IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Face Spoof Detection Using Color Texture Analysis

S.RAMAKOTESWARARAO[1] ,K.Ramya[2], V.Himatrisha[3], V.Sai Harshitha[4]

[1]*Assistant Professor, Department of Electronics and Communication Engineering,*

[1,2,3]*UG Students, Department of Electronics and Communication Engineering,*

DVR & Dr. HS MIC College of Technology, India

Abstract

In modern technology, face recognition system has received great attention. Several desktop, web and mobile applications make use of face recognition for security purpose. A major point of concern is the ability of the face recognition system to prevent an authorised person from having access to the application. Face spoofing through pictures and videos often threatens the system module of a face recognition system by disguising as a real image. A detection technique for face spoofing attack must be such which could be relied on against different mode of attacks. A novel approach to detect spoofed images needs to be developed to reduce and eradicate the effects of spoofing. Several researchers have proposed detection techniques. Some of these past attempts have been reviewed in this paper. I propose in this study, an ensemble machine learning approach for detecting face spoofing. Random forest algorithm an ensemble learning and neural network were used for face spoofing detection. Neural network gave a better classification result.

Keywords: *Random Forest, Ensemble learning, Neural networks*

I INTRODUCTION

One of the emerging technologies is Biometrics. This is a means of access control through identity validation either via thumbprint, iris and facial recognition. This technology has gained more popularity and acceptability in Information technology security, medicine, finance, criminal detection and investigation. In facial recognition, one of the major threats is facial spoofing. Facial spoofing refers to a process where a user's image is deceptively used to gain biometric access. Hackers frequently use a phony face in front of the camera to get around a facial biometric system. The majority of facial recognition technologies are vulnerable to spoofing.

Face spoofing has overtime discouraged the acceptability of facial biometrics. New facial spoofing techniques spring up every time even as anti-spoofing techniques are been discovered. It is of great value to the research world as different people have lost valuable information as a result of spoofing activities.

A novel approach to answer the above questions is proposed. This proposed methodology makes use of the Random Forest and neural network for detecting facial spoofing.

The information technology improves daily with different online applications being created. Biometrics technology is one of the most adopted approaches for login validation. This proposed approach is tested with a dataset of face spoofing activities.

The machine learning model suggested in this literature was applied to the dataset of face spoofing records. I acknowledge that the dataset used is a secondary data. It is also assumed that at the time of downloading the dataset and compiling the report the values are believed to be real and correct.

II LITRETURE SURVY

Face spoofing attack is a topic of common interest in Cybersecurity because it is a threat to biometric technology. The state of art relating to spoofing detection and prevention will be reviewed. suggested a compact learning model for detecting facial spoofing. The authors proposed a double channel neural architecture for the exploitation of both deep and wide features in the detection of face spoofing. Convolutional Neural Network was adopted as the deep

Learning Architecures was proposed for Face Liveness Detection. They used two approaches. The first approach was a nonlinear anisotropic diffusion which relied on a splitting scheme called additive operator. This was used for preserving the boundary locations of the image by enhancing the edges and surface texture. The second

approach was the application of a specialized convolutional neural network to identify the complex features needed for the face classification. They tested this model using Replay-Mobile and Replay-Attack dataset. The best classification result gotten was 96.03%. used Relativity Representation on Rieannian Manifold for detecting face spoofing. To improve spoofing detection, they made use of an SVM which is sensitive to attack inEuclidean space.

III PROPOSED METHODOLOGY

Methodology refers to the pattern of methods applied in a specific are of research or study. In the previous sections, the background of face spoofing prevention was discussed. Previous literatures on preventive and detective measures were also reviewed. In this section, the methodological approach adopted in this research will be explained.

Data processing

Sourcing for a reliable dataset is vital in machine learning. The quality of data used for learning and testing contributes a lot to the reliability of the result. Several open-source websites were browsed for face spoofing datasets. The adopted website for data gathering was Kaggle. Kaggle is an open-source data repository with datasets freely available for data analysis. The dataset used was then preprocessed.

