Face Liveness Detection Using Machine Learning

Sanjay Ganorkar, Supriya Rajankar,Gaurav Rajpurohit

Abstract: To create security frameworks, numerous biometric frameworks are proposed to protect a spoof attack. Face recognition (FR) is one of the most broadly utilized innovations. One of the principle issues of utilizing FR is that the frameworks can easily get attacked by spoof faces. To avoid these attacks by spoof faces and to improve the accuracy of FR frameworks, numerous anti spoofing techniques are available. A protected system needs Liveness Detection in order to shield against such spoofing. The paper proposes liveness detection to identify the spoofing attack. The implemented system basically depends on some statistical face feature along with KNN classifier to identify fake faces. The system shows improved accuracy compared with algorithms in the literature.

Index Terms: *Face liveness, Biometric systems, Spoofing attacks, Illumination characteristic, Face spoof detection*

1 Introduction

In era of internet social media based communications for individual became fast and easy, which brings a simpler communication(interaction) with individuals, but it incorporates numerous security threats. The one of these is transferring and sharing photographs of yourself with the entire world on the web. Consistently, these photographs have higher qualities, as advanced cameras are improving. Anybody, on the web without much stretch can access or download and print photographs. Face recognition applications are increasing day by day, causing a chance of identification and stealing images in such applications. To protect from this kind of scams and spoofing, liveness detection technology have been used in this paper.

2 Literature Survey

In this section various methods from literature for detecting face liveness are proposed. In liveness detection, to avoid the spoofing attack, an antispoofing feature that depends on blinking of eyes, moment of lip, and some other facial expressions are considered. Techniques to anti spoofing in liveness detection methods grouped mostly as movement based, recurrence/frequency based or quality based.

Yang et al [1] represents the approach of features e extracted from the area of face, example, nose as well as eyes. Component based face coding is exploited for liveness detection. The implemented technique comprises of 4 stages:

(1) Detecting the segments of face;

(2) Coding in every portion of the image that are converted into low level or main feature in that image;

(3) Determining the abnormal state face portrayal by pooling the codes with weights received from Fisher rule;
(4)Linking the histograms from all segments into a classifier for identification.

The proposed structure utilizes small scale contrasts between live faces and phony appearances. Gang Pan et al.[2] proposed a security system against photo in face identification utilizing constant liveness identification eye blinking. This technique requires just a conventional camera no other additional hardware equipment to abstain from spoofing assault in nonintrusive way. Eye blinking is physical procedure that momentarily opens as well as closes covers ordinarily in a moment. Nonexclusive camera catches fifteen outlines for every seconds, it allow 2 edges of faces which utilized for hint opposed to parodying assault. Two caught outlines in succession are autonomous. The proposed framework makes good use of eye blinking method to differences between genuine faces and fake faces.

Anjos et al.[3]proposed a technique using front and background movement correlation for inspecting user liveness. The techniques exploit connection between head motion of user and its background. To discover relationship creator uses fine grained movement course. Optical stream is utilized to discover the course of movement. This methodology is simple yet requires several images for analysing liveness, so user cooperation is essential.

Maatta et al. [4]suggested the strategy based on local binary pattern [LBP], that extract feature of smallest textures which were used to avoid spoof attack. For detection of image liveness these texture features are utilised. The technique is robust in comparison with other methods in the literature.

- ***Sanjay Ganorkar is Professor in Electronics and Telecommunication*** *department, in Sinhgad College of Engineering, Vadgaon(bk) Pune 411041, India, Email: srganorkar.scoe@sinhgad.edu*
- ***Supriya Rajankar is Professor in Electronics and Telecommunication*** *department, in Sinhgad College of Engineering, Vadgaon(bk) Pune 411041, India, Email: sorajankar.scoe@sinhgad.edu*
- ***Gaurav Rajpurohit is pursuing his masters degree in Electronics and Telecommunication*** *department, in Sinhgad College of Engineering, Vadgaon(bk) Pune 411041, India, Email: gauravrajpurohit269@gmail.com*

Wang et.al.[5] proposed a system which uses single picture or group of picture by using Fourier spectra to discover the face liveness detection . Feature of live face and phony face, are unique. In this technique albedo surface ordinary are utilized to separate phony and live face. Fourier spectra give the distinctive light reflectivity which provides a lot of difference in live and phony face. For example a Fourier spectrum of phony face contains frequency components with high amplitude than live face.

