

# Face Spoof Detection Using Machine Learning with Colour Features

Mahitha.M.H<sup>1</sup>

<sup>1</sup>PG Scholar, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thiruvilamala, Kerala, India

\*\*\*

**Abstract** - Now a day the authentication techniques use biometric information as the credential of users. For providing more secure, use biometric information as authentication method but biometric information suffered from some attacks. Face Spoofing is one kind of biometric-based attack. In this paper propose a face spoof detection protocol which is based on colour texture analysis. This paper mainly focuses on photo and video face spoof attacks. Here use colour spaces for extracting local texture features and distortion features. Then collected all feature values for SVM training. SVM is a supervised machine learning algorithm which used here to detect genuine faces and spoofed faces.

**Key Words:** Face Spoof Detection, SVM, Texture Features, Distortion Features, Colour Space.

## 1. INTRODUCTION

Now a day's increase the cyber crimes, for providing more security we applied biometric information in authentication techniques. The biometric information such as finger print, Iris, palm print and face are commonly used credential information of user. But attackers can break the biometric based secure system by providing fake sample of biometric information of valid user. Face spoofing is one kind of that attack which occurs when a fake sample of valid users face present to the acquisition sensor. These types of attacks mainly in three types 1) video attack 2) photo attack and 3) mask attack. The video based face spoofing occurs when recorded video of valid user's face used as a fake sample to break the security. In photo attack, attacker present photo of valid user to the acquisition sensor. In mask attack, the attacker wears the mask which similar to the victims face.

Here propose a technique to detect spoofed faces based on colour features. The colour features are very helpful for discriminating fake faces from original faces. There are so many approaches are available to detect spoofed faces but that techniques mainly focus on the light intensity and avoid the chroma components. Chroma components are effective factor for discriminating the fake faces. Some existing face spoof detection techniques are introduced in this paper.

## 2. PRIOR WORK

The prior works of face spoof detection mainly focus on frequency, texture, quality and motion parameters to detect livness of face.

## 2.1 Image Quality Assessment

J. Galbally [1] proposed an approach to detect genuine face based on image quality assessment. In this method the inputted image read as a gray scale for feature extraction. The gray scale image  $I$  is filtered with a low-pass Gaussian kernel for generating the distorted version  $I'$ . Then compute quality between two images  $I$  and  $I'$  by using IQA metric. IQA metric consider the following measures: Pixel Difference measures, compute distortion between two images on the basis of their pixel wise differences. Correlation-based measures, compute the angles between the pixel vectors of the original and distorted images. Edge-based measures take Total Edge Difference (TED) and Total Corner Difference (TCD). Here simple Linear Discriminant Analysis (LDA) used as a classifier for classifying genuine and fake faces.

## 2.2 Image Distortion Analysis

D.Wen [2] proposed a face spoofing detection algorithm based on Image Distortion Analysis (IDA). IDA is the set of features such as specular reflection, blurriness, chromatic moment, and colour diversity. Here combine multiple SVM classifier output for getting final decision and the multiple SVM classifier is represented as ensemble classifier.

## 2.3 Countermeasure for Detect Face Spoofing Attack

A. Anjos [3] proposed fusion of motion and texture based countermeasures. Motion based correlation analysis is used to measure the correlations between the users head movements and the background scene. Texture quality analyzing by using local binary patterns (LBP). Here combine the motion and micro-texture analysis based techniques, the inputted video sequences divided into  $N$  frames window. Here the LBP face description is computed only for the last frame but use whole time window for motion based analysis. The fusion of these two methods is performed at score level using linear logistic regression (LLR). For classification here use linear discriminant analysis (LDA).

## 2.4 Context Based Face Spoofing Detection

J. Komulainen[4] proposed this work to detect the close up fake faces by using HOG descriptors. Here use an upper body detector for analyzing the alignment of the face and the upper half of the torso. A specific detector is used to determine the presence of the display medium. In this approach if the upper body of an face image is not found it concluded that the inputted image is fake otherwise the inputted face image give as an input to the spoofing medium

detector for finding the medium then if the medium is found then the inputted one is spoofed otherwise genuine.

### 2.5 Fourier Spectra Analysis

J. Li [5] proposed this approach for analyzing the Fourier Spectra of face image. This method mainly focuses on two principles for the detection of spoofed samples. First principle is that the high frequency components of the photo images is less than the real face images and Second principle is that the standard deviation of the frequency components in the sequence must be small[5]. If the median of the HFD is smaller than threshold value then inputted face is a spoofed sample otherwise the sample is a live face.

### 2.6 Visual Dynamics Based Face Spoofing Detection

S.Tirunagari[6] proposed an approach to identify the liveliness detection of a user by using the pipeline of DMD+LBP+SVM. Dynamic Mode Decomposition (DMD) algorithm is used to transform video sequences into corresponding image sequences. Extract features from each image sequences by using Local Binary Pattern (LBP) and LBP histogram feature values give as a input to SVM for final classification.

