FACE SPOOFING DETECTION USING MACHINE LEARNING WITH COLOR FEATURES

Sahaya Asha[1], Selvin Pradeep Kumar[2]
[1]ME-AE, St.Xavier's Catholic College of Engineering
[2]AP,ECE, St.Xavier's Catholic College of Engineering
vssahayaasha@gmail.compradeep@sxcce.edu.in

ABSTRACT- The non-intrusive software based face spoofing detection schemes mainly focuses on the analysis of the luminance information of the face images. It discards the chroma component which can be very useful for discriminating fake faces from genuine ones. This project introduces a novel and appealing approach for detecting face spoofing using colour texture analysis. It exploit the joint colour-texture information from the luminance and the chrominance channels by extracting complementary low-level feature descriptions from different colour spaces. By using these features the colour texture is analyzed and extracted by face descriptors from different colour bands. In final the feature vector is fed into a binary classifier and the output score value describes whether it is a real or a fake image.

Keywords - Anti-spoofing, Texture Analysis, Preprocessing, Color model, Classification.

I. INTRODUCTION

A spoofing attack occurs when someone tries to bypass a face biometric system by presenting a fake face in front of the camera. For instance, the researchers inspected the threat of the online social networks based facial disclosure against the latest version of six commercial face authentication systems. They are Face unlock, Face lock pro, Visidon, Veriface, Luxand blink and Fast access. While on average only 39% of the images published on social networks can be successfully used for spoofing, the relatively small number of usable images was enough to fool face authentication software of 77% of the 74 users. In a live demonstration during the International Conference on Biometric described, a intruder with specific make-up succeeded in fooling a face recognition system. These two examples among many others highlight the vulnerability of face recognition systems to spoofing attacks. Assuming that there are inherent disparities between genuine faces and artificial material that can be observed in single images or a sequence of images.In the anti-spoofing techniques analysing the static and dynamic facial appearance properties.

The key idea is that an image of a fake face passes through two different camera systems and a printing system or a display device, thus it can be referred to in fact as a recaptured image. As a consequence, the observed fake face image is likely to have lower image quality compared to a genuine one captured in the same conditions due to the lack of high frequency information. Furthermore, the recaptured images may suffer from other quality issues, such as content-independent printing artifacts or video noise signatures. In the literature, the facial appearance analysis based methods are usually referred to as texture or image quality analysis based techniques because the aforementioned properties can be considered as variations in the facial texture information or image quality.

II. LITERATURE REVIEW

There are many approaches implemented in face spoofing detection to discriminating fake faces into genuine ones.

The effectiveness of anomaly detection approaches demonstrate better generalization properties and using only bonafied features from spoofing attempts[1].The local features of the input images are extracted using quaterionic local ranking binary pattern(QLRBP). These features using two different classifiers namely K-nearest neighbours(KNN) and the support vector machine[2][15]. Thecolor texture analysis analyse the joint color-texture information from the luminance and the chrominance channels using a color local binary pattern descriptor. The inter-database evalution depicts very promising generalization capabilities[4].

A specialized deep convolution neural network to extract complex and high features of the input diffused frame[5]. In patch based CNN alone larger error[6].The optical flow field approach is both feasible and effective. So illumination change will

have an impact on the results[8].The 3D CNN end to end structure is better than that of hand-crafted[9]. 3D MAD works well for print attacks, but it is not suitable for video attack and they may fail in an unseen attack[10].This method uses the difference between pairwise discrete cosine transform co-efficients and logistic regression as a machine learning algorithm[11].The additional illumination is added which raise the energy of high frequency components of a real face by exposing more details of the hair, the skin and lower it[12]. The convolution estimation method is unsuitable for this geometric attributes[13].In hybrid model the equal error rate is 12 times lower than IQA based method. It is imperfect using of hardware[14].

An efficient training strategy has been enable the use of deeper CNN structures and to enable the growth of training data in autonomous way. They not require fixed handcraft features and limited portion of video data is restricted[16].Eye area is extracted from real time camera by using Haar-cascade classifier with specially trained classifier for eye region detection. Features point have extracted and traced for minimizing persons head movements and getting stable eye region by using KLT algorithm[18]. The randon based approaches will not provide a higher classification accuracy. As the number of theta steps is lower and the computation time is increases[19]. The LSTM-CNN parameter is little greater than general CNN architecture [20].

III.PROPOSED METHODOLOGY

The proposed colour texture based face spoofing detection protocol mainly focus on the color spaces to detect spoofed faces three different colour spaces are used here, RGB, YCbCr and HSV.