3 Proposed Method

Fig.1.Shows the schematic block diagram for implemented system. This system is divided into two parts; training and testing.

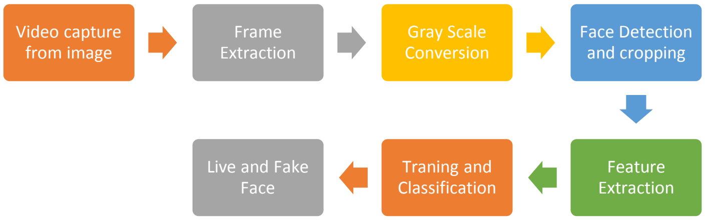

Fig.1 Overall Functional Block diagram of Proposed Face Liveness Detection Method.

3.1 Database

The images are collected from three different persons. The real images were collected directly by capturing image by camera and fake images are collected by capturing the images of printed photo. Database distribution is as tabulated in Table I.

Table I. Distribution of database

Database	**Real**	**Fake**
Total Images	253	712
Training	189	534
Testing	64	178

Input frame of user is taken from live video camera. Input image is passed through preprocessing stage for further feature extraction.

3.2 Preprocessing

In this approach, the color and statistical features are extracted. Hence we required color as well as grayscale image. The color features are extracted in HSV colorspace[6]. For statistical feature extraction, the RGB color is converted to grayscale colorspace. Mathematically, it is expressed as:

$$Gray = \ ((0.3 \ * \ \mathrm{R}) + \ (0.59 \ * \ \mathrm{G}) + \ (0.11 \ * \ \mathrm{B}) \ldots\ldots (1$$

3.3 Face Detection and ROI selection

Face detection is the process of locating the human faces in the scene. Haar cascade classifier as shown in the figure 2 is the algorithm used to detect face in the frame. Initially, the positive (face) and negative (non-face) images are used to train the model. Then features were extracted using convolutional mask.

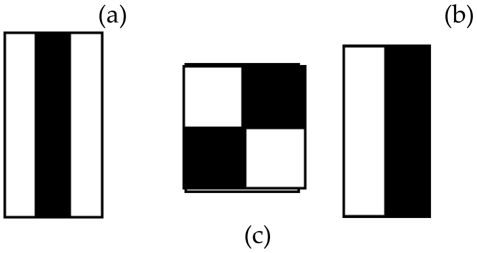

Fig. 2. Haar Feature mask used to detect face in frame.

Each feature is a single value obtained from each kernel by subtracting sum of pixels under bright pixels and pixels under black rectangle [7].

3.4. Extraction of Features

To make framework increasingly productive as well as exact more essential picture parameters are utilized in liveness discovery like Mean of Red, Green, Blue color and Mean of Grayscale, standard deviation and variances, data point count. These features vary for fake image providing different options for finalizing thresholds. The classifiers like SVM and KNN are used for identification.

A) Luminance :

It is a light density passing through a surface in a specific direction. It provides the frequency of reflected light from specific surface. The illuminated properties changes depending on the surface. The luminance determined for live face, differs from phony Because of the three dimensional impact of eyes as well as nose , luminance factor in a live face arbitrary and for phony it is almost same. Illumination can be determined utilizing Red, Green, Blue colors in the image. It is determined by utilizing the equation:

$$Luminance=: (0.299*R + 0.587*G + 0.114*B) \ldots\ldots\ldots \quad (2)$$

B) Variance :

The quantity or amount of black and white (gray) level fluctuation from the average gray level is :

$$\mu_2(Z) = \sum_{i=0}^{L-1}(z_i - m)^2 p(z_i) \ldots\ldots\ldots \quad (3)$$

C) Standard deviation :

The deviation (or) the variance between the pixels in the input image is represented by this feature.

$$S_D = \sigma_b = \left[\sum_{b=0}^{L-1}(b-\bar{b})^2 p(b)\right] \quad \ldots\ldots\ldots\ldots \quad (4)$$

D) Mean of RGB and Mean or Gray scale :

Mean of all the pixels values in the R, G and B colorspace are considered as a feature. For this first separate out the each color channel and then take a mean of each channel separately. The mean of each color is a ratio of Summation of number of pixels to the total number of pixels.