After the source of data for machine learning has been decided, the nxt step is the preprocessing steps to follow. The data for this research was downloaded from Kaggle.

Python programming language was adopted for this research. There are predefined libraies inpython used for data preprocesing. The python libraries used are:

-Numpy**:** Numpy is used for performing scientific calculcations, large multidimensionalarrays and matrices.

-Pandas: Pandas is used for manipulating and analyzing data. To import the dataset into the program, pandas is needed.

-Matplotlib: To create visual representation of data in 2D, the matplotlib library was used.

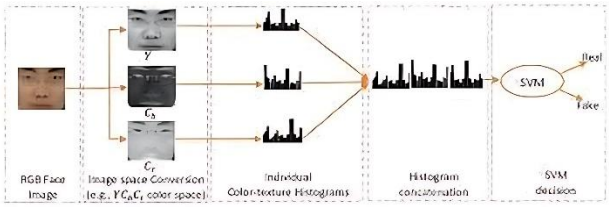
The next step is to indentify missing values and delete them. Data splitting is also done todivide the data into training and testing.

Training and Testing data

Training data refers to the dataset used to train a machine learning algorithm so as to produce the proposed outcome. Training data helps the program to have a clear understanding on how the technology will be applied.

Neural Network

Neural network is a deep learning algorithm that seeks to recognize relationship that exist in adatset by mimicking the pattern in which the human brain works. This is done by creating neurons which serve as channels for moving information from input state to an output.



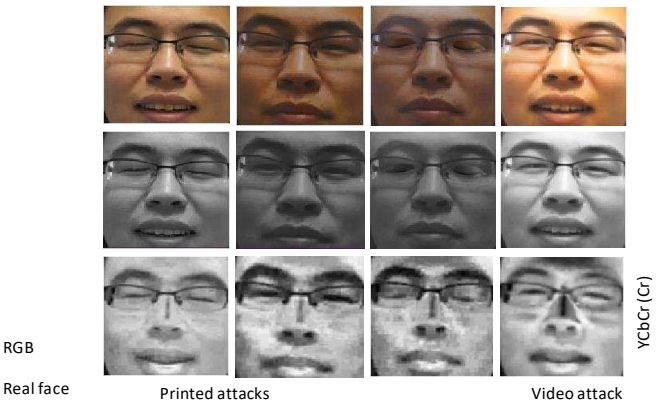
The most crude attack attempts performed, e.g. using small mobile phone displays or prints with strong artifacts, can be detected by analysing the texture and the quality of the captured grayscale face images.

The features used are the texture and quality based features. Texture based descriptors are HOG that deal with shape information, mLBP, deals with local information and Gabour Wavelet to enhance the texture Representation . The quality method extracting image quality features to find the difference between real and fake faces.

Distortion features can capture the quality differences between the different reflection properties of different materials. Quality features are color distortion, colour diversity, specular reflection and blurriness

Face spoofing attacks are most likely performed by display-ing the targeted faces using prints, video displays or masks to the input sensor. The most crude attack attempts performed,
e.g. using small mobile phone displays or prints with strong artifacts, can be detected by analysing the texture and the quality of the captured gray-scale face images. However, as shown in Figure 3, it is reasonable to assume that fake faces of higher quality are harder or nearly impossible to detect using only luminance information of webcam-quality images. In Figure 3, this effect is demonstrated by measuring the similarity between the local binary pattern (LBP) descriptions extracted from a genuine face (Real face 1), another genuine face (Real face 2) and two fake face images (Printed Attack and Video Attack) of the same person. The similarity is measured using the Chi-square distance:

where H_x and H_y are two LBP histograms with N bins. In addition to its simplicity, the Chi-square distance is shown to be effective to measure the similarity between two LBP histograms [48]. From Figure 3, we can observe that the Chi-square distance between gray-scale LBP histograms of the genuine face and the printed fake face is smaller than the onebetween two genuine face images. Moreover, the difference in similarity between the texture descriptions of genuine faces and the Chi-square distance between the genuine face and the video attack is not significant. It is worth noting, however, that similarity measured with pure Chi-square distance does not necessarily indicate that there are no intrinsic disparities in the gray-scale texture representation that could be exploitedfor face spoofing detection.