### 2.7 Motion Based Face Antispoofing

S.Bharadwaj [7] introduced an approach for spoofing detection in face videos using motion magnification. Eulerian motion magnification approach used here to enhance facial expression from captured video. Two types of feature extraction algorithms are implemented here: (i) LBP that provides texture based analysis and (ii) HOOF descriptor which used to extract motion based features.

### 2.8 Texture and Local Shape Analysis

J. Komulainen [8] proposed a method which adopted two powerful texture features, LBPs and Gabor wavelets, for describing not only the micro-textures but also more macroscopic information. HOG extract local shape characteristics by counting occurrences of gradient orientation in localized portions of an image. Each low-level descriptor produces its own face representation but here use homogeneous kernel map to transform the data into compact linear representation. Each vector applied to a linear SVM classifier and combine the individual SVM outputs for determines whether there is a live person or a fake image in front of the camera.

## 3. METHODOLOGY

This paper proposes colour texture based face spoofing detection. Spoofing occurs when an attacker present a fake sample to the acquisition sensor. The prior spoofing detection approaches doesn't work with colour spaces. But the proposed spoofing detection protocol mainly focus on the colour spaces to detect spoofed faces. In this approach the inputted face image converted into different colour

spaces, Table 1 shows different colour representation of an image.

Three different colour spaces are used here, RGB, YCbCr and HSV. RGB is the commonly used colour space which is the set of red, green and blue colours. These three colours are also known as primary colour. By using these three colour we can generate any colour. YCbCr is the combination of luminance and chroma components such as chroma blue (Cb) and chroma red(Cr). HSV represent the Hue, Saturation Value.

The proposed system use different feature vectors for extracting local texture information from the image and some feature extraction techniques are help to avoid specular reflection. Here use the Viola Jones algorithm for face detection. In this approach there have a chance for false detection based on the light intensity. For avoiding this problem here use specular reflection, blurriness, and chromatic moment feature vectors. Fig 1 shows the system architecture of this proposed system.

**Table -1:** Different Colour Space Representation of original, photo and video Image.

IMAGE TYPE	COLOUR SPACE		
	RGB	HSV	YCbCr
ORIGINAL			
PHOTO			
VIDEO			

### 3.1 Viola Jones Face Detection Algorithm

The main goal of this algorithm to determine whether there are any face present or not. The face detection depend some factors such as illumination, location, view point etc. This algorithm consist three ideas 1) image integration, 2) adaBoost learning 3) Cascade classifier.

Steps:

1: compute the integral image from the inputted image. The integral image also known as summed area table. The integral image pixel(x, y) is equal to the sum of the pixels above and to the left of (x, y).

2: Then extract two types of Haar-like features: the vertical feature and the horizontal feature from integral image.

3: Give feature set and a training set of positive and negative images, any number of machine learning approaches to learn a classification function. Here use AdaBoost learning function which consist a weighted sum of many weak classifiers, where each weak classifier is a threshold on a single Haarlike rectangular feature.

4: A strong classifier from AdaBoost contained stages composed into Cascade classifier. The role of each stage is to find whether a given sub-window is not a face or a face. In first stage strong classifier used to classify training samples and calculate number of false positive and false negative. The next stage will train a strong classifier using the samples which are classified as positive by the first stage. Then use the strong classifier to classify the remaining samples and calculate the number of false positive and false negative for this stage. Repeat the stages until one stage get zero false positive and false negative. All threshold value of strong classifiers from each stage are saved to form the final Cascade classifier.

### 3.2 Feature Extraction Techniques

#### 1) Local Binary Pattern (LBP)

LBP is a grayscale local texture descriptor. This feature extraction technique converts selected pixels into binary code. The following step describes how LBP work.

Steps:

- 1: the inputted image divided into cells.
- 2: select center pixels from each cell.
- 3: compare the selected pixels with neighbors of selected pixel.
- 4: Then replace the neighbor pixel with 0 if center pixel is greater than neighbor pixel or 1 if center pixel is less than neighbor pixel.
- 5: collect all replaced neighbor pixel value and convert that binary value into decimal. that represent the center pixel which selected from the cell.

#### 2) Co-occurrence of Adjacent Local Binary Patterns (CoALBP)

CoALBP is a local descriptor which helps to exploit spatial information from adjacent LBP in four different directions such as {upper left, upper right},{lower left, lower right},{left top, left bottom},{right top, right bottom}.

#### 3) Local Phase Quantization (LPQ)

This feature descriptor deal with the blurred images. It use Short Term Fourier Transform (STFT) to extract the local phase information from a targeted pixel x.

#### 4) Binarized Statistical Image Features (BSIF)

This feature extraction technique used to find binary pattern for each pixel in an image by using filter. The number of filter depend the length of the binary pattern of pixels.

#### 5) Specular reflection

This feature helps to avoid specular reflection and normalize illumination of face. Here use an iterative method to separate the components of specular reflection.

#### 6) Blurriness Features

Attackers can conceal the spoofing medium by defocusing the camera. The camera can't focus when face locate in short distance. Spoof faces have a tend to be defocused. Due to defocus there have a chance to occur blur. The blurriness calculated by taking the difference between the input image and its blurred version.

