International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Spoofing Face Detection using LBP Descriptor and KNN Classifier in Image Processing

Priyanka Sharma, Neha Chauhan

Abstract: ***Image processing in today's world used for performing operations on images by using a process of making positive suggestion of face which can be in a photo or video in already existing face database. Extraction of face attributes is done in face detection from photos and also from videos. When any unauthorized person tries to enter in authentication system by presenting fraud image and video is termed as spoofing attack. Biometrics is a technology which recognizes characteristics of human and is prone to spoof attacks. The detection of spoofed faces by recognizing and exploring the fake face and genuine face images is called face spoof detection. The DWT method is used to inspect the textual attribute occurring within the test images. There is a possibility that some unusual disruptions are available like geometric disruption and the artificial texture disruption. Eigen face technique is applicable for taking out attributes. Histogram for every feature or attributes is determined and employed a collation of essence to find out face spoof detection. To explore even if the image is actual and gag, already used approach Support Vector Machine is used. To make face spoof detection more accurate KNN classifier will take the place of the SVM classifier. The Contrast are construct to inspect the performance of the suggest algorithm and the existing algorithm in two parameters accuracy and time of execution. Detection of spoofed faces can be used for security purpose, preventing crime, access control system.***

Keywords: Spoofing attack, Biometrics, Face Recognition, Image Processing, LBP Descriptor, KNN Classifier

I. INTRODUCTION

The procedure use to accomplish some function on the images which produce to renovate the virtue of the image and remove few highlights taken away it is called image processing [1]. Crime is a crucial activity nowadays therefore there is a need of reasonable check on the person so such type of verity course of action are used in manifold region like bank, industries and hospital etc. [2]. In this region there is an enormous favorable outcome, number of applications are applying on them like human-computer interaction, biometric analysis, content-based coding of images and videos [3]. Face are as likely or not the most usual clue used by human to find out the people [4]. Face recognition is the work of fabrication a positive pleading of a face in a photo or video image in position to a previous database of faces [5].

Manuscript published on January 30, 2020.
* Correspondence Author
Priyanka Sharma*, Computer Science and Engineering Department, AP Goyal Shimla University, Shimla, India, Sharma525priyanka@gmail.com
Neha Chauhan, Computer Science and Engineering Department, AP Goyal Shimla University, Shimla, India, e0602@agu.edu.in

It has mostly concentrated on identifying faces from still images due to its extensive range of applications such as person recognition, law imposition, and smart habitat [6]. It start with observation discriminating human faces from other object in the image and then works on identification of these detected faces [7].

A generally virtue manage by excerption a face locality from a human body is known as face detection [8]. As it seems to become most not strenuous action but to be sure it is most strenuous to find out images. We have to mull all the feasible restriction like isolated face or numerous faces, image rotation, pose etc. this allow to standup some false observation of an image, or it occasionally does not accommodate any image [9]. It can be designate in two foremost groups:

A. ***Geometric Approach****:* the pre-processing of the Input image are ready in sequence to detach the background image, then dissimilar facial property are extracted like age, mouth, nose etc.
B. ***Holistic Approach****:* it presume whole parts detail of face rather than restricted part attribute details [10].

In this operation facial region is localized which means to predict those part of an image where a face is present and then formalize the perceived part, So that the face attribute arrangement are in actual location [11]. Biometrics technology are used to compute and examine human body attributes [12]. It can be designate into two parts:

A. ***Physical Characteristics***: it comprise finger print face or iris pattern.
B. ***Activity Characteristics***: it comprise speech indication or wandering pattern.

Biometrics has the prospective to precisely discriminate between permitted person and pretender [26]. This technique involve placing genuine photographs or playing videos recording etc. in the front of camera [13].The discrepancy necessitate become different of gag which is most commonly known as spoofing attack [14]. It is a way of attacking in which attacker submit the fake identity and confirmation to the biometric system in order to acquire ingress to the network [15]. These attack are the attempt to ingress the system by introduce a copy of biometric trait of users which is mode of falsifying the data for access with in system [16]. In face recognition system it is very easy for the attacker procreate attack. Because on the communal networking area the images and videos are very easily obtainable [17]. These attack are very easy to convey by just having digitized images being exhibit on the screen. If we want to discriminate between factual faces and fraud face, face liveness technique is used. Its final cause is investigation of physiological indication inside life [18].

