ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2020 , Volume 1 Issue 2
www.ijisea.org

Face Liveness and Spoof Face Detection and Role of Different classifiers – An Image Processing Perspective

[1] Suresh Bojja , [2] K Naga Prakash
Research Scholar , ECE Department , J.N.T.U.K, Kakinada, Andhrapradesh, India
Professor, ECE Department,GEC , Gudlavalleru, Andrapradesh, India
[1]Surem9@gmail.com , [2]drprakashece@gmail.com

ABSTRACT

Faceliveness detection is a broadly utilized biometric approach. Faceliveness detection is innovation has grown quickly in recent years and it is more straightforward, easy to use and there are so many advantages contrasted with different strategies. In any case, Faceliveness detection has to be robust against Spoof attacks made by non-genuine countenances. In Spoofing attacks, there are different ways to spoofing the recognition system by facial pictures, photo graphs, Masks and playing the video. A safe framework needs Liveness detection, so here we need a Robust Liveness face Recognition as to make and guard the spoof. In this work, face liveness detection and Spoof face detection approaches are categorized based on the various methods and different types of classifiers used for liveness detection and spoof face detection. This literature review helps to understand different spoof attack cases, different methods used for overcome spoof attacks in face recognition system and role of different classifiers. Here, in this paper provides a simple way to understand development of novel and more secured face liveness detection approaches in future.

Key Words: Faceliveness, Spoof attacks, Classifiers

I. INTRODUCTION

In the Real world, there is immense need for security measures against spoofing attacks in bio metric systems. Biometric systems are the quickest developing section of such security industry. There are, some of the known techniques for recognition are facial acknowledgment, fingerprint recognition system, geometry recognition like handwriting, eye recognition system in that , iris and retinal scanner is used. Among these methods, the one which has grown quickly in recent years is Faceliveness recognition system and it is more straightforward, easy to use and helpful contrasted with different strategies. Consequently, it has been applied to different security frameworks. Be that as it may, all in all, face Recognition calculations are not ready to separate 'live' face from 'not live' face which is a significant security issue. It is a simple method to spoof face frameworks by facial pictures, for example, representation photos. So as to make preparations for such parodying, a protected framework needs liveness location.[1]

By this, a review of the most interesting face liveness detection and Spoofing Attacks are Discussed. Then, advantages and disadvantages of various face liveness detection and attacks approaches are discussed. From this, we can compare various techniques to conclude.[2]

II. RELATED WORK

A) GENERALIZED FACE RECOGNITION SYSTEM

A block diagram of face liveness detection and Spoof face Detection system flow is shown in Figure 1, it is important to explain the specific procedure of utilizing liveness detection framework which includes a client to present a biometric sample to the sensor, which is a camera for our situation. The sample image which is pre-processed for the success of the next steps. In the pre-processing the image could be enhanced by using different types of filters. So the sample image is prepared to the subsequent stage of highlighting for the extraction of features. From the feature extraction process is a recognizable sample with distinct features highlights and that permits classifier to choose whether introduced sample test image is genuine (Real) or face (mock) by the training data which is available already. Here , there are different types of classifiers are available for recognition of the liveness(real) or Spoof face (fake).Genuine samples will be pre-processed for identification, while spoofed samples will be automatically discarded for authentication, and in order to measure the performance of liveness detection system.

The following measurements used for Liveness Detection and Spoof Face Detection are defined:
(i)False Reject Ratio (FRR): it is the rate where a live sample is identified as a spoof attack. (ii)False Acceptance Ratio (FAR): it is the rate of system where a fake sample is authenticated as live (genuine) sample.(iii)Failure to Acquire (FA): it is the rate of the system when it fails to perform samples collection.(iv)Mean Transaction Time (MTT): it is the average of system's required time for making a decision.(v)Receiver Operating Characteristic (ROC): Plots that are used to select the operating threshold of the system with prior knowledge of the FRR and FAR probability. [4]

