© 2018 IJSRST | Volume 4 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Face Spoofing Detection Techniques using Biometrics

Kevin Josy[1], Harikrishnan. M[2]

[1]M.Tech Scholar, Department of Computer Science and Engineering, Rajagiri School of Engineering and Technology, Kakkanad, Kochi, India

[2]Assistant Professor, Department of Computer Science and Engineering, Rajagiri School of Engineering and Technology, Kakkanad, Kochi, India

ABSTRACT

The modern biometric technologies provides us better convenience and security features. Face Recognition Biometric systems are being used and deployed in applications such as surveillance, forensic investigation etc., but it is vulnerable mostly in case of face spoofing attacks. Such spoofing can be done by means of video frames, printed photo. To detect these types of attacks, the liveness of face detection is being developed, and also being deployed in face recognition biometric systems. If these methods don't exist in the face recognition biometric systems, it may give permission to a malicious person to masquerade as authentic users to the data file system. To address these problems, it's important to develop a secure biometric recognition system. The current method and approach to detect the liveness within the facial biometrics by making use of the feature extraction methods, includes Local Binary Pattern (LBP), Color Moment Features (CMF). In the proposed system combining two or three features proposed mainly, Histogram of Oriented Gradients (HOG), Spectral Information Divergence (SID), Binarized Statistical Image Features (BSIF), Weber Local Descriptor (WLD) and Local Phase Quantization (LPQ). Support Vector Machine (SVM) classifier gives the result as whether the image is spoofed or real. Done detailed survey on face spoof detection methods, feature methods and algorithms that are existing today and being used for the detection of spoof images. Based on the facts gathered, the execution with minimum and simple use of hardware makes biometric systems better secured and robust.

Keywords: Face Anti-Spoofing, Spoof Detection, LBP, CMF, SVM, SID, LPQ, BSIF, HOG and WLD.

I. INTRODUCTION

Biometric techniques uses the behavioural features or biological features for authenticating the user. The traditional authentication techniques like passwords, pin numbers etc. has lesser convenience and worst security compared with the biometric technologies. However, one of the challenging factors in biometric technique is to identify theft, which is commonly known as spoofing attacks.

The spoofing attack occurs generally when an aggressor seek to bypass the face biometric system by using a fake face image in front of an authenticating camera [7]. The attacker tries to masquerade as authorized user or someone else through data malfunction and achieving unauthorized access. Thus, the biometric system is exposed to the possibility of being harmed by many attacks, mainly print attacks, reply attack and 3D masking [1].

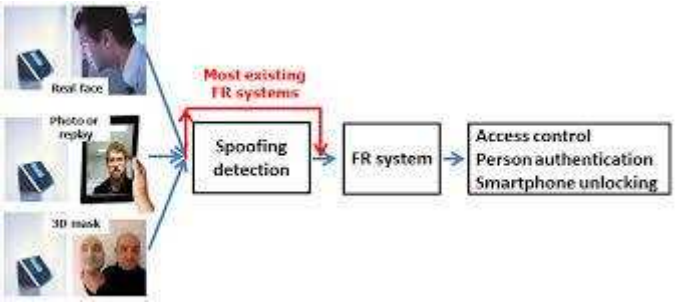

Fig. 1. FR with Spoof Detection [4].

When we compare face recognition with other biometric systems or techniques, face recognition is mostly user convenient due to its accessibility, as it doesn't require any hardware additionally, as in the case of other biometric technique. Face Recognition (FR) systems are used in areas like employee identification, banking domain etc. So, face spoof detection biometric system has to be deployed along with the face recognition system, thereby providing security by preventing the unauthorized users by detecting their identity in less response time and preventing their access to the system

Face Recognition technique is being used rapidly now a days, based on its convenience and also the user-friendly interface provided to users. In modern society, biometrics has increased in its significance. Main agenda of security systems is verifying the identity of individual [6]. Thereby, preventing the sacred resources from being accessed by impersonators. Impersonators try to gain access to the system through spoofed biometrics. So, we make use of liveness detection in order to improve biometric system performance. Liveness detection mechanism is one of the challenging issues faced, that confirms the biometric security systems truthfulness against spoof attacks [8].

The first section of this paper gives an introduction to the biometrics. The second section is regarding what all methods, features are being used in face spoof detection to determine the spoof and real images. The third section is about the proposed system architecture. The fourth section is about the experimental results obtained while carrying out the proposed methodology. The final section discusses the conclusion and future work.