The appointment of exhibit are betimes elucidate series, the exhibit are grouped in three categories: unconfirmed, confirmed and semi confirmed methods.
The automatic text categorization has been broadly considered and enormous favorable outcome is also seen in this region, it also includes machine learning approaches [19].

SVM methods is introduced in order to regression, assortment and pattern remembrance of the details. K-Nearest neighbor depends on analogy learning. The samples are created by n-proportions attributes. Each proportion manifest a point inside some quantum. By every of the distinctive lines the top most part of the training proportions are accumulate in n-proportion pattern [26]. Decision Tree Classifier is abiding supervised learning methods used for the grouping and regression of details. The objective is to encouraging an imitation which can divine the value of a targeted not consistent by just learning straightforward decision manufacturing rules [20].

II. RELATED WORK

Yaman, et al. [21] proposed a deep-learning face spoof detection approach by using two various deep learning methods. The restricted percipient region (LRF)-ELM and CNN are known to happen these two schemes. For increasing the speed of processing of a model, LRF-ELM was introduced lately in which a convolution and pooling layer was included. There are a succession of entanglement along with pooling layers, however, present within CNN. Higher number of entirely attached stratum might also be obtainable within the CNN model. NUAA and CASIA are the two common face deception investigation of databases on which the experiments were conducted to evaluate the performance of proposed approach. The execution of LFR-ELM perspective was known to be preferable within both the databases as per the juxtaposition constituted for the end.
Killioglu, et.al [22] proposed a maiden elevated algorithm to take out the pupils from the eye region. An erratic flank is selected by the proposed spoofing algorithm once the umpteenth constant numbers of frames that include pupils were identified. For activating the chosen direction's LED on a square frame that comprises eight LEADs for each flank, a signal was sent to Arduino. To look into whether the flank to pupil and the continuance of LED match, the direction of eye is observed once the selected LED is activated. The data that comprise liveness details is given as output by the algorithm in occurrence if the compliance's require are adequate. High favorable outcome proportion is attain as per the praxis organizing using this proposed method.

Keyurkumar, et.al [23] designed an abandoned smartphone spoof attack database (MSU USSA) that incorporate not less than 1000 subjects. Using the anterior as well as back camera of a smartphone, the images of print and replay attacks are congregate. Different strength channels, image regions, as well as attribute descriptors are used for examine the image deformation of print and replay attacks. The Android smartphone is used to evolve well organized face spoof detection approach. As per the experiments control it is seen that to perceive the face spoofs of both, cross-database and intra-database trail environments, the proposed methods give effectual results. There were around 20 participants incorporate within the assessment which showed that the performance of proposed method within actual applications was very good.
Alotaibi and Mahmood, [24] proposed a methodical appliance using fixed frame of sequenced frames in order to solve the face spoofing attack matter. For generating a speed-circuitous image, an AOS-construct plan was applied along with a large time step measurement. The sharp boundary and texture attribute attend within the input image are take out by applying large time step variable. When the input video was reclamation twice, it was seen that on every side the organ of sight, snout, lips and cheek regions, there were few sharp boundary and crush regions in attending within the fake face images. Thus, the sharp boundary were destructed and the situation of pixels were changed due to this. Therefore, the scatter frame would be give rise to be given to the deep CNN network by give rise to an auto-encoder within the all-inclusive construction within the future work.

Shervin, et.al [25] proposed a new methodical rules through which the effects of unseen attack types could be known on the basis of certain existing factors. By the command place, the representative that were of indistinguishable to that of a test sample were excluded as per the novel mechanism. For accounting the variability of imaging conditions, two of after and bury database examination were performed by applied the proposed mechanism. This paper proposed a novel along with really pragmatic articulation of the spoofing observation issue with acclaim to the abstract alterations. To train the systems, only the positive samples were require by the new articulation. In the supervision of the end, the examination conducted showed that there was still necessitate to magnify the scrutiny evaluate since the manufacturing of both the strategy was nope up to the mark.

III. PROPOSED METHOD

In this section, we explain our approach of face spoof detection used to differentiate between genuine and spoofed face. The architecture of our proposed system is presented in Fig.1. Which shows different steps. Using DWT technique, textual features are analyzed and attributes are extracted by Eigen feature method and finally we used KNN classifier to find whether the image is genuine and spoofed.