RGB is commonly used colour space which is the set of red ,green and blue colours. YCbCr is the combination of luminance and chromo components such as chroma blue and chroma red. HSV represents the hue, saturation, value.

Texture descriptors originally designed for gray-scale images can be applied on colour images by combining the features extracted from differentcolor channels.

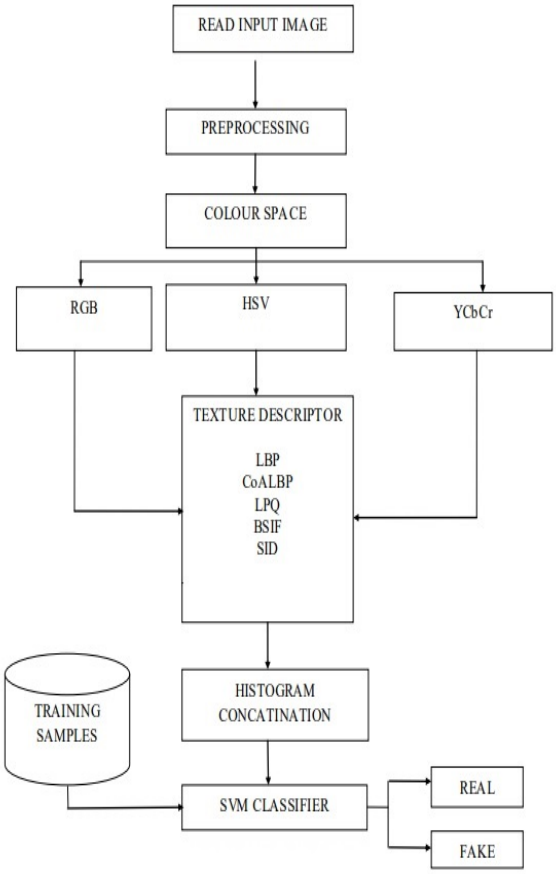

Figure1 Face Spoofing Detection Architecture

A. Preprocessing

The aim of pre-processing is an improvement of the image data that suppresses unwilling distortions or enhances some image features important for further processing, although geometric transformations of images that means rotation, scaling, and translation are also classified among pre-processing methods. In this project the input color image is converted into gray image. Using suitable cropping or face detection schemes, the image is cropped and then resized to meet the requirement. The image is then normalized to have uniform intensity or gray level. Image is then filter redusinglowpass filter.

B. Color Space

Skin detection is the process of finding skin colored pixels and regions in an image or a video. The primary key for skin recognition from an image is the skin color. But color cannot be the only deciding factor due to the variation in skin tone according to different races. Other factors such as the light

conditions also affect the results. Therefore, the skin tone is often combined with other cues like texture and edge features. This is achieved by breaking down the image into individual pixels and classifying them into skin colored and non-skin colored. One simple method is to check if each skin pixel falls into a defined color range or values in some co-ordinates of a color space. There are many skin color spaces like RGB, HSV, YCbCr, YIQ, YUV, etc. that are used for skin color segmentation. In this method used a new threshold based on the combination of RGB, HSV and YCbCr values.

C. **Texture Descriptor**

Texture descriptors originally designed for gray-scale images can be applied on colour images by combining the features extracted from different colour channels. Colour texture of the face images is analyzed using five descriptors.

I. Local Binary Pattern

The local binary pattern are used to computed the binary code by thresholding. Thus the threshold values are collected into histogram.

II. Co-accurence of Adjucent LBP

The co-accurence LBP discards spatial information to exploit the spatial relation between patterns.

III. LocalPhase Quantization

Deal with blurred image. Phase information extracted by short term fourier transform to analyse neighbourhood. Quantized and collected into histogram.

IV. Binarized Statistical Image Features

Image regions are conveniently represented by histograms of pixels binary codes.Convolving the image with linear filter and binarizing filter response.

V. Scale Invariant Descriptor

Image is first resample densely enough on a log polar grid, rotations and scalings in the original image domain. Fourier transform is applied on the resampled image, invariance to both scale and rotation is achieved.