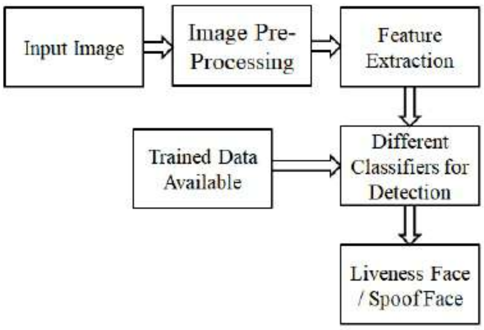

Figure 1: Shows the Block diagram of generalized face liveness and Spoof Face detection system

B) SPOOF ATTACKS IN FACE RECOGNITION SYSTEM

This section examines different types of Spoof Attacks and the strategies use for face spoof recognition. Industries as well as cell phones organizations are likewise incorporating these face detection techniques in their gadgets for locking and opening the phones. A few research articles, conferences and Research journals accompanied imaginative thoughts for giving security to confront face Spoof Recognition system.

1. Attack by the Photographs: This attack is a simple attack, that a fake person will attack the system by presenting a photograph of the approved user. The Attackers can either catch the photos from an advanced gadget, for example, a camera or a mobile without taking consent from the person or can obtain photographs from the web-based life stage like social media. The attacker either prints the image or displayed in front of the face recognition devices to make fraud accessing of system.

2. Attack by Replay Video: This attack not uses the photographs, but attacker uses a replay video of the approved person, and that video has the behavior traits of an individual like blinking of eye and expressions like lip and head movement. Hence these Replay video attacks more efficiently works compared with the attack by the photographs.
3. Attack by 3D or Paper cut Mask: This attack is more authenticating than the photographs and video attacks. For making efficient face recognition system against this mask attacks in this days is very important. The 3D masks are made by the expensive 3D printers. [6]

By Comparing with the photographs, another prominent characteristic of live face is the occurrence of the non-rigid deformation and appearance change, such as mouth and lip movement variations and 3D or Paper cut masks.

III. DIFFERENT METHODOLOGIES USED IN LIVENESS FACE RECOGNITION SYSTEM

A) BASED ON TEXTURE

Image quality assessment, Dynamic and Static texture Analysis, color parameters

In the Texture Based analysis the genuine user texture pattern will be used to detect the Real Face (Liveness Face) or Fake Face (Spoof Face). Here the texture features are obtained from the face image or sequence of images. Generally this texture based analysis classified in to 3 categories: Parameters which are used for image quality assessment, Dynamic Texture analysis and Static Texture Analysis [10].

(i) Parameters which are used for image quality assessment: are generally called Image Quality Assessment (IQA) Parameters where IQA attempts to assess the errors in input face image. The parameters are consider here are Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Normalized Absolute Error (NAE), Signal to Noise Ratio (SNR), Total Edge Difference (TED), Maximum Difference (MD), Structural Similarity Index (SSI) and Average Departure (AD). Each of these eight IQA parameters is presented in Table-1.

Table 1: Shows Image Quality Assessment Parameters (IQA)

Acronym	Description	Reference
PSNR	$PSNR(I,\hat{I}) = 10log\left(\frac{Max(I^2}{MSE(I,\hat{I})}\right)$	[1], [2]
MSE	$MSE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})^2$	[3],[5]
NAE	$NAE(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j} - \hat{I}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j}\rvert}$	[4], [6], [7]
SNR	$SNR(I,\hat{I}) = 10\log\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{NM.MSE(I,\hat{I})}\right)$	[8]
TED	$TED(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{E_{i,j}} - \hat{I}_{E_{i,j}}\rvert$	[9]
MD	$MD(I,\hat{I}) = Max\,\lvert I_{i,j} - \hat{I}_{i,j}\rvert$	[10],[11]
SSI	$SSI(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_y^2 + \sigma_y^2 + C_2)}$	[3],[4]
AD	$AD(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})$	[5],[6]