E) Data point count :

Data points are the non-zero elements in the grayscale images. Basically the fake images contain less numbers of data points than real image.

3.5 Classification

After feature extraction classification is done. In classification KNN (K -nearest neighbour) classifier is used to differentiate between live face among with fake image.

In all machine learning methods, this algorithm is easiest classifier to inferential among all of them. The efficiency of KNN is more as compare to SVM, Gradient boosting as well as stochastic gradient descent (SGD). Object in the KNN are classified by its more poll in its neighbor [8].

1. Each information pixel inside the informational collection is the class in the set, Class = {c1,..., cn}.
2. The information focuses', k-nearest neighbors (k being the quantity of neighbors) are then found by breaking down the distance matrix.
3. The k-nearest information determines the proper class among the set.
4. From the data or information, the most common class name given to analyzed data.

4 RESULT AND DISCUSSIONS

The evaluation is carried out using Qualitative and Quantitative basis.

A) Qualitative Analysis :

The training dataset image samples are as shown in Fig. 3

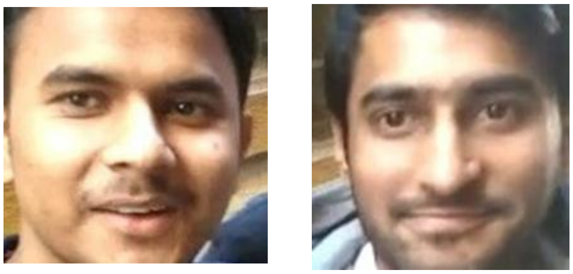

Fig.3.(a) Training data sample of real images

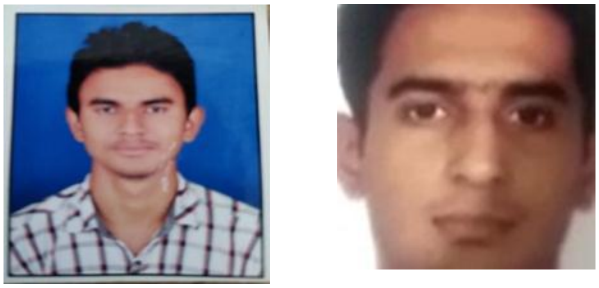

Fig.3.(b) Training data sample for Fake images

The output of the proposed system for fake and real images are as shown below fig 4.

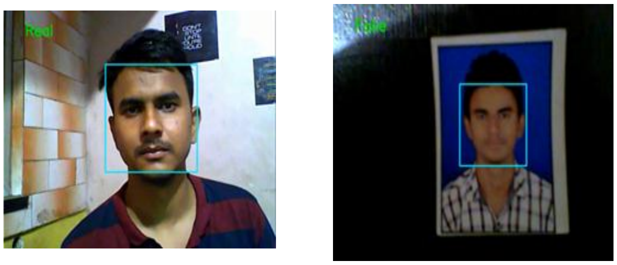

Fig. 4. Output (a) Real image (b) Fake image

B) Quantitative Analysis :

The accuracy of the proposed system has been evaluated using two algorithms, i.e. K-Nearest Neighbour algorithm, Support Vector Machine (SVM) algorithm. The performance of the classifiers are as shown in Table II.

TABLE II: Performance analysis

Algorithm	Parameters	Accuracy (%)
SVM	RBF(kernel)	77.41
KNN	K=1	97.69
	K=3	96.77
	K=5	96.31
	K=7	95.39

From TABLE II, it is observed that KNN algorithm for k=1 shows highest accuracy among two. Hence for classification of fake and real frames, KNN algorithm is used.

Performance Analysis of the implemented system is shown in Figure.5. KNN Classifier shows the highest accuracy 97.69% as compared to other classifier like SVM(kernel), SGD, Decision tree classifier and etc.