Research on non-intrusive software-based face spoofing detection has mainly been focusing on analysing gray-scale images and hence discarding the colour information whichcan be a vital visual cue for discriminating fake faces from genuine ones. In a very recent work, Wen *et al.* [6] proposed colour quality based features that describe the chromatic degradation and the lack of colour diversity of recaptured face images. However, the actual local variations in colour texture information was not exploited for face spoofing detection.

Texture analysis of gray-scale face images can provide sufficient means to reveal the recapturing artefacts of fake faces if the image resolution (quality) is good enough to capture the fine details of the observed face. However, if we take a close look at the cropped facial images of a genuine human face and corresponding fake ones in Figure 2, it is basically impossible to explicitly name any textural differences between them because the input image resolution is not high enough.

To emulate the colour perception properties of the humanvisual system, colour mapping algorithms give a huge im-portance to the preservation of the spatially local luminancevariations at the cost of the chroma information [14]. Humaneye is indeed more sensitive to luminance than to chroma,thus fake faces still look very similar to the genuine oneswhen the same facial images are shown in colour (see, Figure2). However, if only the corresponding chroma component is considered, some characteristic differences can be alreadynoticed. While the gamut mapping and other artefacts cannot be observed clearly in the gray-scale or colour images, they are very distinctive in the chrominance channels. Thereby, colour texture analysis of the chroma images can be used for detecting these gamut mapping and other (colour) reproduction artefacts. This present work extends our preliminary colour texture based approach presented in [15] and provides an in-depthanalysis on the use of colour texture analysis for face spoofingdetection. In addition to the colour local binary patterns(CLBP) descriptor [16] used in our prior work [15], we explorethe facial colour texture content using four other descriptors:the local phase quantization (LPQ), the co-occurrence of adja-cent local binary patterns (CoALBP), the binarized statisticalimage features (BSIF) and the scale-invariant descriptor (SID)

The facial representations extracted from different colour spaces using different texture descriptors can also be concate- nated in order to benefit from their complementarity. This kindof fusion is investigated more closely in Section V-B. The proposed method can operate either on a single video frameor video sequences, thus practically real-time response can be achieved.

A. Colour Spaces

RGB is the most used colour space for sensing, represen-tating and displaying colour images. However, its application in image analysis is quite limited due to the high correlation between the three colour components (red, green and blue) and the imperfect separation of the luminance and chrominance information. On the other hand, the different colour channels can be more discriminative for detecting recapturing artefacts,
i.e. providing higher contrast for different visual cues from natural skin tones.

In this work, we considered two other colour spaces, HSV and YCbCr, to explore the colour texture information in addition to RGB. Both of these colour spaces are based on the separation of the luminance and the chrominance components.In the HSV colour space, hue and saturation dimensions definethe chrominance of the image while the value dimension corresponds to the luminance. The YCbCr space separates the RGB components into luminance (Y), chrominance blue (Cb) and chrominance red (Cr). It is worth noting that the representation of chroma components in HSV and YCbCrspaces is different, thus they can provide complementary facial color texture descriptions for spoofing detection. More detailsabout these color spaces can be found

B. Texture Descriptors

In principle, texture descriptors originally designed for gray-scale images can be applied on color images by combine- ing the features extracted from different color channels. In this present study, the color texture of the face images is analyzed using five descriptors: Local Binary Patterns (LBP), Co-occurrence of Adjacent Local Binary Patterns (CoALBP), Local Phase Quantization (LPQ), Binarized Statistical Image Features (BSIF) and Scale-Invariant Descriptor (SID) that have shown to be very promising features in prior studies related to gray-scale texture-based face anti-spoofing. Detailed descriptions of each of these features are presented in the following.