II. METHODS AND FEATURES

This section describes the basic methods, feature descriptors that are used for determining whether an image is spoof or real one. The various features that are used in this spoof detection system are discussed:

A. Classifiers

1) Support Vector Machine(SVM): Support Vector Machine has high classification accuracy and is a widely used pattern classification method. Kernel based SVM uses non-linear maps to transform the data from low dimensional space to high dimensional space. Thus, any linearly non-separable data can become linearly separable. The efficiency of SVM depends on inner product between pair of observations.

Support Vector Machine is supervised machine learning algorithm, which is meant to use for classification or regression problems. Kernel trick used by this technique for transforming data, based on this, leads to determining the boundary between possible outputs. Support Vector Machine classifier is good in most challenging scenario of comparisons [2].

$$K(x, y) = \sum_{i=1}^{n} min\,(x_i, y_j) \quad (1)$$

Where, x & y are LBP histograms. n denotes dimension numbers in LBP histogram.

B. Histograms

1) Color Histogram: Color Histogram is a well-organized representation of image color content as if color pattern is unique compared with rest of data set. Color Histogram is much easier to compute and characterizes effectively both local and global color distribution in an image. It is robust to rotation and translation about view axis & changes with viewing angle, occlusion and scale.

In histogram, each component is defined based upon the number of pixels distributed for each quantized bin. More bins initiate more discrimination power. But more number of bins increases the computational cost drastically and may not be appropriate for

making indexes suited for image database. To reduce the bin numbers, use opponent color space that enables the histogram brightness to down sample. The color histogram can be generated for any sort of color space, broadly utilized for three-dimensional spaces like HSV or RGB.

For digital image, it represents pixels number having colors in each of fixed list of color image, set of possible color which span image color space. For monochromatic image, intensity histogram is used. For multi-spectral image, each pixel is represented by arbitrary measurement number. Color histogram is N-dimensional, N denotes measurement number. The color histogram can be displayed and represented as smooth function which defined over color space that approximates pixel counts. In color histogram, while computing different color pixels in an image, if color space is large, it then divides the color space into certain number of small intervals called bin. This process called color quantization. Count of the number of pixels in each of bins gives color histogram of image [10].

2) HSV Color Histogram: HSV Color Histogram separates the luminance pixel color component from chrominance. Chrominance includes saturation, hue, and value. The RGB color components are described in terms of HSV, consists of hue, saturation and value. Hue describes true color property. Saturation describes the intensity value and also measures the degree diminished by white light to pure color. Color strength can be altered through saturation. Value describes the brightness value and possess the average value of RGB color component. Color information provided by hue and saturation is explained by color circle.

It is a perfect tool for progressing image processing algorithm. HSV histogram process initiated through RGB model conversion to HSV color space and after that histogram is processed and evaluated. Results in a graphical representation of image color [10].

C. Descriptors

1) Local Binary Pattern: Local Binary Pattern is a powerful and excellent image representation which extracts the information in texture which is changed to local gray-scale variation. LBP is a powerful descriptor used to represent the local structures [9].

In the LBP operations, every pixel image is considered as threshold to its neighbor in order to get binary bit string which can be used to form round number [5]. In real applications, images are usually classified into many small non-overlapping blocks of same size, to maintain spatial relation of objects. LBP is combined with Histogram of Oriented Gradients(HOG) descriptor, which improves detection performances on image datasets[3]. LBP has lots of importance in real world applications due to its robustness to monotonic gray-scale changes and its computational simplicity makes it possible to figure out challenging real-time settings in the image [2].

$$LBP_{P,R}(x,y) = \sum_{P=0}^{P-1} s\left(f(x,y) - f\left(x_p, y_p\right)\right) 2^p \quad (2)$$

Where, variables P, R are defined as, P : no. of neighbourhood // R : radius

s(z) denotes threshold function. $s(z)= \begin{cases} 1, & z \geq 0 \\ 0, & z < 0 \end{cases}$

2) Color Moments: Color Moments are measures, which characterize the distribution of color in an image. It's mostly used for color indexing purposes as features in image retrieval applications. Single image is compared with image dataset with features pre-computed to find and retrieve similar image.

In image retrieval applications, only first three color moments are used as features and most color distribution information contained in low-order moments. Color moments can be used under lighting changing condition that encodes color and shape information, but never changes with respect to rotation and scale [10].

Color moments can be computed for any color model. Three color moments computed per channel. For example, nine moments for RGB color moments and twelve for CMYK color moment. Color moments are computed in a similar way as moments probability distribution are computed [5].

Color moments can be computed by using the following terms:

(a) Mean: The average color in image is taken as mean, the first color moments [5]. Formula is as follows,

$$E_i = \sum_{j=1}^{N} \left(\frac{1}{N} P_{ij}\right) \qquad (3)$$

Where, N denotes pixel numbers in image. P_{ij} denotes value of j^{th} pixel image at i^{th} color channel.