- Following are the various steps of the flowchart:

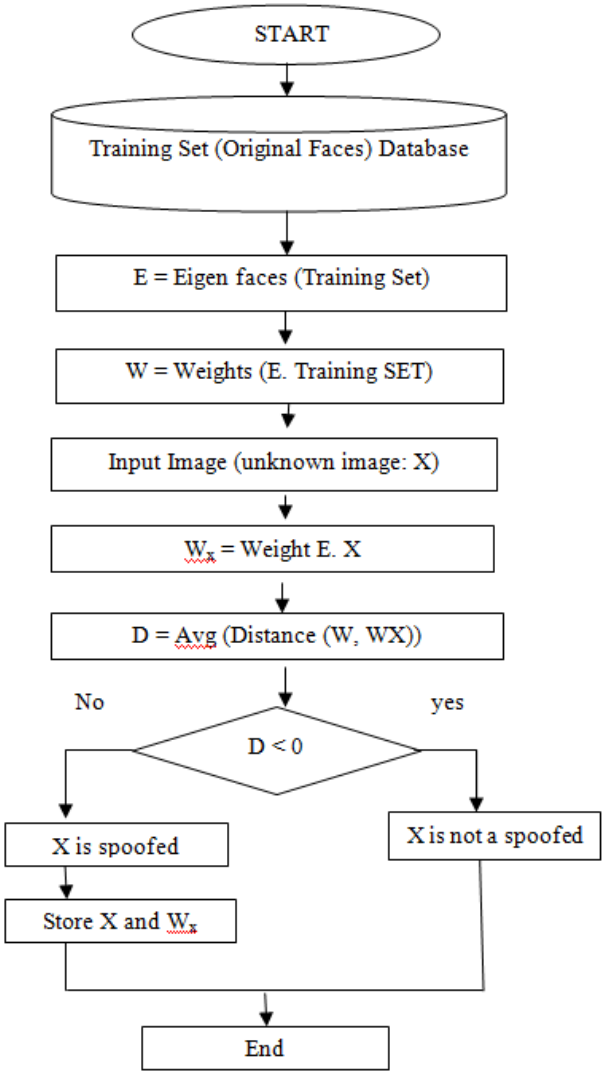

Fig. 1. The flowchart of proposed algorithm

- The following are the description of each steps in detail.

Step 1: Input the number of images to prepare the training set for the spoof and non-spoofed faces
Step 2: Eigen Feature Calculation of input training image
2.1. Calculate the Eigen feature of each image.
2.2. Store the calculated feature in the database with image label.
Step 3: Input the test image which is the unknown image.
3.1. Calculate the Eigen feature of the unknown image.
Step 4: Apply KNN classifier for the detection of spoofed and non-spoofed unknown image
4.1. Calculate distance between the features of the unknown image and all the images Stored in the database.
4.2. If distance between the images is above zero than it is non-spoofed otherwise it is spoofed.

A. Dataset

Input is taken from AT & T dataset. In this type of dataset 10 different images of 40 unique subjects are extracted. All the images should be seize at apart time period having apart lighting, facial gesture (open/closed organ of sight, grin/ not grin) and also have all the facial details. The images have to be seize in dark similar framework with the subject at the upright position, anterior position (some side movements).In this research work, the face spoof discriminant is most broadly used for the discriminant of face spoofing data due to which the uncertified users are prevented in the bio-matrix system. Traditionally the discriminant of the spoofing is executed using SVM classifier method.

