Implementing a system for Face Fraud Detection in Online Exam

Mr. Pratik Kamble [1], Dhruv Shelke[2], Harshal Netkar[3], Ashish Sonawane[4], Swaraj Naik[5], Shubham Kondhane[6]

[1](Professor, Department of Information Technology, MMCOE, Pune, Maharashtra, India)

[23456](Students, Department of Information Technology, MMCOE, Pune, Maharashtra, India)

***Abstract*— Online examination is an essential component of E-learning, that has grown exponentially day by day. Cheating in online exams is so easy all over the world regardless of the levels of development.**

This paper presents a robust face liveness detection method using a face that can be used in detecting spoof attacks for differentiation between legitimate and illegitimate users. The system uses the light reflection concept for detecting a photo face or real face while recording a video or taking an image of the examinee during an examination. The face detection is done using Haar cascade and SVM is used for face recognition. The LBP filter technique is used for detecting the light reflection of an image

Keywords—Face fraud detection, light reflection, LBP Filter technique, face liveness detection, Support Vector Machine, Haar Cascade classifier, Feature Extraction.

I. INTRODUCTION

Online activities, exams, or courses are the more feasible and safest option for everyone starting from primary students to secondary or higher because of this covid situation. But there is no guaranty of genuinity of the result in the online examination processes as there are more chances of doing malpractice and cheating throughout the examination. Because it is remotely submitted without any monitoring from physical proctors. Many universities reported widespread cheating in online examinations that were conducted. Face recognition is a widely used biometric approach [1]. Face recognition is widely viewed as an alternative means of authentication to replace traditional password methods in different applications for access control. Despite significant improvements face recognition systems are vulnerable to spoof attacks [2][3] made by non-real faces. It fails to detect the 'real face from 'photo face' which is a major security threat in the online exam. Anyone can give the exam, by putting the photo of the real examinee in front of the camera. Such, approaches are very much limited to deal with this problem.

Liveness detection has been a very active research topic, can differentiating the feature space into living and non-living. To differentiate spoof and live to face some fundamental illumination characteristics, texture factors, and other image properties are used. Light reflected from the live face is random because of the 3D structure [3] [6] of the nose, eyes of the live face. But when we use a 2D image (spoof image) light reflected from the 2D image [3][6] is uniform because the surface is plane. So according to these phenomena of reflecting light, the proposed system gives values so that we get differentiation in the fake and live face.

A. Objectives of Proposed System

The objectives of the proposed work are as follows:

- To implement the robust face liveness detection system for detection of spoof attacks.
- To differentiation between legitimate and illegitimate examinee during examination.
- To detect the photo image and real face of examinee during an examination.

II. LITERATURE SURVEY

There are different techniques used by the different researchers for cheating detection. Some of the efforts made by the researchers are as follows:

A. Face Liveness Detection Using Machine Learning [2]

Author: Leslie Ching Ow Tiong and HeeJeong Jasmine Lee

Technique used: KNN, SVM classifier

Description: The author proposes liveness detection to identify the spoofing attack. The Haar cascade is used to load the images into the system for detecting the frontal face. Now different features are collected from the extracted face image. SVM, KNN machine learning algorithm has been implemented. The SVM, KNN algorithm shows 77.41% and 97.69% accuracy.

B. E-cheating Prevention Measures: Detection of Cheating at Online Examinations Using Deep Learning Approach - A Case Study [4]

Author: Leslie Ching Ow Tiong and HeeJeong Jasmine Lee

Technique used: Deep Neural Network (DNN), Long-Short Term Memory (LSTM), Recurrent Neural Network (RNN).

Description: Leslie Ching Ow Tiong et al. [4] designed an online examination as a case study, which consisted of multiple-choice questions, in which an e-cheating intelligent agent was used to detect any potential cheating. The e-cheating intelligence agent consists of two main agents: the network IP detection agent and the behavior detection agent from which network IP is detected by using a Rule-based Expert System and behavior is detected with DenseLSTM. The LSTM network to extract better feature representation for abnormal behavior prediction. The average accuracy rate is 90%, which is quite high to alert the lecturers to review the exam result of concern.