(b) Standard Deviation: Standard Deviation is obtained by taking the variance square root of color distribution, the second color moments [5]. Formula as follows,

$$\sigma = \sqrt{\frac{1}{N} \sum_{j=1}^{N} \left(P_{ij} - E_i\right)^2} \qquad (4)$$

Where, E_i denotes mean value or 1^{st} color moment for i^{th} color channel of image.

(c) Skewness: Skewness measures the asymmetric color distribution and gives the shape information of color distribution, the third color moments [5]. Formula used to calculate the skewness is as follows,

$$s_i = \sqrt[3]{\frac{1}{N} \sum_{j=1}^{N} \left(P_{ij} - E_i\right)^3} \qquad (5)$$

Where, E_i denotes mean value or 1^{st} color moment for i^{th} color channel of image.

(d) Kurtosis: Kurtosis taken as the fourth color moment, has resemblance to the skewness. It provides color distribution shape information and also, it's a measure of how tall or fault distribution is while compared with normal distribution [7].

(e) Higher-order Color Moments: Higher-order color moments are not used as a part of color moments set because it requires more data for good estimation of value. Lower-order color moments provides enough information which are necessary [5].

3) Spectral Information Divergence(SID): Spectral Information Divergence is mainly a spectral classification method for hyperspectral images, which make uses the divergence measure in order to match the pixels to the reference spectra. The pixels are similar for the smaller divergence. It can't classify the pixel measurement that is greater than specified threshold maximum divergence. The endmember spectra used by SID is from ASCII files. SID make uses the endmember spectra which is from special libraries or ASCII files and also it's possible to extract directly from image as ROI average spectra.

4) Local Phase Quantization(LPQ): Local Phase Quantization is an image descriptor which is useful for characterizing the underlying image texture. It is robust to centrally symmetric blur. It is insensitive to the image blur, so it is efficient in face recognition from sharp images and blurred images.

5) Histogram of Oriented Gradients(HOG): Histogram of Oriented Gradients is a feature descriptor used for detecting the object in image processing. It counts the gradient orientation occurrence in the image localized portions. HOG is somewhat similar to shape contexts, edge orientation histogram and scale invariant feature transform descriptor. HOG is computed on dense grid of uniformly spaced cells and for accuracy improvance make use of overlapping local contrast normalization. The main advantage of using HOG is that it is operated on local cells, also it's invariant to

photometric transformation and geometric transformation, but not for object orientation. Thus changes would reflect only in larger spatial regions.

6) Binarized Statistical Image Features(BSIF): Binarized Statistical Image Features is one among local image descriptors which encodes the texture information for image region representation which is suitable for histogram. BSIF computes, for each pixels the binary code by linearly projecting local image patches onto a particular subspace, where the basis vectors are from natural images via independent component analysis and binarizing coordinates via thresholding. The basis vectors determines the length of binary code string.

7) Weber Local Descriptor(WLD): Weber Local Descriptor is a simple, powerful and robust local descriptor. The patterns that percept from human not only depends on stimulus change such as light, sound but also based on original intensity of stimulus. WLD is basically derived from the Weber's Law. In Weber's Law, any change can be recognized only if the ratio of change of stimulus to original stimulus is large enough. WLD and LBP have similar advantages in the computation efficiency, because both are dense descriptors that are computed for every pixel. It depends on center pixel's intensity and also on local intensity variations. WLD performs excellent in face detection and texture classification. For texture classification, the normalized histogram metric is used for comparing the distance between histograms.

D. Filter

1) Median Filter and Averaging Filter: The Median filter and Averaging filter is used for removing the salt and pepper noise from the images. These filters set values corresponding to input values for output pixels to neighborhood average pixel values. The median filter set the output pixel values to the neighborhood pixels median which determines the output pixel value rather than by mean. The extreme values called outliers, mean is very much sensitive where median is less sensitive. So Median filter is better convenient to remove extreme values without affecting image sharpness. Median filter is also called as Rank filtering, because median filter is a specific case order statistic filtering.

2) Linear Filtering: Linear filtering is used for removing the noise in the image. It can be used to remove noises mainly Gaussian Noise Salt and Pepper Noise. There are other filters like Gaussian Filter or Averaging Filter which are suited for removal of noise. This can be explained by illustrating an example, the Averaging Filter is used for grain noise removal from the photo graph. In this filter, each pixels gets set to pixels average in neighborhood, local variations affected by grains reduced drastically. The Gaussian Filter is used mainly for reducing the noise level in images.