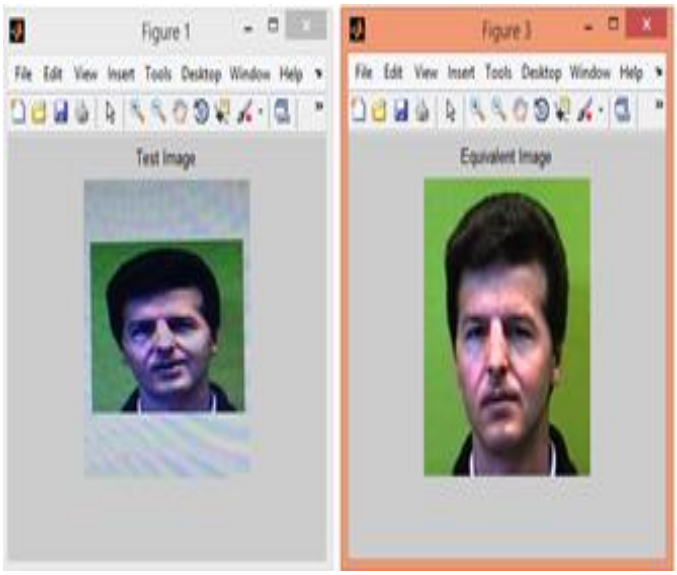

Fig.2. Classification with SVM Classifier

The SVM classifier will take input both training and test set and classify test image into test or equivalent class. The Eigen characteristics remove procedure require to be appeal for the characteristics extraction. The consequence acquire from the SVM classifier assertion the test representation the image is fraud or genuine. The exactness of SVM classifier is dimensioned in the procedure of the ascertain procedure as there are somewhat proportionalities between the textual attributes of the spoofed images. The face spoof discriminant technique is proposed for the classification of fake face and genuine face image. In the first phase, the technique of Eigen face discriminant is applied and applied histogram for face detection for every extracted attributes, and calculate the histogram for that features, and give later input for the classification. The representative are used to describe the n-proportions numeric attributes in the KNN classifier. The point in n-proportions expanse is denoted by a representative. If there is any undisclosed representative present then the KNN classifier match the k-training samples and the pattern space is chosen which is nearest to the unknown representative. Nearness is elucidate by the Euclidean distance. Nearest neighbor classifier smash accompanied by the heaviness to every attribute unlike any other machine learning technique. These circumstances render up to spacious amount of inexactitude when immeasurable amount needless data are present within the network. The nearest neighbor classifier is used for the divination motivation in order to substantiate whether the image is genuine or spoofed. In this way, the average value of the genuine valued connected with the KNN classifier is given back to the classifier. The KNN classifier is examine as the simplest procedure amongst all the other machined learning methods.

The Eigen procedure is used to scrutinize the characteristics interconnected accompanied by the test images. The KNN classifier is appealed where we desire to discriminant whether the image is genuine or spoofed.

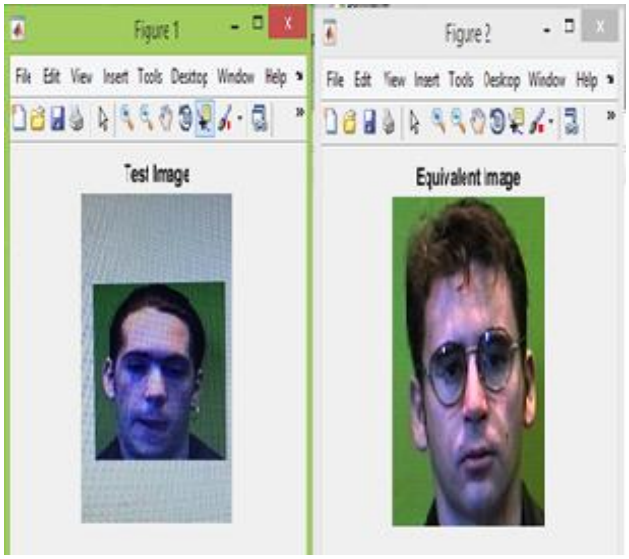

Fig. 3. Classification with KNN Classifier

The attributes of the training image is extracted with the Eigen method and accumulate in the data base. The attributes of the test image is also taken out with Eigen method and is given as input to the KNN classifier. The test image is designate into artificial or genuine class by using KNN classifier.