These assessment parameters are compared with the Liveness or spoof face by compared by finding the EER, FAR, HTER values when compared to existing methods for Face Live Detection.[12]

(ii) Dynamic Texture Analysis: In this Texture analysis spoofing detection can be identified by spatiotemporal LBP (Local Binary Patterns).In this, analyzing the structure of the facial areas using LBP – TOP (Three Orthogonal Planes) provides an efficient face recognition system. [11]
(iii) Static Texture analysis :In this analysis an empirical evaluation study is performed which compares indexing the values for the planes , if it is the colour image, grey scale texture, and colour texture methods for classification tasks on texture images data set taken under either (constant)Static conditions.[14]

B) BASED ON MOTION

(i) Focus distance based: In this analysis is it relies on Depth of Field (DoF) [17] which determines the range of focus variations at pixels from the sequentially taken images. The DoF is the range between the nearest and farthest objects in a given focus. To increase the liveness detection performance[16].Based on different distance based camera focusing and lightning conditions the images are captured from the genuine user, from this liveness detection will be carried out.

C) OPTICAL FLOW BASED

In this method, face images are extracted from a sequence of frames, from this optical flow is calculated. The optical flow calculated as, first calculate the velocity vector ‘x’ of each pixel which gives the information like speed and direction of the pixel, which is moving. In this technique each frame converted into a set of vectors, which gives the information about each pixel direction and velocity motion in between each frame, which contains information about type of motion and the object. By this motion vector is determined i.e the length of the motion vector. Thus the motion of the object can be represented by optical flow. After obtaining the motion information converted into images. By using different classifiers liveness face is recognized. [15]
(iii) Clues Based method: A high quality training data or with the user collaboration an Accurate and reliable Faceliveness detection system will be developed in this clues based method. Table 1 outlines these spoofing information, as far as input information (Image) quality, equipment, and client joint effort, for examination. [5]

Table 2 : Shows Outlines spoofing information

	Data Quality	Additional Hardware	User Collaboration
Signs			
Facial expression	High	No	Middle
Depth information	High	No	Low
Mouth movement	Middle	No	Middle
Head movement	High	No	Middle
Eye blinking	Low	No	Low
Degradation	High	No	Low
Multi-modal	***	Yes	Middle/High
Facial thermogram	***	Yes	Low
Facial vein map	***	Yes	Middle
Interactive response	***	Yes	High

D) BASED ON FACE SIGN INDICATIONS: EYE BLINKING OR LIP MOVEMENT

Blinking activity is an action represented by the image sequence which consists of images with close and non-close state. The eye movement based system is for detecting eyes in sequential input images and then variation of each eye region is calculated and whether the input face is real or not is determined.[16] In few techniques conditional Random Fields (CRFs) are used for face liveness detection by blinking activities and lip movements or we can say facial expressions. Using different types of discriminative models we can compare the CRFs which are generated by observation sequence of images.[18][19]

C) BASED ON MORPHOLOGICAL OPERATIONS

Using of morphological operations is a new approach for detecting the live ness face in face recognition system. In this technique boundary scalar transformation of original and morphological constructed profile shapes are generated. From these profile shapes a set of feature vectors is created. A ranking of most similar faces was obtained by ordering the Euclidean distances. Morphological opening and closing of the profile silhouette gives new information about profile faces and decrease differences among profile images. By using the profile shapes face liveness or Spoof face will be detected in the recognition system. [20].

IV.CLASSIFIERS USED IN FACE RECOGNITION SYSTEM

There are different types of classifiers which are used in the face recognition system, which are the decision makers for detecting the fake or real face. Hence, these classifiers are plays an important role in any face recognition system. These classifiers are like SVM (Support Vector machines), CNN (Convolution Neural Networks), Decision Tree, K-NN.