C. E-exam Cheating Detection System[5]

Author: Razan Bawarith, Dr. Abdullah Basuhail, Dr. Anas Fattouh and Prof. Dr. Shehab Gamalel-Din

Technique used: Fingerprint Reader and Eye Tribe Tracker

Description: The author implemented an E-exam management system, which is used to detect and prevent cheating in online exams. The system used a fingerprint reader authenticator and eye tribe tracker in exam sessions, which can track the examinee status as cheating or non-cheating during the exam. Using this parameter the total time on the out screen and the number of times on the out screen were computed. The given system provides 97.78 % accuracy in detection..

D. Context based Face Anti-Spoofing, Biometrics: Theory, Applications and Systems [7]

Authors: Jukka Komulainen, Abdenour Hadid, Matti Pietikainen

Technique Used: local binary patterns (LBP) & SVM classifier

Description: Abdenour Hadid et al.[7] proposed a method local binary patterns (LBP) which is a powerful texture operator, for describing the micro-textures and their spatial information. The vectors in the feature space are then given as an input to an SVM classifier which determines whether the micro-texture patterns characterize a fake image or a live person image.

E. Face recognition with liveness detection using eye and mouth movement [8]

Authors: Avinash Kumar Singh; Piyush Joshi

Concept Used: eye and mouth movements

Description: The author proposes a robust liveness detection scheme based on the challenge and response method. The liveness module utilizes face macro features, especially eye and mouth movements for liveness detection. The system can detect five types of attacks like spoofing attacks with various means, like using the photograph, videos. An experimental test conducted on 65 persons on the University of Essex face database confirms that removal of eye and nose components results from 75% misclassification.

F. Anti-Spoofing Application for PCs with Users' Liveness Detection Using Blink Count [9]

Authors: Arpita Nema,

Description: Technique Used : LBPs, Convolutional Neural Nets (CNNs)

Authors presented face antispoofing strategies using Convolutional Neural Nets (CNNs) & and Local Binary Patterns (or LBPs). Initially, the CNN extracts the global/deep features and LBPs help to extract the local/color texture features. The classification of the spoofed face and genuine face is performed by Support Vector Machines (SVMs). These two feature extraction models generate two lists of probabilities. These probabilities are then fused to recognize non-spoofed faces from spoofed faces.

G. Face Liveness Detection Based on the Improved CNN with Context and Texture Information [10]
Authors: Chenqiang Gao ; Xindou Li ; Fengshun Zhou ; Song Mu
Technique Used: Improved Convolutional neural network (CNN
Description: The author proposes improved Convolutional neural network (CNN) architecture using two bypass connections that concurrently use low-level complete information and high-level semantic information to differentiate a fake image. Since texture information is important for describing face images, it is approved under the conventional recognition framework of the Support vector machine (SVM). The improved CNN and the texture feature-based SVM are fused.

III. PROPOSED SYSTEM

A. System Design

In face recognition systems, replay attacks where a pre-recorded video of the user is played and a printed photograph is placed in front of the camera are the two most common ways to do the fraud while attending the examination. The proposed solution helps to detect the fraud that happens in examination and maintain its integrity and genuinity of the result in the online examination. Figure 1 shows the design of the system