III. PROPOSED SYSTEM

To develop an improved live face spoof detection system to prevent face spoofing based on the feature extraction process and system being trained using image dataset, thus by preventing spoofing attacks occurrence. The main vulnerability of face authentication system is attacks based on spoofing, to address this issue with face authentication system, the only solution is that the deployment of a Secure Face Detection System, the primary step is to design and deploy it.

The work is based on detecting spoof images and real images and thus giving the access to authorized users only. Here, many features are being taken for detection of spoof images and real ones. All the features are considered by combining two or three features for the spoof detection. It's done based on Local Binary Pattern (LBP) and Color Moments

which are for face texture and image quality respectively.

The proposed method is useful for detecting the real ones and spoof ones with effective methods of approaches. Here focusing on extraction of features mainly Color Moment Feature (CMF), Local Binary Pattern (LBP), Histogram of Oriented Gradients (HOG), Spectral Information Divergence (SID), Binarized Statistical Image Features (BSID), Local Phase Quantization (LPQ) and Weber Local Descriptor (WLD). The proposed methods goal is to give a robust and simple approach for face spoof detection. Datasets are collected from various available images from different sources consisting of real ones and also spoof ones.

The Framework of Proposed Methodology is shown in the figure below

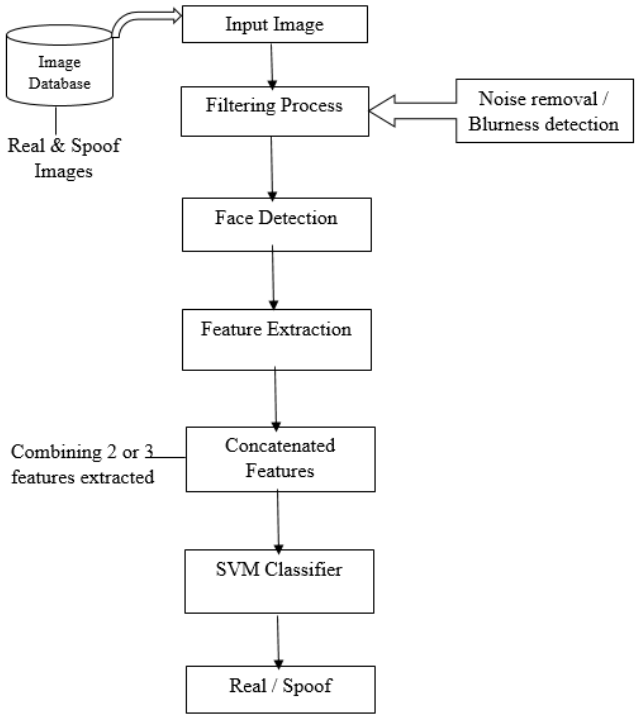

Fig. 2. Framework of Proposed Methodology.

The proposed Face Spoof Detection System's High Level System Architecture is shown below

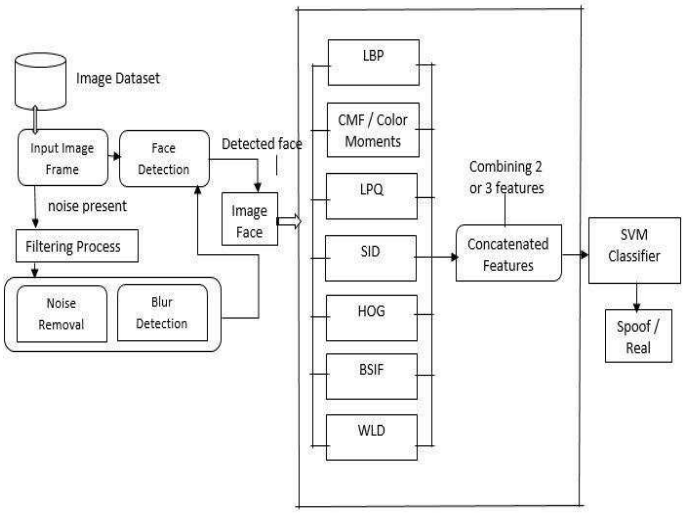

Fig. 3. High Level System Architecture.

IV. RESULT AND DISCUSSION

The proposed face spoof detection system is implemented by using MATLAB and also to verify the system accuracy and performance. The testing phase consists of gathered dataset consisting of spoof images as well as real images. This image dataset is used for the system training process and also for system testing process. For the system training, around 100 percent of dataset images are used and for testing around 75 percent are used. In this proposed face spoof detection system work, the extra features that are mentioned in the work are extracted from the images in order to specify the image as spoof or real one in much more accurate manner. Then the Support Vector Machine (SVM) is used as the classifier, in order to classify the image as spoof or real. The classifier is selected based on the comparative study and practice work done. SVM and ANN classifier are compared based on the accuracy obtained after feature extraction process. SVM provides better accuracy than ANN classifier.