IV EXPERIMENTAL RESULTS AND ANALYSIS

In this section, we present and discuss the results obtained using the different colour texture descriptors on the different colour spaces. We begin our experiments by comparing the performances of the colour texture features and their gray- scale counterparts. Then, we will combine complementary facial colour texture representations to form the final facedescription used in our anti-spoofing method and compare its performance against the state-of-the-art algorithms. Finally, we evaluate the generalization capabilities of the proposed approach by conducting cross-database experiments.

Modules

Image acquisition

pre-processing

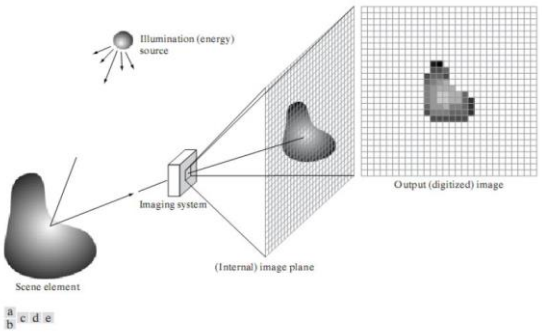
Feature extraction

Segmentation

Classification

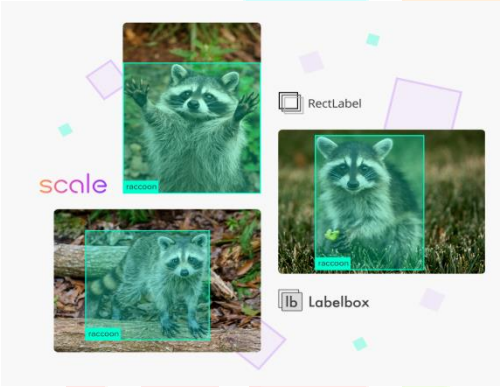
Image acquisition

Image acquisition can be defined as the act of procuring an image from sources. This can be done via hardware systems such as cameras, encoders, sensors, etc. Irrefutably, it is the most crucial step in the MV workflow because an inaccurate image will render the entire workflow useless.



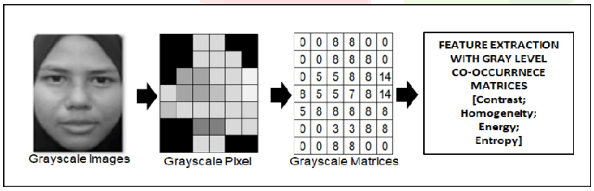
Pre-processing

The main aim of an image pre-processing is an improvement of data such as image that reduces the unwilling distortions or enhances some features, simply we can said that remove the unwanted disturbance from the image.



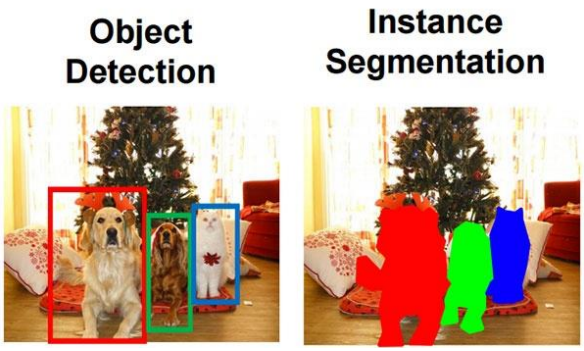
Feature extraction

It is a part of the reduction process in dimensionally in which an initial set of the raw data is divided and reduced to more manageable groups



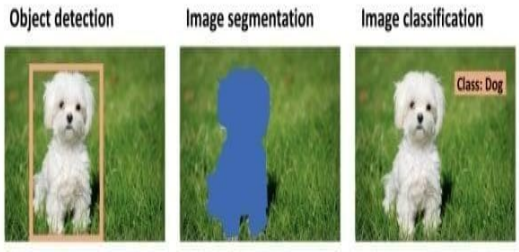
Segmentation

Image segmentation is a commonly used technique in digital image processing and analysis to partition an image into multiple parts or regions, often based on the characteristics of the pixels in the image



Classification

The task of identifying what exactly in the image. That process is going to happen by the model is trained to recognize various classes. For eg: you may trained a model to recognize the three different animals in the image.