D**. Classification**

The proposed method provides an effective way of leveraging the generalization capabilities of SVM face anti-spoofing. The data randomization like bootstrapping approach is an effective way of preventing SVM from over-fitting caused by small training data. However, in the proposed approach randomly sampled small batches from the whole training dataset. Thus, there is a chance that some of the samples having different properties from the other samples in the database. The proposed method can be attributed to dropout mechanism used for regularizing the SVM networks. Since the data is randomly sampled, some of the training data is prevented to pass through the SVM. The introduction of this new data to the SVM, the loss is increased that results in weight adjustment of the hidden layers and hence the SVM continuous without over-fitting on the training data. Further, the training time is reduced substantially by using small random batches for training SVM on small scale database. On contrary, training using the proposed technique on large scale database with small random batches with high-end GPU may result in an increase in the overall training time. While using the proposed method for large scale data, the batch-size need to be set according to the size of the training data.

IV.RESULTS AND DISCUSSION

Due to the characteristic of proposed method, it is quite hard to employ it to current popular datasets. In this project, we utilize several self-collected anti-spoofing datasets on different spoofing media to verify our proposed method. For genuine faces, all people in datasets are allowed to change their head poses freely. If some subjects wear glasses, we use their photos with glasses as attacking images. We use three methods to conduct spoofing attacks high quality color photos printed on resin coated papers, photos printed on A4 papers and photos displayed on the tablet screen. In all printed spoofing attacks, photos are allowed to be warped freely. To demonstrate the benefit of active near infrared images in our proposed algorithm, besides images using the same spoofing media. Before classifying the following steps to be which are shown in figures below.

Figure2 Original input image

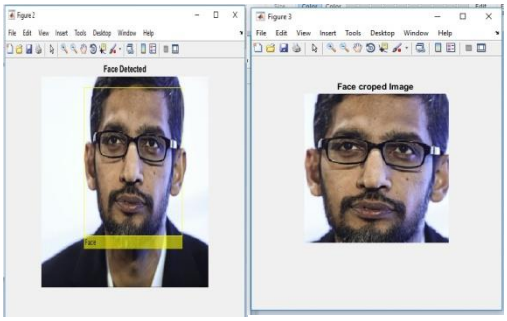

Figure3 Face detection and cropped image

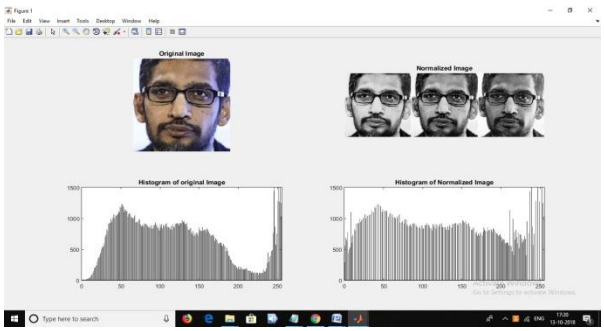

Figure4 Normalized image

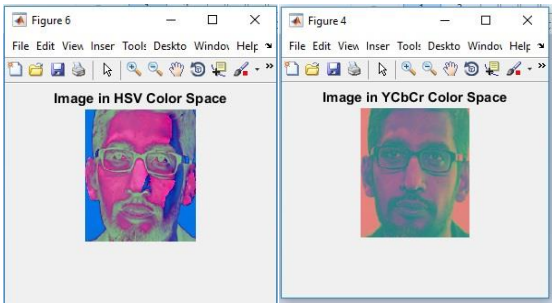

Figure 5Color space images

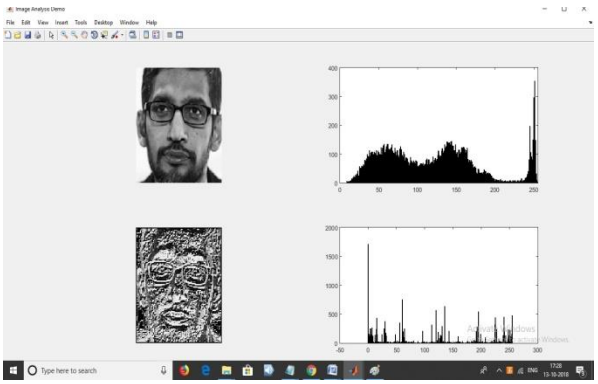

Figure6Binarized image

VI. CONCLUSION

The facial representation extracted from different color spaces using different texture descriptors. By extracting holistic face representation from luminance and chrominance images in different color spaces. In future, the T test is use for feature selection to reduce high time consumption due to high feature size. The classifier need high training sample so by applying sparse classifier it will be reduced. In future the texture descriptor histogram are concatenated into one histogram. Then the SVM classifier can be classified, thus the image is fake or real.

