video with black frame glasses in frontal 2 view, and the last clip is having video without glasses in upward view. The blinking number in each clip varies from 1 to 6 times.

*E. 3D Face Shape based analysis*

DOI: 10.17148/IJARCCE.2022.114141

The novel liveness detection method, based on 3D structure of the face is proposed by Andrea Lagorio et al. 3D features of the captured face is computed by the proposed algorithm to identify if a live face is presented before the camera or not. 2D source can be identified and distinguished due to their lack of surface variation since they have very low surface curvature.

An the approximation of the actual curvature value at each point is calculated from the main components of the Cartesian coordinates within a given neighborhood. The mean curvature of the 3D points lying on the face surface is then computed. The authors designed two experiments. In the first one, they used FS and GVS sets. The distribution of the mean curvature values for the two sets was separated, and the value of the False Rejection Rate (FRR), was computed as zero.

In the second experiment they used the FS and the Bosforus sets. In order to determine the sensitivity of the algorithm, they perform various experiments with values ranging from 4 to 20. For different values of radius, the value of the False Rejection Rate (FRR) at rank 1 is always equal to zero.

### *F. Binary Classification based analysis*

The technique of anti-spoof problem as a binary classification problem was introduced by Tan et al. The key idea is that a real face is different from a photo since the former is 3-D while the later is 2-D. The surface roughness of a real face is different from a photo. The authors presented a real-time and non-intrusive method formulated as a binary classification problem. Two strategies were proposed to extract the essential information about different surface properties of a live human face or a photograph, in terms of latent samples using the Lambertian model.

Two new extensions to the sparse logistic regression model were employed based on these strategies which allow quick and accurate spoof detection. The standard sparse logistic regression classifier was extended both nonlinearly and spatially for classification, to improve its capability of generalizing high dimensional and small size samples. It was observed that the anti-photo spoof performance significantly improved with the nonlinear sparse logistic regression, while the spatial extension leads to a sparse low rank bilinear logistic regression model.

A publicly available photograph-imposter database containing over 50K photo images from 15 subjects is collected by the authors for evaluation purpose. The authors presented a real-time and non-intrusive method formulated as a binary classification problem. Two strategies were proposed to extract essential information on the different surface properties of a living human face or a photo, in terms of latent samples with the help of Lambertian model. Two further expansions to the sparse logistic regression model were employed based on these strategies which allow quick and accurate spoof detection.

The standard sparse logistic regression classifier was extended both nonlinearly and spatially for classification, to improve its capability of generalizing high dimensional and small size samples. It was observed that the anti-photo spoof performance significantly improved with the nonlinear sparse logistic regression, while spatial expansion leads to a small sparse bilinear logistic regression model. A widely available photographic imposter database containing over 50K photographs from 15 subjects is collected by the authors for evaluation purpose.

## PROPOSED METHODLOGY

In this project, we treated liveness detection as an example of Binary Classification Problem. Given an input image, we'll train a Convolutional Neural Network capable of distinguishing real faces from fake/spoofed faces. We trained a liveness detector model which detects and extracts ROIs(region of interest) from our training(video) dataset. To create our liveness detector we utilized OpenCV, Deep Learning, and Python. OpenCV is a cross-platform library using which we can develop real-time computer vision applications. It mainly focuses on image processing, video capture and analysis including features like face detection and object detection. Deep learning is a type of machine learning and artificial intelligence (AI) which mimics how humans acquire certain types of knowledge. Methods are able to take advantage of very large datasets of faces and learn and compact representations of faces, enabling modern models to to first perform as-well and later to outperform the face recognition capabilities of the current system. To build our face recognition system, we'll first perform face detection, extract face embeddings from each face using deep learning, train a face recognition model on the embedding, and then finally recognize faces in both images and video streams with OpenCV. The first step was to gather our real vs. fake dataset.

To accomplish this task, we: First recorded a video of ourselves using our smartphone (i.e., "real" faces). Held our smartphone up to our laptop/desktop, replayed the same video, and then recorded the replaying using our webcam (i.e., "fake" faces). Applied face detection to both sets of videos to form our final liveness detection dataset. After building our dataset we implemented, "LivenessNet", a Keras + Deep Learning CNN. This network is purposely shallow, ensuring that: We reduce the chances of overfitting on our small dataset.

The model itself is capable of running in real-time (including on the Raspberry Pi). Overall, our liveness detector was able to obtain 89% accuracy on our validation set. To demonstrate the full liveness detection pipeline in action 3 we created a Python + OpenCV script that loaded our liveness detector and applied it to real-time video streams.

## RESULT ANALYSIS

Here, liveness detection approaches are categorized based on the type of liveness indicator used to assist the liveness detection of faces. Three main types of indicators were mainly used: motion, texture and life sign. Motion analysis mainly differentiates the motion pattern between 3D and 2D faces.It uses the fact that, planar objects move significantly different from real human faces which are 3-D objects. Motion analysis usually depends on optical flow calculated from video sequences. When using motion analysis, it is very hard to spoof by 2D face image and is independent of texture and user collaboration is not needed.