A. Experimental Setup

The following setup is to implement the face spoof detection system, for performing the experiments and to record the analyzed results.

- MATLAB
- Webcam
- Desktop with 4GB

B. Result

1) System Training Process: System Training process uses the image dataset consisting of real and spoof images. For system training, around 100 percent of dataset images are used.

2) Face Detection: System Training is performed using the image dataset-consisting of real as well as spoof images and input face image detected by Viola-Jones Algorithm.

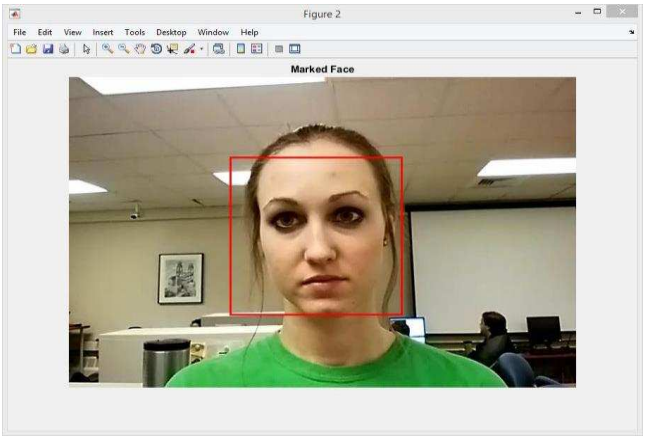

Fig. 4. User Face Detected from Input Image

3) SVM Training Process: In SVM Training process, training the system with Support Vector Machine by using linear support vector machine classifier for classifying the image as spoof or real.

4) System Testing Process: System Testing process also uses the same image dataset consisting of real as well as spoof images and required features are selected. For testing around 75 percent of dataset images are used.

Fig. 5. System Testing.

3) Image in LBP & HSV: Face detected from input image is represented, grey scale image in Local Binary Pattern (LBP) and RGB image in Hue Saturation and Value (HSV).

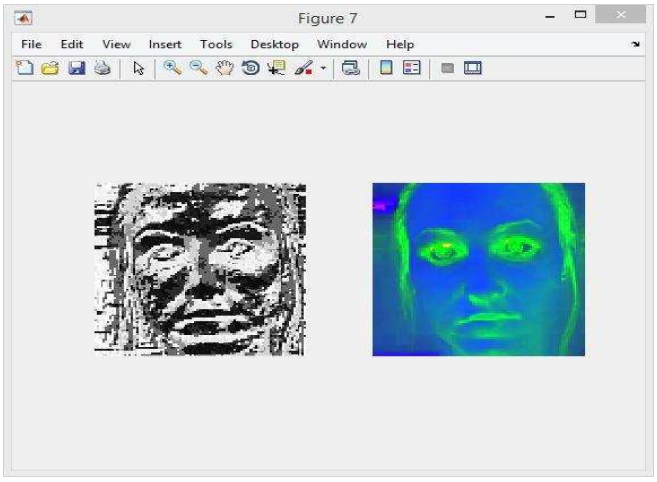

Fig. 6. Detected Face Image in LBP and HSV.

4) Feature Extraction Process: In the feature extraction process all features are extracted, the proposed features consists of Local Binary Pattern (LBP), Color Moment Features (CMF), Histogram of Oriented Gradients (HOG), Spectral Information Divergence (SID), Binarized Statistical Image Features (BSIF), Weber Local Descriptor (WLD) and Local Phase Quantization (LPQ).

For concatenated feature, combination of two or more features are selected and single feature are also taken for analysis purposes.

Here concatenated feature and individual features are selected in order to determine the accuracy of each features illustrated as proposed work. The result is been noted down and also illustrated a graph representing the accuracy of all features in the proposed face spoof detection system.

Fig. 7. Graphical representation of accuracy of all features proposed

5) Noise & Blur Detection: Noise and Blur are detected from input image by using Median Filter for noise removal and Winer Filter for blur detection.