V CONCLUSIONS AND FUTURE WORK

In this article, we proposed to approach the problem of face anti-spoofing from the colour texture analysis point of view. We investigated how well different colour image representa- tions (RGB, HSV and YCbCr) can be used for describingthe intrinsic disparities in the colour texture between genuine faces and fake ones and if they provide complementary rep- resentations. The effectiveness of the different facial colour texture representations was studied by extracting different local descriptors from the individual image channels in the different colour spaces.

Extensive experiments on the three latest and most challeng-ing spoofing databases (the CASIA FASD, the Replay-Attack

Database and MSU MFSD) showed excellent results. On the CASIA FASD and the MSU MFSD, the proposed facial colour texture representation based on the combination CoLBP and LPQ features computed over HSV and YCbCr colour spaces outperformed the state of the art, while very competitive results were achieved on the Replay-Attack Database. More importantly, the proposed approach was able to achieve stable performance across all three benchmark datasets unlike most of the methods proposed in the literature. Furthermore, in our inter-database evaluation, the facial colour texture repre- sentation showed promising generalization capabilities, thus suggesting that colour texture seems to be more stable in unknown conditions compared to its gray-scale counterparts. To be consistent with many previous studies, it is worth noting that face normalization or the limits of the face bounding box were not optimized in our experiments.However, these are shown to be important factors alreadyin intra-database tests [6], [10], [56] and

we noticed thatthey also significantly affect the cross-database performance. Improving the generalization capabilities of the colour texture analysis based face spoofing detection will be the mainobjective of our future work. Thus, we will study moreclosely how the size of the normalized face images and theused face bounding box and different face normalizationmethods affect both the intra-test and, especially, the inter-test performance. It is also of interest to investigate whether some feature descriptors or colour spaces lead to more robust and stable face representations across different acquisitionconditions and spoofing scenarios. In addition, we aim to derive use case scenario specific facial colour representations and consider person-specific training for face spoofing detection.

The financial support of the Academy of Finland, Infotech Oulu, Nokia Foundation, the Northwestern Polytechnical Uni-versity, and the Shaanxi Province is acknowledged.

REFERENCES

[1] Y. Li, K. Xu, Q. Yan, Y. Li, and R. H. Deng, "Understanding OSN-based facial disclosure against face authentication systems," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communica-tions Security*, ser. ASIA CCS '14. ACM, 2014, pp. 413–424.

[2] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in *Biometric Technology for Human Identification*, 2004, pp. 296–303.

[3] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in *Proceedings of the 11th European conference on Computer vision: Part VI*, ser. ECCV'10, 2010, pp. 504–517.

[4] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in *5th IAPR International Conference on Biometrics (ICB)*, 2012, pp. 26–31.

[5] J. Galbally and S. Marcel, "Face anti-spoofing based on general image quality assessment," in *Proc. IAPR/IEEE Int. Conf. on Pattern Recog- nition, ICPR*, 2014, pp. 1173–1178.

[6] D. Wen, H. Han, and A. Jain, "Face spoof detection with image distortion analysis," *Transactions on Information Forensics and Security*,vol. 10, no. 4, pp. 746–761, 2015.

[7] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, "Is physics-based liveness detection truly possible with a single image?" in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2010, pp. 3425–3428.

[8] J. Määttä, A. Hadid, and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," in *Proceedings of International Joint Conference on Biometrics (IJCB)*, 2011.