VII. REFERENCES

1. AbdenourHadid, JukkaKomulainen and ZinelabidineBoulkenafet (2015), 'Face anti-spoofing based on color texture analysis' in IEEE International conference on Image Processing(ICIP).
2. AladineChetouani, EmnaFourati, WaelElloumi (2017), 'Face anti-spoofing with image quality assessment' Bio-engineering for smart technologies(BIO SMART) , 2nd International conference on, pp.1-4.
3. Amin Jourabloo, YousefAtoum, Yaojie Liu (2017), 'Face anti-spoofing using patch and depth based CNNs',Biometrics (IJCB), IEEE International joint conference on, pp:319-328.
4. Amir Mohammadi, Andre Anjos, OlegsNikinsins, Sebastine Marcel (2018), 'On effectiveness of anomly detection approaches against unseen presentation attacks in face anti-spoofing' ,the 11th IAPR International conference on Biometrics(ICB).

5. Ane Cornelia, GunawanDewantoro, IwanSetyawan (2018), 'Face anti-spoofing method based on quaternionic local ranking binary pattern features', Signals and Systems(IC sigsys) International conference on, pp:92-97.
6. AusifMahmood, Aziz Alotaibi (2016), 'Enhancing computer vision to detect face spoofing attack utilizing a single frame from a replay video attack using deep learning', in Optoelectronics and Image Processing(ICOIP), International conference on IEEE, pp:1-5.
7. BalajiRaoKatika, KannanKarthik (2017), 'face anti-spoofing based on sharpness profiles' ,Industrial and Information systems(ICIIS), IEEE International conference on, pp:1-6.
8. Baowei, Hong Li, Nan Li and Wei Jiang (2009), 'A liveness detection method for face recognition based on optical flow field', In Image Analysis and Signal Processing, International conference on, pp:233-236.
9. Chengyun Liu, JunyingGan, Shanlu Li, YikuiZhai (2017), '3D convolutional neural network based on face antispoofing', Multimedia and Image Processing(ICMIP), 2nd International conference on, pp:1-5.
10. Guoying Zhao, JukkaKomulainen, Pong-Chi Yuen, Xiaobai Li (2016), 'Generalized face anti-spoofing by detecting pulse from face videos', Pattern recognition(ICPR), 23rd International conference on, pp:4244-4249.
11. Hyunho Kang (2015), 'Face anti-spoofing based on image block difference and logistic regression analysis', Consumer Electronic-Berlin(ICCE-Berlin), IEEE 5th International conference on, pp:493-495.
12. JunyanPeng, Patrick PK Chan (2014), 'Face liveness detection for combating the spoofing attack in face recognition', International conference on wavelet analysis and pattern recognition, pp:176-181.
13. Killioglu M, Taskiran M, Kahraman N (2017), 'Anti-spoofing in face recognition with liveness detection using pupil tracking', Applied Machine Intelligence and Informatics(SAMI), IEEE 15th International symposium on, 000087-000092.
14. Lai Man Po, Mengyang Liu, Yasar Abbas Ur Rehman (2017), 'Deep learning for face anti-spoofing: An end-to-end Approach', Signal Processing Algorithms, Archietectures, Arrangements and Applications(SPA), pp:195-200.
15. Lei Tian, Wenze Yin, Yue Ming (2016), 'A face anti-spoofing method based on optical flow field' Signal Processing(ICSP), IEEE 13th International conference on, pp:1333-1337.
16. Liming Chen, Yinhang Tang(2017), '3D facial geometric attributes based anti-spoofing approach against mask attacks', Automatic face and gesture recognition, 12th IEEE International conference on, pp:589-595.
17. Linghen Li, Lei Li, XiaoyiFeng, Xiaoyue Jiang, Zhaoqiang Xia (2017), 'Face anti-spoofing via Hybrid convolutional neural network', the Frontiers and Advances in Data Science(FADS), International conference on, pp:120-124.
18. Muhammad Asim, Muhammad YaqoobJaved, Zhu Ming (2017), 'CNN based spatio-temporal feature extraction for face anti-spoofing', Image Vision and Computing(ICIVC), 2nd International conference on, pp:234-238.
19. RazvanD.Albu (2015), 'Face anti-spoofing based on randon transform', 13th International conference on Engineering of Modern Electric Systems(EMES), pp:1-4.
20. Shan Li, Weihong Deng, ZhenqiXu (2015), 'Learning temporal features using LSTM-CNN architecture for face anti-spoofing', in pattern recognition(ACPR), 3rd IAPR Asian conference on, pp:141-145.