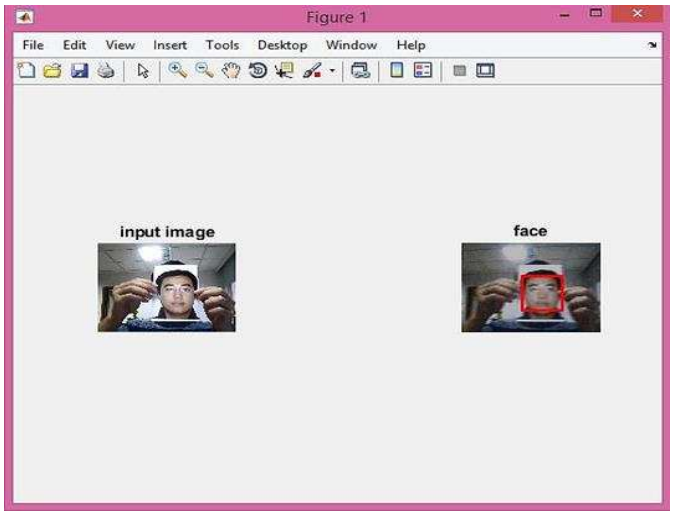

Fig. 8. Noise & Blur detection from Input Image.

The figure below shows the input image and denoised input image after noise is removed from the image through noise removal process.

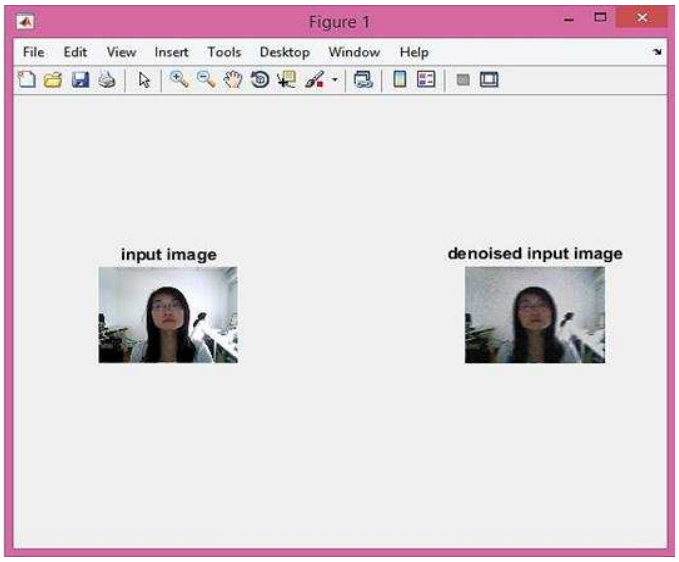

Fig. 9. Input Image and Denoised Input Image.

Graph representing the prediction accuracy for noise and blur detection from input image using Median Filter for noise removal and Winer Filter for blur detection.

Concatenated feature of LBP, CMF and HOG are selected.

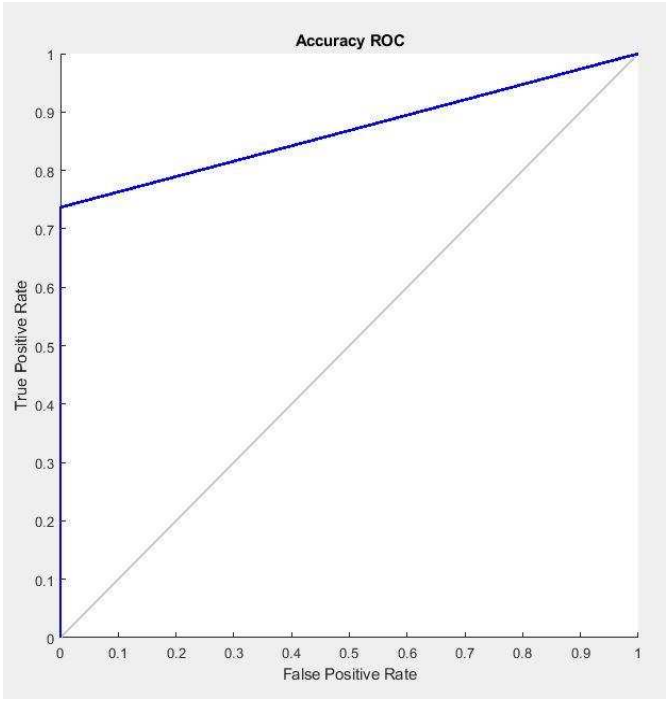

Fig. 10. Accuracy Graph

6) Live Demo: In Live Demo section in the proposed system, determines the live face of the user through the webcam, whether the input image is real or spoof one. Focusing on how efficiently system analysis the input image in live scenario.

Concatenated feature of LBP, CMF and HOG are selected.