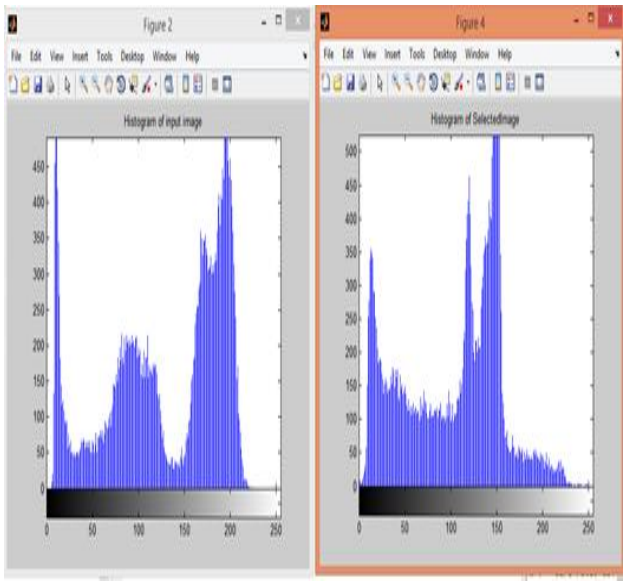

Fig. 4.Histogram of input image and selected image

The histogram bin count of input image in fig.4 shows increase at point 200. While there is decreased in the bin count at 200 in fig. histogram of selected image. It means that the input image is classified as spoofed image because its bin count rises at 200.

IV. EXPERIMENTAL RESULTS

The proposed research is implemented into MATLAB along with the results are evaluated in terms of various parameters as shown below.

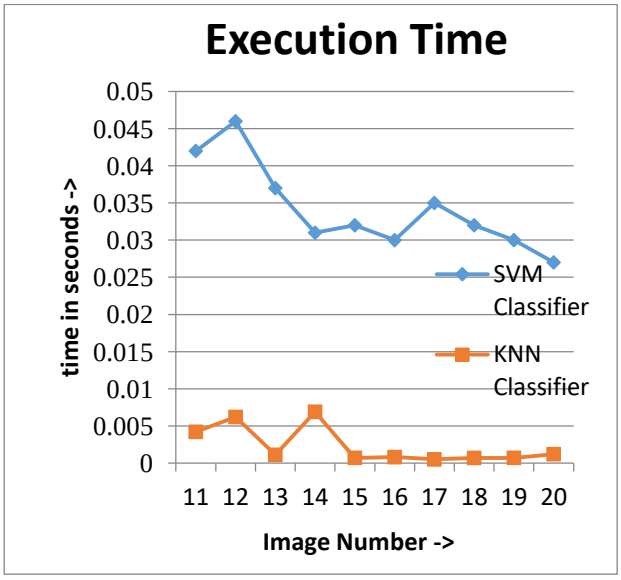

Fig. 5. Execution Time

Fig. 5 display the comparisons amongst the proposed KNN classifier as well as the previously existed approaches of SVM according to their execution time. The results ensure that the KNN classification approach minimizes the execution time accompanied by SVM approach.

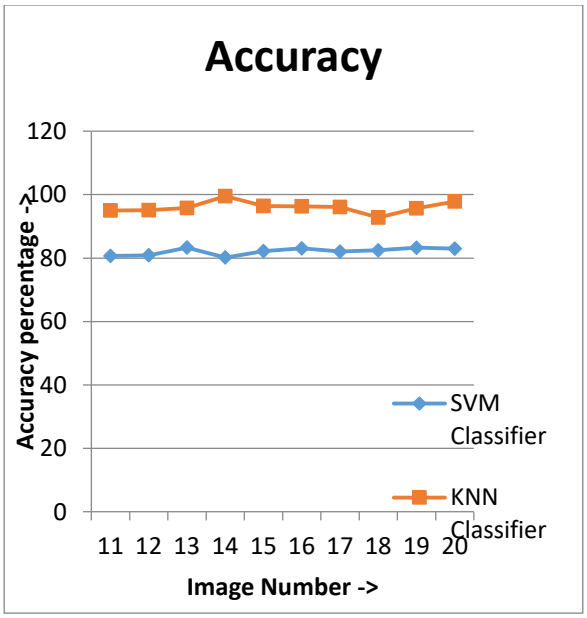

Fig. 6. Accuracy Comparison

Fig. 6. shows the juxtaposition between proposed KNN approach and SVM based face spoof detection scheme based on their accuracy. According to the performed inspect, the accuracy of KNN approach is more than the accuracy of face spoof detection as compared to the prevenient SVM approach.

