International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 7 Issue: 8 19 - 22

Face Liveness Detection using Feature Fusion Using Block Truncation Code Technique

Prasad A. Jagdale
Dept. of Compute Engineering,
Pimpri Chinchwad College of Engineering,
Savitribai Phule Pune University, India

Sudeep D. Thepade
Dept. of Compute Engineering,
Pimpri Chinchwad College of Engineering
Savitribai Phule Pune University, India

Abstract - Nowadays the system which holds private and confidential data are being protected using biometric password such as finger recognition, voice recognition, eyries and face recognition. Face recognition match the current user face with faces present in the database of that security system and it has one major drawback that it never works better if it doesn't have liveness detection. These face recognition system can be spoofed using various traits. Spoofing is accessing a system software or data by harming the biometric recognition security system. These biometric systems can be easily attacked by spoofs like peoples face images, masks and videos which are easily available from social media. The proposed work mainly focused on detecting the spoofing attack by training the system. Spoofing methods like photo, mask or video image can be easily identified by this method. This paper proposed a fusion technique where different features of an image are combining together so that it can give best accuracy in terms of distinguish between spoof and live face. Also a comparative study is done of machine learning classifiers to find out which classifiers gives best accuracy.

Keywords: *Face Recognition, Face Liveness Detection, Face Password, Face Detection, BTC*

*****

I. INTRODUCTION

Nowadays the personal stuffs are very precious and this data could be anything such as bank details, important cards, password, jewellery, important documents etc. Everyone try their own ways to protect their belongings from outer world to avoid the exploitation of it. To avoid misuse there are different systems available to protect such valuable things such as lockers, safety box protect by security systems. The best way to secure is by doing the use of biometric systems, biometric systems such as voice recognition, finger print recognition, eye iris recognition or face recognition.The biometric systems works only with the person who has complete authority. Problem arises when these systems can be easily get bypassed by tricking the secure system. Spoofing attack is one the trick technique to bypass the system. Spoofing attack is nothing but creating a similar looking structure which will help to bypass the system. Spoofing can be done using spoof finger, voice or face.In biometric face recognition (FR) is widely used for securitypurposes as compared to other systems like fingerprint, voice oriris. Face recognition can be done using digital image processing or video. These digital image or video protection can be easily hacked i.e. spoofing attack can occur. Spoofing of such system can be done byimages, masks (Similar looking dummy face) or video played on media player devices. Images or video of person can be easily available from social media or can beeasily captured from some distance using some long focal length cameras. Face recognition systems will not give full assurance of protect data/software if they don't support face liveness detection functionality [1], Liveness detection is a process where system verifies that face which being captured from camera is from a real live person present at the moment or it is from some other virtual image is being captured.

To extract the feature for liveness detection of face image OTSU segmentation has been applied for the feature extraction with Multi Layer Perceptron (MLP) network BTC and TSBTC plays very significant role and these feature helps to distinguish between gender classification [2]. There are some existing Face recognition systems that can be easily tricked by spoofing attacks with virtualfaces. A lot of researchers focus on dealing with anti-spoofing of photosor videos. Existing face liveness methods often use single image feature toaddress face spoofing problems, which are not reliable and robust. [3]Face recognition system follows the basic procedure as follows, 1. Capture the image 2. Detect the face from the captured image 3. Compare detected face with all the faces present in the dataset.The dataset contains different features extracted from different faces which help to identify the input face. If this procedure is used in biometric face recognition security software then such systems will be poorly secured which can be easily spoofed

To avoid spoofing attack on such biometric system a new model is introduce named face liveness detection. In this

proposed method the face liveness detection method is implemented based onface feature extraction and accuracy is increased further by using fusion ofdifferent features all together.

II. LITERATURE SURVEY

In[1], Biometric system is widely used to recognize the authorized person based on either behavioural characteristics or physical. But this canbe spoofed using various traits. Spoofing attack is nothing but attacking or harming biometric recognition system using security features touse system without permission of authorized user.In liveness detection, anti-spoof depends on feature used like eye blinking, lip moment and various facial expressions the light reflection face,background still and the object is moving (LBP).Depend on methods used to avoid spoofing, liveness detection methodsclassified mainly as motion based, frequency based or quality based.

In[2], The focus is on face gender recognition with OTSU image segmentation based feature extraction andfurther categorization of male and female subjects using Multi-Layer Perceptron technique.Face gender recognition is significantly an efficientcognitive process and there is definitely a need of robust methodsfor efficient categorization of male and female subjects. This feature named TSBTC& BTC can be integrated with the method proposed in this paper.

In[3], proposed method in this paper uses 3 features which mainly focused on a typical face spoofing attack whose process is composed of capturing the face of user digitally and then displaying that image on screens or prints of that image on papers,which are recaptured. This process maybring several differences between genuine face images and fake faceimages;to identify such attacks paper proposes three kinds of featuressuch as, Hue Channel Distribution Features, Specular Reflection Ratio Features, Blurriness Features. Using all these feature and a classification modelis used which classifies the spoofing and real face.