#### 7) Chromatic Moment Features

This feature extraction technique helps to detect recaptured images such as photo and video image. The human eye can detect the colour variations of fake and original samples but system fail to detect the colour variation due to the illumination and variations of camera. For avoiding this problem chromatic moment features used here.

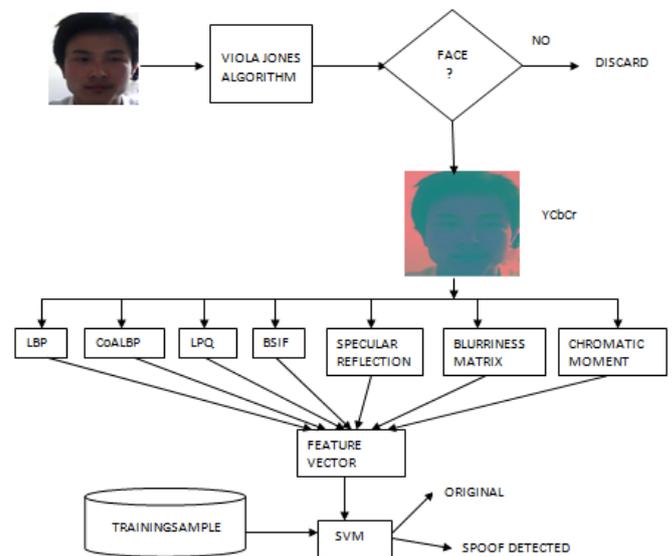


Fig -1: System architecture

### 3.3 Classification Algorithm

Support vector machine used for classification which help to detect spoofed faces and original faces. SVM is a supervised machine learning algorithm. The two main goal of SVM is, to maximize the distance between decision boundaries and classify all input variables correctly. Extracted feature values and types of input sample give to SVM for training. After

training the SVM generate a classification matrix which consist set of similar feature vector with types of class. When an image inputted for testing SVM compare the feature values of inputted image to the feature values of different classes. If feature vector of inputted image similar with any class of features value then SVM determine the inputted image belonging into that types of class.

**4. RESULTS AND DISCUSSION**

We evaluate different types of spoof attacks based on colour features: LBP, CoALBP, LPQ, BSIF and Distorted features such as specular moment, blurriness, chromatic moment There are so many face databases are publically available NUAA, CASIA & MSU are commonly used databases for spoof test experiment. The efficiency result on spoof attacks without using any colour spaces shown in table 2 and the efficiency result on spoof attacks using any colour spaces shown in table 3 under 13,754 training samples. In table 4 shows the efficiency result on spoof test using both colour texture and distorted features. As per the table results, from table 4 give better performance result compared to table 2 and 3.

**Table -2:** The efficiency result on the test of different types of faces without using colour space

Types of face	Correct Prediction %	Wrong prediction %
Original face	6.96	1.08
Photo face	3.4	9.42
Video face	5.6	8.3

**Table -3:** The efficiency result on the test of different types of faces using colour space

Types of face	Correct prediction %	Wrong prediction%
Original face	8.2	2.4
Photo face	5.7	3.1
Video face	4..08	6.02

**Table -4:** The efficiency result on the test of different types of faces using colour space and distorted features

Types of face	Correct prediction %	Wrong prediction%
Original face	9.01	0.02
Photo face	8.75	2.8
Video face	8.0	1.34

**5. CONCLUSION**

In this paper, proposed a solution for avoiding face spoof attackers based on colour texture analysis with distortion features. If this system use only colour texture analysis to detect spoofed faces, the attackers can break the system by defocusing the camera. For avoiding these problem here applied distorted features with colour features which give effective result in spoof detection.

**REFERENCES**

- [1] J. Galbally and S. Marcel, "Face anti-spoofing based on general image quality assessment," in Proc. IAPR/IEEE Int.Conf. on Pattern Recognition,ICPR, 2014, pp. 1173–1178.
- [2] 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.
- [3] J. Komulainen, A. Anjos, A. Hadid, S. Marcel, and M. Pietik"ainen,"Complementary countermeasures for detecting scenic face spoofing attacks," in IAPR International Conference on Biometrics, 2013.
- [4] J. Komulainen, A. Hadid, and M. Pietik"ainen, "Context based face antispoofing,"in Proc. International Conference on Biometrics: Theory, Applications and Systems (BTAS 2013), 2013.
- [5] 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.
- [6] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. S.Ho, "Detection of face spoofing using visual dynamics," IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp.M. Young, The Technical Writer’s Handbook, Mill Valley, CA: University Science, 1989.
- [7] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and S. Richa, "Computationally efficient face spoofing detection with motion magnification," in Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, Workshop on Biometrics, 2013.
- [8] J. Komulainen, A. Hadid, and M. Pietik"ainen, "Face spoofing detection from single images using texture and local shape analysis", Biometrics, IET, vol. 1, no. 1, pp. 3 10,March 2012.