Images	Accuracy		Performance time	
Image Number	SVM Classifier	KNN Classifier	SVM Classifier	KNN Classifier
11	80.69 %	95.03 %	0.042 second	0.0042 second
12	80.89 %	95.12 %	0.046 second	0.0062 second
13	83.33 %	95.81 %	0.037 second	0.0011 second
14	80.20 %	99.53 %	0.031 second	0.0069 seconds
15	82.20 %	96.46 %	0.032 second	0.0007 seconds
16	83.05%	96.34 %	0.030 second	0.0008 second
17	82.04 %	96.11%	0.035 second	0.0005 seconds
18	82.44 %	92.8 %	0.032 second	0.00069seconds
19	83.25 %	95.7 %	0.030 second	0.0007 seconds
20	82.96 %	97.86 %	0.027 second	0.0012 seconds

Fig.7. Accuracy and performance time comparison between existing and proposed classifier

As shown in Fig.7. the accuracy of the SVM and KNN classifier is compared for the performance analysis. It is analyzed that accuracy of KNN classifier is high as compared to SVM for the face spoof detection. The Performance time of the introduced and present algorithm is compared for the performance analysis. The Performance time of the proposed algorithm is less as compared to existing algorithm. The accuracy is represented in percent and time is represented in seconds.

V. CONCLUSION AND FUTURE WORK

Face spoof detection approach is introduced to recognize the artificial faces added due to the uncertified access to the data. The two steps of face spoof detection approach have attribute extraction and classification. The method of Eigen vector are employed to taking out attributes and SVM is employed for the classification in the extant technique. It is examined that accuracy is diminished for the face spoof detection when SVM classifier is employed. In this research work, the method of Eigen vector are employed to take out attributes and histogram is created which is generated for both input image and selected image. It is employed to demonstrate intensity adumbration of an input image or elected image. The technique of KNN is used at the place of SVM which enhance the accuracy of face spoof detection. The simulation of introduced and extant method is done in MATLAB by considering AT & T dataset. Two parameters are used to examine the performance which are accuracy and execution time. On the foundation of the result acquired there is enhancement in accuracy and the reduce time of execution by using this novel approach proposed in this work. Thus highest accuracy of image is 99.53% and least time of execution is 0.0005 second. In future, the proposed algorithm can be tested in the other classifiers like Naïve Bayes for the face spoof detection. The proposed algorithm can be further extended for the Iris Spoof detection.