A) SUPPORT VECTOR MACHINE

SVMs is an efficient classifier used in face recognition system. The Support vector machine comes in the category of supervised learning .The SVM used for regression and classification. Support Vector Machines (SVMs) as a very effective method for general purpose pattern recognition. Intuitively, given a set of points belonging to two classes, a SVM finds the hype plane that separates the largest possible fraction of points of the same class on the same side, while maximizing the distance from either class to the hyper plane. This hyper plane is called Optimal Separating Hyper plane (OSH) which minimizes the risk of misclassifying. The application of SVMs to computer vision problem. Train a SVM for face detection, where the discrimination is between two classes: Liveness face and Spoof face. The other application of the is used to recognize 3D objects also. However, the appearances of these objects are explicitly different, and hence the discriminations between them are not too difficult. It is difficult to discriminate or recognize different persons (hundrends or thousands) by their faces because of the similarity of faces. Hence, the discrimination functions learned by SVMs can give much higher recognition accuracy than the popular standard Eigen face approach [21][22] [23].The advantages of SVM are very efficient method ,but it has algorithm complexity is more and it run slowly.

B) CNN (CONVOLUTION NEURAL NETWORKS)

The convolutional neural network (CNN) is a class of deep learning neural networks. CNNs represent a huge breakthrough in image recognition. They're most commonly used to analyse visual imagery and are frequently working behind the scenes in image classification. CNN has different layers; they are Convolutional layers, ReLU layers, pooling layers, and a fully connected layer. In this, Convolutional layers apply a convolution operation to the input. This passes the information on to the next layer. Pooling combines the outputs of clusters of neurons into a single neuron in the next layer. Fully connected layers connect every neuron in one layer to every neuron in the next layer. After this, Processes the features through the network. The final fully connected layer provides the "voting" of the classes. Trains through forward propagation and back propagation for many, many epochs. This repeats until a well-defined neural network with trained weights and feature detectors.by this CNN will identifies the liveness and spoof face in recognition system. This CNN is very efficient for large data set, but high computational cost and lazy learner.

C) DECISION TREE

Decision tree also uses supervised learning algorithm and is used for classification. Decision tree is applicable in both cases that are continuous and categorical output and input variables. A decision tree is defined as a connected, acyclic, undirected graph, with a root node, zero or more internal nodes (all nodes except the root and the leaves), and one or more leaf nodes (terminal nodes with no children), which will be termed as an ordered tree if the children of each node are ordered (normally from left to right). A tree is termed as univariate, if it splits the node using a single attribute or a multivariate, if it uses several attributes. A binary tree is an ordered tree such that each child of a node is distinguished either as a left child or a right child and no node has more than one left child or more than one right child. For a binary decision tree, the root node and all internal nodes have two child nodes. All non-terminal nodes contain splits.

A Decision Tree is built from a training data set, which consists of objects, each of which is completely described by a set of attributes and a class label. Attributes are a collection of properties containing all the information about one object. Unlike class, each attribute may have either ordered (integer or a real value) or unordered values (Boolean value). These attributes form the internal nodes of a decision tree, while the values of these attributes represent the branches of the tree. Leaf node represents a class of a classifying attribute. It contains records belonging to the same class. Decision tree is traversed from top to bottom by performing test on each internal node that comes in the way until the leaf node is encountered. If attribute is continuous rather than discrete then a threshold is formed and tests are performed on that threshold value. Several methods have been proposed to construct decision trees. These algorithms generally use the recursive-partitioning algorithm, and its input requires a set of training examples, a splitting rule, and a stopping rule. The decision trees are generally categorised as Classification tree (predict a class for a new instance) and Regression tree (predict a real number).[24]

D) K-NN CLASSIFIER

The K-NN is also the classifier of the category of supervised learning algorithm. In supervised learning the targets are known to us but the pathway to target is not known. To comprehend machine learning nearest neighbour's forms is the perfect example. Let us consider that there are many clusters of labelled samples. The nature of items of the same identified clusters or groups are of homogeneous nature. Now if an unlabelled item needs to be labelled less than one of the labelled groups. Now to classify it K-nearest neighbours is easy and best algorithm that have record of all available classes can perfectly put the new item into the class on the basis of largest number of vote for k neighbours. In this way KNN is one of the alternate to classify an unlabelled item into identified class. Selecting the number of nearest neighbours or in another words calculating k value plays important role in determining the efficiency of designed model.