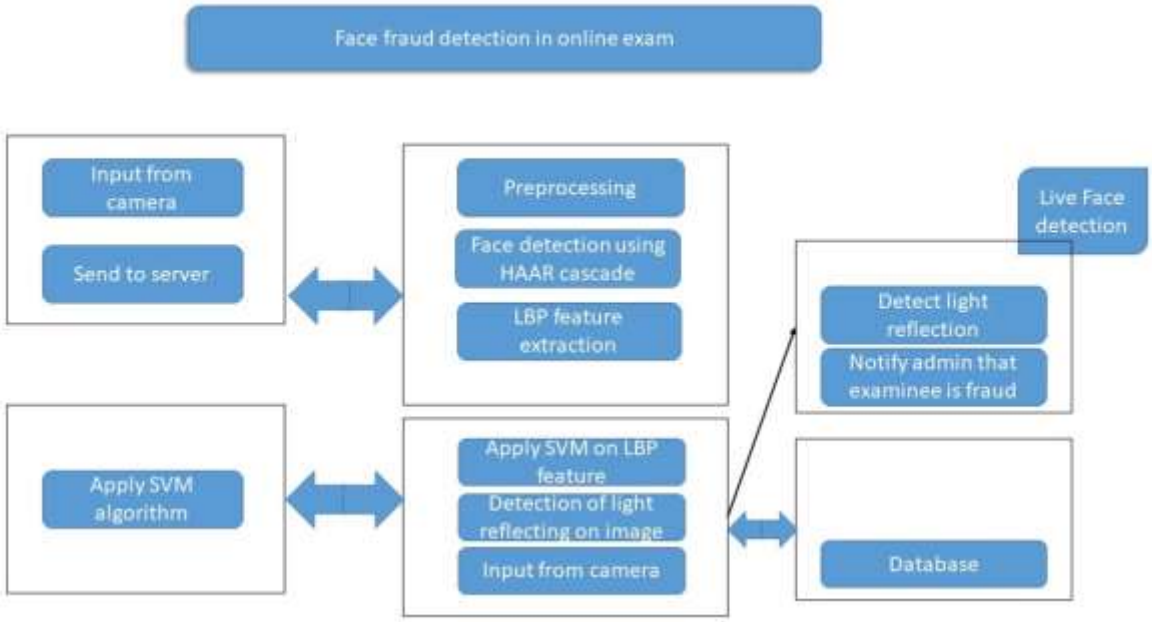


Figure 2: System Architecture

The module wise working of the proposed design is given below:

- **Image/Video from Live Camera:** The camera takes a live video and grabs images of examinees attending online examination using a camera with a specific time interval. The camera act as a sensor to collect the face biometric for processing. The frame extraction is done from the video and sends it to the application server for matching.
- **Face Detection:** The Haar cascade Classifier is used for face detection from images. The captured image is analysed to determine whether it is real or fake
- **Image Pre-Processing:** Image preprocessing techniques such as noise removal, normalization, or RGB to Gray Scale Image are applied on the detected face, to get fine tune image. The image is converted into Grayscale by taking the average of each pixel RGB.
- **LBP (Local Binary Patterns Histograms) Feature Extraction:** The Gabor filters are used for feature extraction from an image. These features like Eyes, Nose, and Mouth Location provide us the changes in the face due to light reflection on an image.
- **Feature Extraction:** Recognition of the face is done by using SVM classifier on the LBP facial features. By recognizing the face, difference between the actual face and the photograph is identified as the images that are captured from an image or videos tend to have less colour when they are recaptured. The certain colour texture is lost when an image is captured from another image. Such change is identified by the SVM algorithm.
- **Alert Notification:** The system help us to detect fraud faces using light reflection patterns on a human face using the knowledge that every object reflects light differently. It Identify Genuine/ Photograph Faces if such face detected an alert notification is send to the admin.

III. ALGORITHMS USED

A. Haar cascade Classifier

The Haar cascade classifier is used to detect face from images captured by the camera.

Step 1: This technique scans the complete image having window size (typically 24×24 pixels) and searched for Haar features for the scanned image. (Haar features are estimated using area of every rectangle, multiplying each by their respective weights, and then summing the results.)

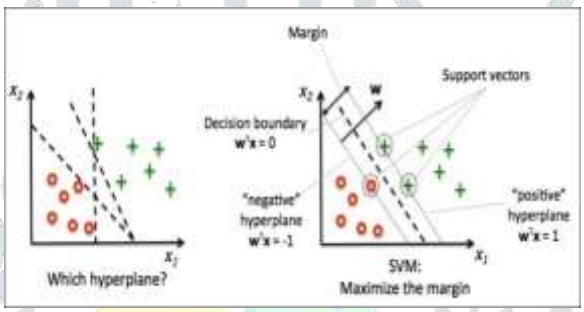
Step 2: The Haar feature classifiers produce an output that is fed to the stage comparator.

Step 3: The stage comparator adds the outputs of the Haar feature classifiers and compares them to a stage threshold to determine if the stage should be passed.

Step 4: If all of the stages are completed successfully, the face candidate is determined to be a face.

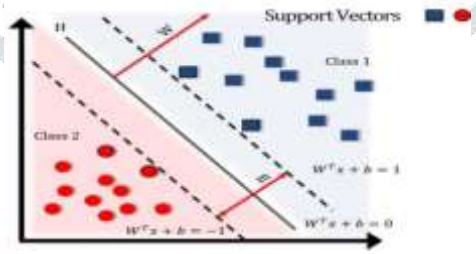
B. Support Vector Machine

- SVM is a powerful classifier that is able to distinguish two classes. SVM classifies the test image in to the class with highest distance up to the neighboring point in the training.
- SVM training algorithm built a model that predict whether the test image fall into this class or another.
- SVM necessitate a vast training data to decide a decision boundary and computing cost is very high although we are using single pose (frontal) detection.
- The SVM is a learning algorithm for classification which attempt to discover the finest distinguishing hyper plane which minimize the error for unseen patterns.