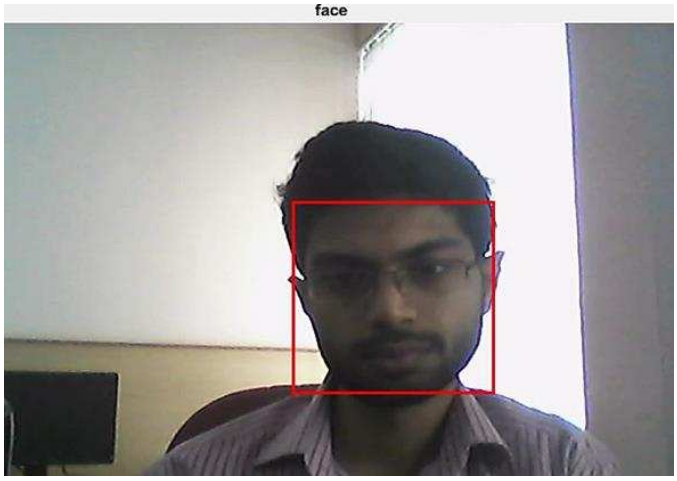

Fig. 11. Face detected in live demo

Determining the live face of the user by identifying the user face. The detected face represented in LBP and RGB and also showing the result, identified as real or spoof.

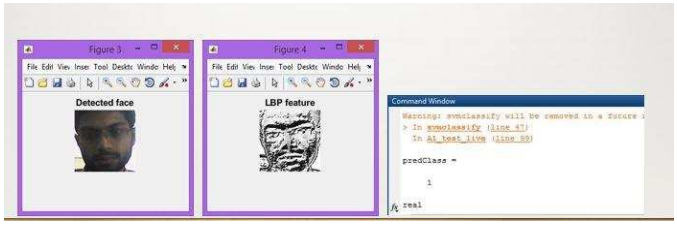

Fig. 12. Identified as real image.

7) Sample for Real Image: Determining the real image by identifying the face of the user. Concatenated feature of LBP, CMF and HOG are selected.

Figure below represents the input image and detected face of the user from input image.

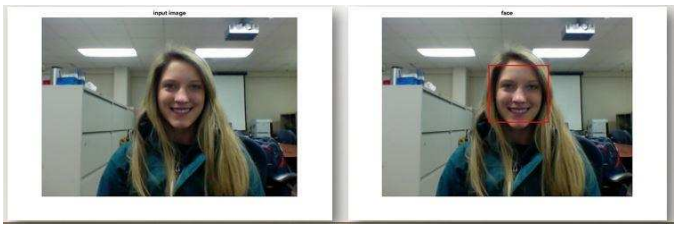

Fig. 13. Sample for real image.

Screenshot of the face detected from input image represented in RGB and LBP.

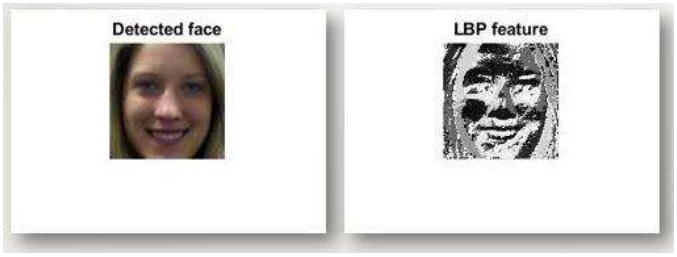

Fig. 14. Sample for real image with detected face in RGB and LBP

Screenshot of input image detected as real one and correctly predicted as real one.

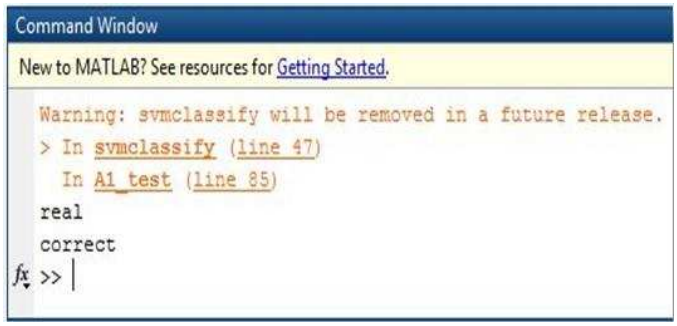

Fig. 15. Screenshot of input image detected as real one.

8) Sample for Spoof Image: Determining the real image by identifying the face of the user. Concatenated feature of LBP, CMF and HOG are selected.

Figure below represents the input image and detected face of the user from input image.

Fig. 16. Sample for spoof image.

Screenshot of face detected from input image represented in RGB and LBP.

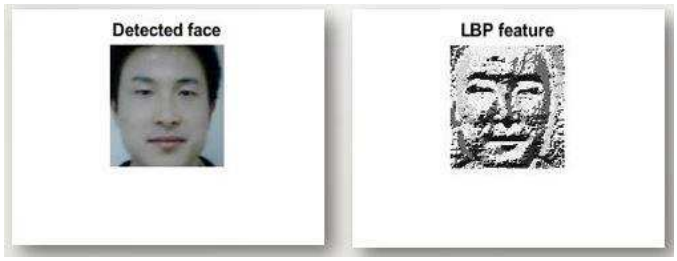

Fig. 16. Sample for spoof image with detected face in RGB and LBP

Screenshot of input image detected as spoof one and correctly predicted as spoof one.