REFERENCES

1. S.Padmappriya, K. Sumalarha, “Digital Image Processing Real Time Applications,” Int. Jour. of Engg. Sci. Invention, 2018, pp.46-51.
2. S. Saha, S.Basu, M. Nasipuri, “A Comprehensive Survey on Diff. Tech. and App. of Digital Image Processing,” in Proc. Of Int. Conf. on computing, comm. and manufng., 2014.
3. Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, “A Face Anti-spoofing Database with Diverse Attacks,” in Proc. ICB, Mar./Apr. 2012, pp. 26–31.
4. P. G.Sarpate,Ramesh R.Manza, “Face Recog. using Hog and Diff. classification tech.,” Int. Journal for Research Engg. App. Mang., Jan 2019.
5. B. Khemani, Archana Patankar, “Face Recognition to Handle facial Expression, Occlusion, and Posture Variation,” Int. Jour. of Ad. Research, Ideas and Innov. in Tech., 2017, vol 3.
6. Thazheena T, Aswathy Devi T, “Face Recog. under Occlusion by Facial Accessories: A Review,” Int. Journal of Advance Research in Electronics and Communication Engineering, vol 7, jan 2018.
7. T. Dhawanpatil, B. Joglekar, “Face spoof detet. using Multiscale Local Binary Pattern Approach,” IEEE, 2017.
8. W. Haider, H. Bashir, A. Sharif, I. Sharif and Abdul Wahab,” A Survay on Face Detection and Recognition Approaches”, Int. Science congress Association, April 2014.Volume 3(4).
9. L. Sun, G. Pan, Z. Wu, and S. Lao, “Blinking-Based Live Face Det. using Cond. Random Fields,” in Proc. AIB, 2007, pp. 252–260.
10. W. Bao, H. Li, N. Li, and W. Jiang, “for Face Recog. Based on Live. Detect. Method on Optical Flow Field,” in Proc. IASP, Apr. 2009, pp. 233–236.
11. M. Vatsa, and R. Singh, S. Bharadwaj, T. I. Dhamecha, “Comput. Eff. Face Spoofing det. with Motion Mag.,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2013, pp. 105–110.
12. T. Tan, and A. K. Jain, J. Li, Y. Wang, “Live Face Det. Based on the Analysis of Fourier Spectra,” Proc. SPIE, vol. 5404, pp. 296–303, Aug. 2004.
13. I. Ching., A.Anjos and S. Mar., “On the Effect. of Local Binary pat. in Face Anti-spoof.,” in Proc. IEEE BIOSIG, 2012, pp.1–7.
14. K. Koll., H. Front., M. I. Faraj, and J. Bigun, “Real-Time Face Detect. and Motion Anal. with App. in „liveness“ Assessment,” IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, Sep. 2007.
15. J. Yang, Z. Lei, S. Liao, and S. Z. Li, “Comp. Depent. Descriptor Face live. Detect. with,” in Proc. IJCB, Jun. 2013, pp. 1–6.
16. P.Raval, r.R Sedamkar, Sujata Kulkarni, “Face spoof Detet. using Image Distort. Features,” Int. Journal of Innovt. Rech. in Sci. , Engg and Tech., vol 6, sep. 2017.
17. S. Tirunagari, N. Poh, D. Wind., A. Ior., Nik S, and Anthony T.S. Ho., “Det. of Face Spoofing Using Visual Dynamics”, 2014, IEEE Trans. On Info. Forensics and Security.
18. Saptarshi Chakraborty and Dhrubajyoti Das, “An Overview of Face Liveness Detection”, 2014, Int. Journal on Info. Theory (IJIT), vol.3, no.2
19. T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, “Face Live. Detect. using 3D Struct. Recovered from a Single Camera,” in Proc. ICB, Jun. 2013, pp. 1–6.
20. Di Wen, Hu Han, and Anil K. Jain,” Face Spoof Detect. with Image Distortion Analysis”, IEEE Trans. on Info. Forensics and Security, Vol. 4, No. 3, 2015, pp. 90-102.
21. Y. Akbulut, A. Sengur, Ü. Budak, S. Ekici, “Deep Learng. Based Face Live. Detect. in Videos”, 2017, IEEE.
22. M. Killioglu, M. Taskiran, N. Kahraman, “Anti-Spoof. In Face Recog. with Liveness Detect. Using Pupil Track. ”, SAMI 2017, IEEE 15th Int. Symposium on Applied Machine Intel. and Inf.
23. K. Patel, Hu Han, and Anil K. Jain, “Spoof Detect. on Smartphones Secure Face Unlock:”, 2016, IEEE Trans. On Info. Forencs and Security.
24. Aziz A., A. Mahmood, “Enhancing Comp. Vision to Detect Face Spoof. Att. Utiil. a Single Frame from a Replay Video Attack Using Deep Learng.”, 2016 Int. Conference on Opto. and Image Processing.
25. S. Rahimzadeh, Arashloo, J. Kittler, and W. Christmas, “An Anomaly Detect. App. to Face Spoof. Detect: A New Formulation and Eval. Protocol”, 2017 IEEE.
26. Priyanka Sharma, Ms. Neha Chauhan, “Face Spoof Detection Technique to Differentiate Spoofed and Non Spoofed Faces: A Review”, June 2019, Journal of Emerging Technology and Innovative Research (JETIR).

AUTHORS PROFILE

Priyanka Sharma received the diploma in computer science engineering from LR Poly technique Solan in 2014, Himachal Pradesh Takniki Shiksha board, hamirpur, Himachal Pradesh, India. Btech degree in Computer Science Engineering from the university Institute of Information Technology, Himachal Pradesh, India in 2017, she is currently pursuing MTech. Degree in computer science engineering from AP Goyal Shimla University, Shimla, Himachal Pradesh, India, she had published 1 paper earlier. Her Study and research interest include image processing, in particular face recognition and face detection.

Neha Chauhan is currently an Assistant Professor in department of computer science engineering at AP Goyal Shimla University, received the Btech and Mtech Degree in Computer Science Engineering from AP Goyal Shimla university, Shimla , Himachal Pradesh, India, she had published 5 papers earlier , Her research interest area is data mining , particulars in web Mining, predictive analysis, Clustring.