The accuracy and efficiency of k-NN algorithm basically evaluated by the K value determined. A larger number for k value has advantage in reducing the variance because of noisy data. The KNN is an unbiased algorithm and have not any assumption of the data under consideration. It is very popular because of its simplicity and ease of implementation plus effectiveness. The k-NN not create model so abstraction process not included. It takes high time to predicate the item. It requires high time to prepare data to design a robust system.[26]

V.CONCLUSION

The main aim is to understand what Faceliveness and Spoof Face in Face Recognition System. By this, the researchers have the reasonable thoughts about face liveness detection new methods, and understand about what are the new strategies to develop new methods and explore the gaps in the research. The growth in the Faceliveness and Spoof Face Recognition system is significant in future and there are so many challenges for the researchers for implanting the new ideas, technologies and methods those would result in significant solutions to the problems of the biometric system. Combination of more than one Face Recognition methods on the test data of Spoofing and Liveness information would give the significant solutions in FRS (Face Recognition System).In this paper, explained various methods used in FRS and different classifiers.

REFERENCES:

[1] Anil K. Jain, Patrick Flynn, Arun A. Ross, “Handbook of Biometrics”, Springer, 2008.

[2] AN OVERVIEW OF FACE LIVENESS DETECTION, International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014

[3] Insight on face liveness detection: A systematic literature review, International Journal of Electrical and Computer Engineering (IJECE) Vol. 9, No. 6, December 2019, pp. 5165~5175 ISSN: 2088-8708, DOI: 10.11591/ijece.v9i6.pp5165-5175.

[4] A. Adler and S. Schuckers, Security and Liveness, Overview, in Encyclopedia of Biometrics, S. Z. Li and A. Jain, Eds. Boston, MA: Springer US, 2009, pp. 1146–1152.

[5] G. Pan, L. Sun, Z. Wu and S. Lao, "Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera," 2007 IEEE 11th International Conference on Computer Vision, Rio de Janeiro, 2007, pp. 1-8.Shihong Lao Sensing&Control Technology Lab. OMRON Corporation, Japan lao@ari.ncl.omron.co.jp

[6] A Review on Different Face Spoof Detection Techniques in Biometric Systems M. Tech. Scholar Kanika kalihal Asst. Prof. Jaspreet Kaur Dept. of Electronics and Communication Rayat & Bahra Institute of Engineering & Bio-Technology Mohali, India

[7]T. De Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, “LBP-TOP based countermeasure against face spoofing attacks,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7728 LNCS, no. PART 1, pp. 121–132, 2013.

[8]A. Bhaskar and R. P. Aneesh, “Advanced algorithm for gender prediction with image quality assessment,” 2015 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2015, pp. 1848–1855, 2015

[9] I. Chingovska, A. Anjos, and E. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” Int. Conf. Biometrics Spec. Interes. Gr., 2012, pp. 1–7

[10] P. Pravallika, “SVM Classification For Fake Biometric Detection Using Image Quality Assessment: Application to iris, face and palm print,” in 2016 International Conference on Inventive Computation Technologies(ICICT), 2016.

[11] Freitas Pereira, T.d., Komulainen, J., Anjos, A. *et al*. Face liveness detection using dynamic texture. *J Image Video Proc* 2014, 2 (2014). https://doi.org/10.1186/1687-5281-2014-2

[12] Fernandes, Steven Lawrence, and G. Josemin Bala. "Developing a Novel Technique for Face Liveness Detection", Procedia Computer Science, 2016.

[13] J. Peng and P. P. K. Chan, “Face liveness detection for combating the spoofing attack in face recognition,” in International Conference on Wavelet Analysis and Pattern Recognition, 2014, vol. 2014-Jan., pp. 176–181.