But, motion analysis needs video and it is very difficult to use motion analysis when the video have low motion activity. This approach can be spoofed by 3D sculptures and it needs high quality images. Texture analysis techniques mainly take the advantage of detectable texture patterns such as print failures, and overall image blur to detect attacks. This approach works on the assumption that fake faces are printed on paper, and the printing process and the paper structure that produce texture features can differentiate those printed images from real face images.

Here, the user face is printed on a paper and presented in front of the camera for verification or identification. Using texture analysis to identify real faces is useful in such situations, as the printing procedure and paper usually contains high texture characteristics. Texture analysis-based approach is easy to implement and it does not need user collaboration. But, a very diverse paper and printing textures can occur, and the systems built on texture analysis must be robust to different texture patterns which require the existence of a very diverse dataset.

It is also possible that the attack is performed using a photo displayed on a screen, which will produce very low texture information. Motion analysis will be helpful to get over the dependency on certain texture patterns. However, motion analysis may face problems when there is low motion information. This can happen because behavior of the user may be different, high noisy images and low resolution. Motion analysis might also fail when spoof attacks is performed using more sophisticated methods, just like 3D sculpture face model.

## FUTURE SCOPE

• Accuracy of this project model is average:

The proposed model has limited dataset thus making it somewhat bias towards the dataset. We are trying to overcome it by introducing or adding more dataset and thus increasing the accuracy.

• The screening or filtering mechanism are still in their early stages:

The screening mechanism is still in early stage thus working on distorted or low-quality video is not as effective as expected.

• This project does not work with multiple faces:

The major drawback of our research is that it works only on single face. In case of multiple faces, the detector might work incorrectly.

• This project doesn’t work with animal faces:

Needless to say, we haven’t tried or worked on animal faces. So, it is a domain left unexplored.

## CONCLUSIONS

Inspired by various face liveness detection techniques, we came up with the above proposed methodology which gives around 89% accuracy on our validation set. It may be biased towards the dataset we used as we have used very limited dataset with limited overfitting. The training accuracy might change as we increase our dataset but it will all lead to a better facial recognition system. Experiments carried out with a unified experimental setup and evaluation methodology showed that the dynamic texture-based countermeasure was able to consistently outperform prior work on both datasets. In a future work, we will study the generalization capabilities of the proposed countermeasure using multiple face antispoofing databases. In other words, we plan to perform cross-database experiments by training and tuning the face description solely on one dataset and test on another one.

## REFERENCES

[1] Asim, M.; Ming, Z.; Javed, M.Y. CNN based spatio-temporal feature extraction for face anti-spoofing. In Proceedings of the 2017 2nd International Conference on Image, Vision, and Computing (ICIVC), Chengdu, China, 2–4 June 2017; pp. 234–238.

[2] Tu, X.; Zhang, H.; Zie, M.; Luo, Y.; Zhang, Y.; Ma, Z. Enhance the Motion Cues for Face Anti-Spoofing using CNN-LSTM Architecture. arXiv 2019, arXiv:1901.05635.

[3] 1Saptarshi Chakraborty1 and Dhrubajyoti Das Dept. of Computer Science and Engineering, National Institute of Technology, Silchar, India, International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014.

[4] Parveen, S.; Ahmad, S.M.S.; Abbas, N.H.; Adnan, W.A.W.; Hanafi, M.; Naeem, N. Face Liveness Detection Using Dynamic Local Ternary Pattern (DLTP). Computers 2016, 5, 10.

DOI: 10.17148/IJARCCE.2022.114141

[5] Gragnaniello, D.; Sansone, C.; Poggi, G.; Verdoliva, L. Biometric Spoofing Detection by a Domain-Aware Convolutional Neural Network. In Proceedings of the 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Naples, Italy, 28 November–1 December 2016; pp. 193–198.
[6] Rehman, Y.A.U.; Po, L.M.; Liu, M. LiveNet: Improving features generalization for face liveness detection using convolution neural networks. Expert Syst. Appl. 2018, 108, 159–169.
[7] Wang, T.; Yang, J.; Lei, Z.; Liao, S.; Li, S.Z. Face Liveness Detection Using 3D Structure recovered from a single camera. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–6.
[8] Tang, D.; Zhou, Z.; Zhang, Y.; Zhang, K. Face Flashing: A Secure Liveness Detection Protocol Based on Light Reflections. arXiv 2018, arXiv:1801.01949.
[9] Yeh, C.; Chang, H. Face Liveness Detection Based on Perpetual Image Quality Assessment Features with Multi-Scale Analysis. In Proceedings of the 2018 IEEE Winter Conference on Applications of Computer Vision (WACV), Lake Tahoe, NV, USA, 12–15 March 2018; pp. 49–56.