In[4],Enhanced face local binary pattern (ELBP) ofa face map is extracted as a classification feature to identify whetherthe face map is a real face or a fake face. This paper proposed a methodwhich is usedfor solving the problem of face liveness detection and its divided into the3 categories Such as Texture analysis,Feature fusion and Motion analysis. NUAA dataset is used which is base dataset for this proposed method.

In[5], paper presents, multi resolution approach to gray-scale androtation invariant texture classification based on local binary patternsand nonparametric discrimination of sample and prototype distributions. The method is based on recognizing that certain local binary patterns,termed uniform, are fundamental properties of local image texture andtheir occurrence histogram is proven to be a very powerful texturefeature.

After studying all [1] [2]and [4] papers, it's found that when different features are extracted from face and when they are given to classifiermodel, and the results gives different accuracy. So to generalize andconsidering as a product development different techniques which givesthe higher accuracy value can be fused to give the best result.

III. PROPOSED SYSTEM

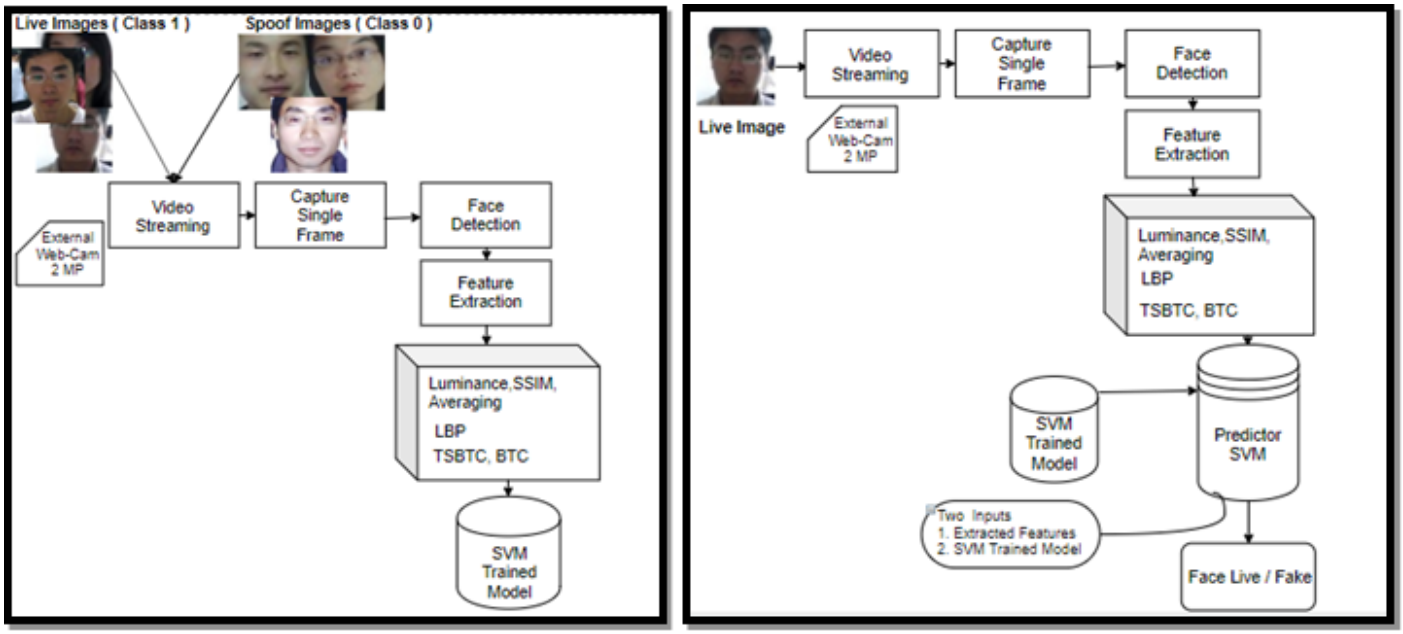

Fig. .1. Live face detection system software Design (Training SVM Model) Images Taken [13].

The proposed live face detection system software product can beintegrated with current systems which will help to stop face spoofingattack. Systems do work in three phases such asReading Data, Predict Output,Update Training Data.

PHASE 1: Reading Data

1. Start recording frames from web cam
2. Capture a single frame
3. Extract following features
   Luminance, SSIM, Energy, Entropy, MeanRBG,MeanYCbCr,LBP, BTC,TSBTC
4. Store it in Features.xlsx file
5. Repeat Step 2 till all frames don't get cover
6. Take mean of all recorded frames from saved .mat file
7. Send the mean value to classifier algorithm

PHASE 2: Predict Output(Testing Accuracy Model)

1. Read the mean values input
2. Load trained data of all features
3. Apply SVM on both Step 2 and Step 3
4. Send the Step 1 Input to SVM predictor function
5. Display the predicted accuracy of model.

IV. EXPERIMENTATION&RESULTS

Plan of Execution :

In this project features from base paper are used which helps to distinguish between real and fake face which leads to detect the face liveness.In the first stage different pairs of features tested shown in below Accuracy chart [Fig.4]. Then at end after testing all features pair are taken for fusion of features and with Block Trucation code (BTC) and (TSBTC) then at end all features are combined to gether and tested with Support Vector Machine Classifier and Fig 2 shows the database of Spoof/Fake face dataset vs Live Face Dataset.