Distinguishing Hyper Plane To Minimize The Error

- The data which cannot be distinguished the input is mapped to high-dimensional attribute space where they can be separated by a hyper plane. This projection is well performed by means of kernels.



Separating Hyper Plane By Equation

- If training set of samples and the equivalent resultant values {-1, 1}. So SVM intend to get the best separating hyper plane specified by the equation W^Tx+b that make use of the distance between the two classes as shown in above figure.

V. EXPERIMENTAL DETAILS

The systems GUI was designed using tkinter library of python. Core Technologies used were Python. The database is used for storing the user's face. Faces i.e when the registered user appears in the camera system detects the real face or for an unregistered user, it is showing a fraud face.

SCREENSHOTS:

For making use of the system user needs to register to the system first. The below figure shows the details that need to be added to the system. A new student can take a student's image and save it to the database for later matching. If students are already registered to the system, the user can start the exam, meanwhile the camera captures the examinee images.

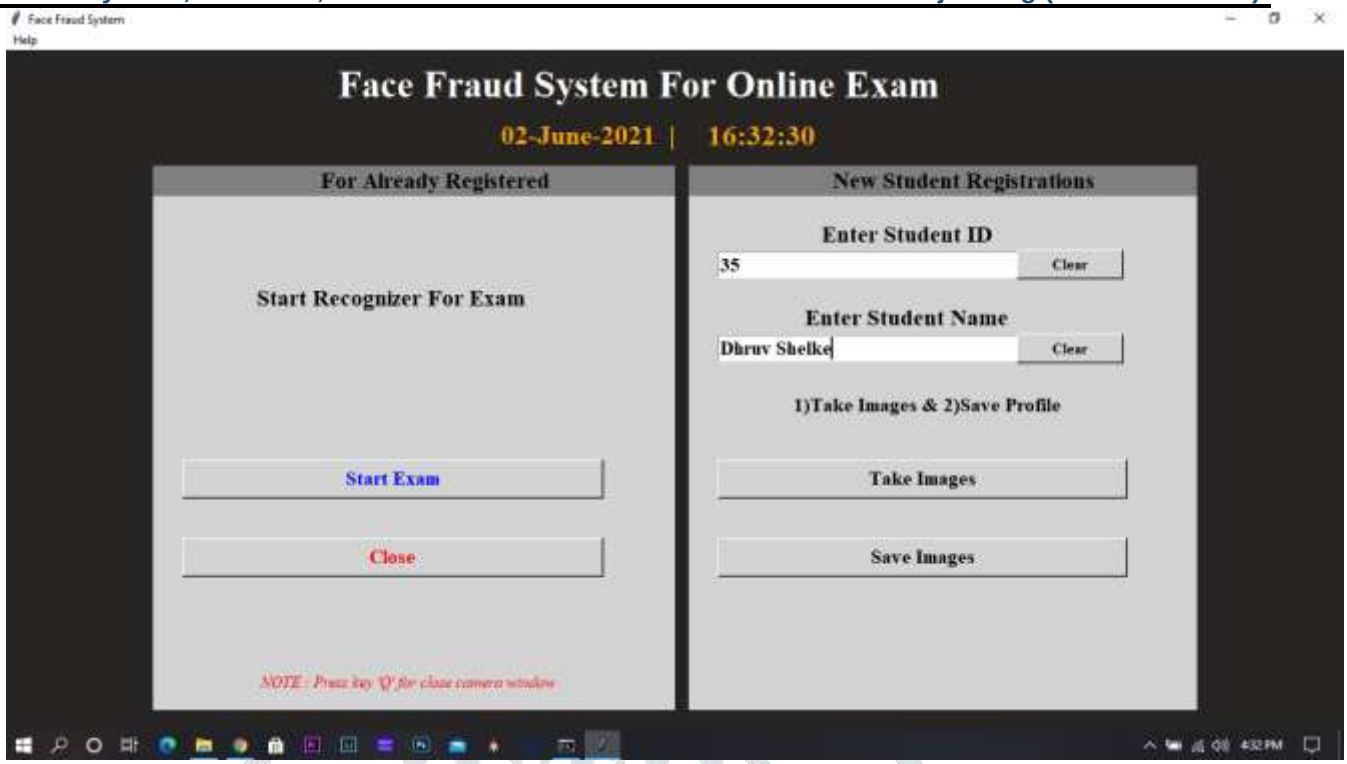
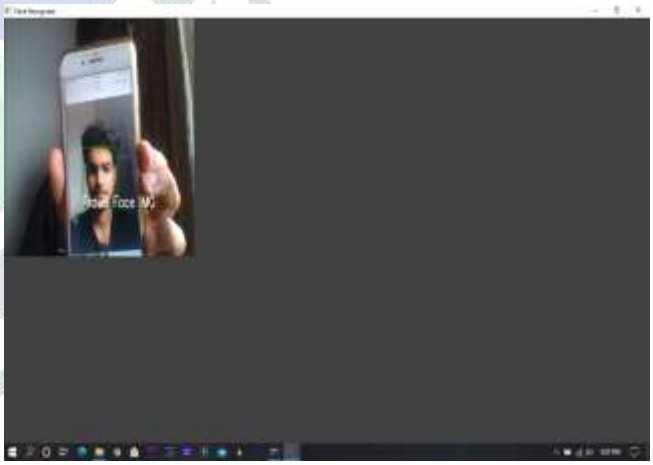