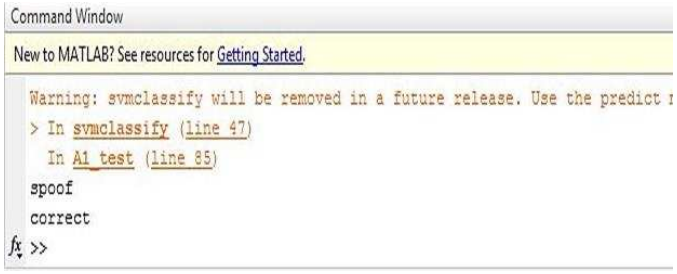

Fig. 17. Screenshot of input image detected as spoof one.

V. CONCLUSION

The face recognition systems are being used widely in many applications as a security feature. So, it needs to be secure from all vulnerabilities like spoofing attacks. Brief information regarding the methods and classifiers that are used in face spoof identification is discussed. Based on the comparison among classifiers performed and based on the facts gathered, SVM classifier is much suited to classify the image as real or spoof one. Based on the survey on different methods that are existing in-order to determine the spoof image, proposing strong mechanism for biometric system to be more robust to spoof through the variety selection and combination of different methods such as Local Binary Pattern (LBP), Color Moment Features (CMF), Reflection, Histogram of Oriented Gradients (HOG), Spectral Information Divergence (SID), Binarized Statistical Image Features (BSIF), Weber Local Descriptor (WLD), Local Phase Quantization (LPQ) etc. Classifier being used for differentiating the image as spoof or real one. Based on the comparison done SVM classifier is much better and suited, than other classifiers like ANN for determining image is real or spoof as SVM results in better accuracy than ANN.

VI. FUTURE WORK

The future work should work on proposing efficient method to capture quality images which will help to have more accurate output as well as test cases should be analysed and also working on video streams as an input to the Face Recognition System. Thus by, avoiding the misuse of user data by means of unauthorized access through spoofing.

VII. REFERENCES

[1] K. Patel, Hu Han, Anil K. Jain, “Secure Face Unlock: Spoof Detection on Smartphones.”, IEEE Trans. Inf. Forensics Security, vol. 11, no. 10, Oct 2016.

[2] D. Windridge, N. Suki, S. Tirunagari, A. Iorliam, A. Ho and N. Poh, “Detection of face spoofing using visual dynamics.”, IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 762–777, Apr. 2015.

[3] V.Ravibabu, Dr.N.Krishnan, “A Vary Approach to Face Recognition Veritable Mechanisms for Android Mobile against Spoofing.”, IEEE International Conference on Computational Intelligence and Computing Research, Dec 2014.

[4] A. K. Jain, G Ott, K. Patel and H. Han, "Live face video vs. spoof face video: Use of moir patterns to detect replay video attacks.", in Proc. ICB, pp. 98-105, May 2015.

[5] Aniati Murni Arymurthy and Retno Kusumaningrum, "Color and Texture Feature for Remote Sensing Image Retrieval System: A Comparative Study.", IJCSI International Journal of Computer Science Issues, Issue 5, vol. 8, no. 2, September 2011.

[6] H. Han, D. Crouse, A. K. Jain, D. Chandra and B. Barbello, "Continuous authentication of mobile user: Fusion of face image and Inertial measurement unit data.", in Proc. ICB, pp. 135–142, May 2015.

[7] Jukka Komulainen, Zinelabidine Boulkenafet and Abdenour Hadid, "Face anti-spoofing based on color texture analysis.", IEEE International Conference on Computational Intelligence and Computing Research, 2015.

[8] Jianwei Yang, Zhen Lei, Shengcai Liao, Stan Z.Li, "Face Liveness Detection with Component Dependent Descriptor.", IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[9] Ivana Chingovska, Andre Anjos and Sebastien Marcel, "On the Effectiveness of Local Binary Patterns in Face Anti-spoofing.", IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[10] Ruchi Kapadia, Swarndeep Saket J, "Hybrid Approach For Effective Feature Extraction Technique In Content Based Image Retrieval.", IJARIIE-ISSN(O):2395-4396, 2017.

[11] Ms. Rekha P.S and Mrs. R.Sumathi, "Spoofing Face Recognition using Neural Network with 3D Mask.", International Journal of Emerging Technology in Computer Science and Electronics (IJETCSE), ISSN: 0976-1353, vol. 14, Issue 1, April 2015.