Fig. .2. Sample images of Spoof vs Real Live Face from NUAA image dataste.[13]

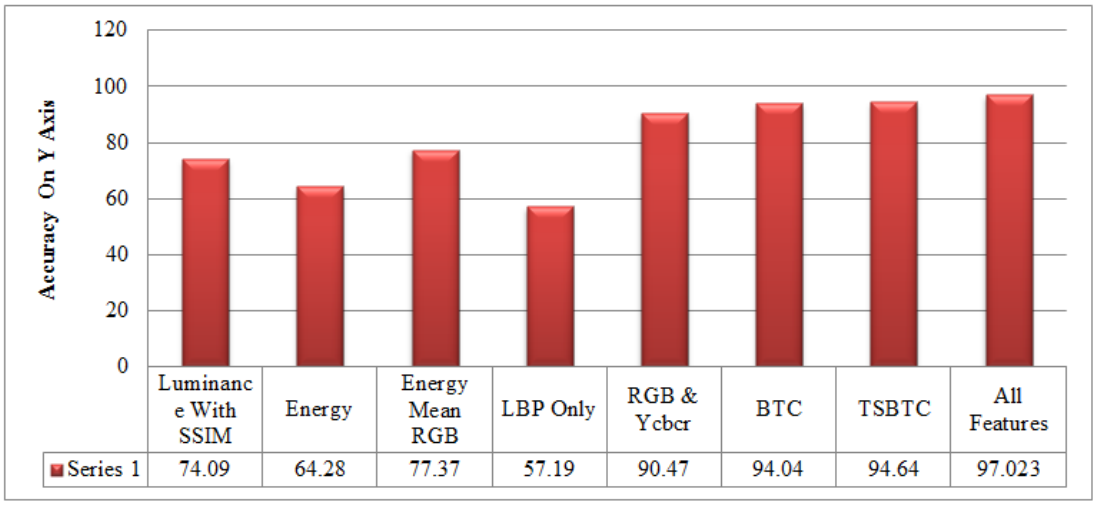

Fig. .3. Comparison OF Different Features with Fusion Features Using SVM Classifier Accuracy

This below chart in Fig. 4 shows that from Fig. 3 features who gives accuracy values high are selected then they are fused with TSBTC and BTC feature extraction which in results accuracy of proposed system has been increased by 13.38%

V. TRAINING AND TESTING

For Training 400 images are used consist of 200 Fake and 200 real faceimages, fake images consist of print outs, mobile display, tab display etc. Then to classify the fake and real face images the classification model of "Suppoert Vector Machine" is used. This SVM classifies data perfectly actoring to class parameter. To test the trained data and algorithm 40 inputsare taken and each one is passed through the algorithm, as the chartshows different accuracy generated after testing the inputs.

VI. CONCLUSION

Proposed method is simple for face liveness detection method usingillumination characteristics and image quality factors. To capture thedifference between fake and live face, features illumination and SSIMused. Other image qualities used to make system more efficient. Fromabove results it is conformed that proposed method can easily differentiate under different conditions and for various camera qualities.
Moreover this method doesn't require any other hardware other thancamera. This method efficiently works for 2D images printed on papers and videos played on media player device like mobile or tablet and able to detect the spoofing attacks.Also the results shows that when TSBTC is added in fusion technique accuracy gets increased up to 97.023% and Fig 5. Shows that SVM classifiers gives best accuracy, followed by KNN followed by J48.

For future, we will decrease the processing time and will increase theaccuracy by collaborating i.e. fusion of more best different techniques of face liveness detection.

VII. BIBLIOGRAPHY

[1] D. Garud and S. S. Agrwal, "Face liveness detection," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, 2016, pp. 789-792.
doi: 10.1109/ICACDOT.2016.7877695

[2] Thepade, Sudeep D., and DeepaAbin. "Face Gender Recognition Using Multi Layer Perceptron with OTSU Segmentation." 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). IEEE, 2018.

[3] Face Liveness Detection with Recaptured Feature Extraction 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC) 978-1-5386-3016-7/17C 2017 IEEE

[4] X. Liu, R. Lu and W. Liu, "Face liveness detection based on enhanced local binary patterns," 2017 Chinese Automation Congress (CAC), Jinan, 2017, pp. 6301-6305.
doi: 10.1109/CAC.2017.8243913

[5] Multiresolution Gray-Scale and Rotation Invariant Texture Clas-sification with Local Binary Patterns IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 24, NO. 7, JULY 2002

[6] Measures of Skewness and Kurtosis http://www.itl.nist.gov/div898/handbook/eda/section3/eda35b.htm (Last Accessed On : 12th June 2019)

[7] Local Binary pattern algorithm study http://www.scholarpedia.org/article/LocalBinaryPatterns (Last Accessed On : 12th June 2019)

[8] http://parnec.nuaa.edu.cn/xtan/NUAAImposterDB_download.html (Last Accessed On : 12th June 2019)