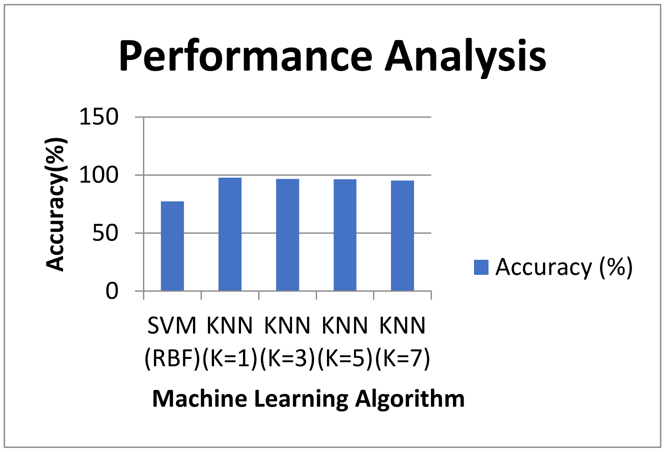

Fig.5. *Performance analysis of implemented Machine Learning Classifier.*

4.1 Prediction model

The collected data or the comparison between the live face and fake face is fed to the classification learner to visualize the data. Blue color indicates live images while red indicates face images. This toolbox is useful to analyze features as shown in figure 6.

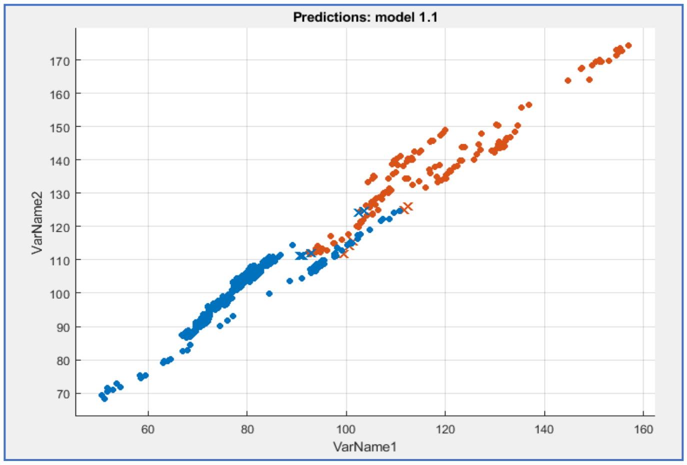

Fig.6: Prediction model of data splitting between both the images.

5 Conclusion

In most of the authentication system, face plays important role. In face recognition systems, the face features of authenticated system are extracted to developed a system. But these system may recognize the person from photos. This is a system failure. Hence to improve the face recognition system, face liveness detection plays vital role. In this method frame is extracted from input stream. After that, image is converted into gray scale, because the input to haar cascade is gray scale image. Haar cascade load into the system for detecting the frontal face. Now different features are collected from extracted face image. SVM,KNN an machine learning algorithm has been implemented. The SVM, KNN algorithm shows 77.41% and 97.69% accuracy. The proposed system is implemented using OpenCV library. In future, the deep learning algorithm can be implemented to improve the accuracy and to minimize the dependency on the feature engineering. Image should be capture on different light conditions for better accuracy. In future work can be carried out on efficient method to capture quality image which will help to have more accurate output as well as test cases should be analysed.

References

[1] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness location with part subordinate descriptor," in Proc. IEEE Int. Conf. Biometrics (ICB), Jun. 2013, pp. 1–6.

[2] G. pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink - based enemy of spoofing in face acknowledgment from a conventional web camera," in Proc. IEEE eleventh Int. Conf. Comput. Vis. (ICCV), Oct.2007, pp. 1–8.

[3] Anjos, M. M. Chakka, and S. Marcel, "Movement based counter-measures to photograph assaults in face acknowledgment," IET Biometrics, vol. 3, no. 3, pp. 147–158, Sep. 2014.

[4] J Maatta,A.Hadid, M.Pietikainen,"Face Spoofing Detection From Single images Using Micro Texture Analysis", Proc. Intn Joint Conference on Biometrics,2011, Washington, D.C., USA

[5] Wang, T. Tan, and A. K. Jain, "Live face location dependent on the investigation of Fourier spectra," Proc. SPIE, Biometric Technol. Human Identification., pp. 296–303, Aug. 2004.

[6] home.wlu.edu.lambertk/classes/101/Images.pdf.

[7] Ongoing Face Recognition Using Python And OpenCV.

[8] Vaidehi, S.Vasuhi et.al, "Individual confirmation utilizing face detection" Proceedings of the World Congress on Engineering and Computer Science, pp 222-224, 2008.