[14] International Journal of Science and Engineering Applications Volume 2 Issue 4, 2013, ISSN-2319-7560 (Online) www.ijsea.com 78 Facial Feature Extraction Based on Local Color and Texture for Face Recognition using Neural Network S.Cynthia Christabel Sethu Institute of Technology. Kariapatti. M.Annalakshmi Sethu Institute of Technology. Kariapatti. Mr.D.Prince Winston SSCE Aruppukottai.

[15] International Journal of Computer Applications (0975 – 8887) Volume 91 – No 1, April 2014 31 A Study of Liveness Detection in Face Biometric Systems S.Hemalatha Assistant Professor Department of Computer Applications Sri Ramakrishna Engineering College Coimbatore-22, India Amitabh Wahi, Ph.D Professor Department of Information Technology Bannari Amman Institute of Technology Sathyamangalam, India.

[16] International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 12, Issue 12 (December 2016), PP.01-09 1 Fuz - SVM Classifier Based Object Face Liveness Detection with Combined HOG-LPQ Mohan K1, Dr. P Chandrasekhar2, Dr. Sak Jilani3 1Research Scholar, Vel-Tech University, Chennai, India. 2Head, Dept. Of Electrical Engineering, Vel-Tech University, Chennai, India. 3Professor, Dept. Of E.C.E, Mits, A.P, India

[17]. sooyeon Kim, Sunjin Yu, Kwangtaek Kim, Yuseok Ban, Sangyoun Lee, “Face liveness detection using variable focusing”, Biometrics (ICB), 2013 International Conference on, On page(s): 1 – 6, 2013.

[18]. Lin Sun, Gang Pan, Zhaohui Wu, Shihong Lao, “Blinking-Based Live Face Detection Using Conditional Random Fields”, ICB 2007, Seoul, Korea, International Conference, on pages 252-260, August 27-29, 2007.

[19]. H. K. Jee, S. U. Jung, and J. H. Yoo, “ Liveness detection for embedded face recognition system”, International Journal of Biological and Medical Sciences, vol. 1(4), pp. 235-238, 2006.

[20] Z. Liposcak and S. Loncaric, "Face recognition from profiles using morphological operations," Proceedings International Workshop on Recognition, Analysis, and Tracking of Faces and Gestures in Real-Time Systems. In Conjunction with ICCV'99 (Cat. No.PR00378), Corfu, Greece, 1999, pp. 47-52.

[21] Shaoyan Zhang and Hong Qiao, "Face recognition with support vector machine," IEEE International Conference on Robotics, Intelligent Systems and Signal Processing, 2003. Proceedings. 2003, Changsha, Hunan, China, 2003, pp. 726-730 vol.2.

[22] See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/2427763 Face Recognition by Support Vector MachinesFace Recognition by Support Vector Machines Guodong Guo, Stan Z. Li, and Kapluk Chan School of Electrical and Electronic Engineering Nanyang Technological University, Singapore 639798 fegdguo,eszli,eklchang@ntu.edu.sg

[23]M. A. Turk and A. P. Pentland. Eigenfaces for recognition. J. Cognitive Neurosci., 3(1):71–86, 1991.]

[24] C. Agarwal and A. Sharma, "Image understanding using decision tree based machine learning," ICIMU 2011 : Proceedings of the 5th international Conference on Information Technology & Multimedia, Kuala Lumpur, 2011, pp. 1-8.

[26] nternational Journal on Future Revolution in Computer Science & Communication Engineering ISSN: 2454-4248 Volume: 3 Issue: 6 , IJFRCSCE | June 2017, Available @ http://www.ijfrcsce.org.Classifiers in Image processing ,1Rama Gaur 2Dr. V.S. Chouhan 1Ph.D. Scholar (ECE) Jodhpur National University, Jodhpur, Rajasthan, India 2Professor and Head ECE department MBM Engineering college, Jodhpur, Rajasthan, India