Figure: Student Registration

The system takes continuous images, of the candidates who are attending the exam. If any reflection is detected on the face image, then it is considered as a fake image (spoofing image) and an alert notification is sent to the admin. The outputs of the proposed system for fake and real images are as shown below fig.

(a) Real Face



(b)Fake Face

VI. CONCLUSION

We propose a system that uses light reflection patterns getting from the photo while recording a video or taking an image of the examinee during an examination for detecting a fake face or real face. Spoofing detection becomes a major issue for which an urgent solution is needed in the security field. The system is a strong solution for providing a secure online examination or avoid fraud/ spoof attacks in online exams so that the genuinity of the result is maintained. The system used Haar cascade for detecting a face from a video and an SVM classifier is used for recognizing the face. The Support Vector Classification algorithm is used on the LBP facial features for face recognition. BAed on light reflection pattern system detect fraud faces and send alert notification to the admin. The implemented system is one step towards the advanced identity verification approach and provides genuine results in the online examination.

REFERENCES

[1] Saptarshi Chakrabortyand Dhrubajyoti Das,"AN OVERVIEW OF FACE LIVENESS DETECTION",International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014.

[2] Sanjay Ganorkar, Supriya Rajankar,Gaurav Rajpurohit,"Face Liveness Detection Using Machine Learning",INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 09, SEPTEMBER 2019.

[3] Shun-Yi Wang , Shih-Hung Yang 2,*, Yon-Ping Chen 1 and Jyun-We Huang,"Face Liveness Detection Based on Skin Blood Flow Analysis",Symmetry 2017, 9, 305; doi:10.3390/sym9120305.
[4] Leslie Ching Ow Tiong and HeeJeong Jasmine Lee,"E-cheating Prevention Measures: Detection of Cheating at Online Examinations Using Deep Learning Approach - A Case Study",JOURNAL OF LATEX CLASS FILES, VOL. XX, NO. XX, JAN 2021.
[5] Razan Bawarith, Dr. Abdullah Basuhail, Dr. Anas Fattouh and Prof. Dr. Shehab Gamalel-Din,"E-exam Cheating Detection System",(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 4, 2017.
[6] Saptarshi Chakraborty and Dhrubajyoti Das2,"AN OVERVIEW OF FACE LIVENESS DETECTION",International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014.
[7] Jukka Komulainen, Abdenour Hadid, Matti Pietikainen, Context based Face Anti-Spoofing, Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on Pages: 1-8, 2013.
[8] Avinash Kumar Singh; Piyush Joshi; G. C. Nandi,"Face recognition with liveness detection using eye and mouth movement",2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014).
[9] Arnav Anand; Dinesh Kumar Vishwakarma,"Face Anti-Spoofing by Spatial Fusion of Colour Texture Features and Deep Features", 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS).
[10] Chenqiang Gao ; Xindou Li ; Fengshun Zhou ; Song Mu,"Face Liveness Detection Based on the Improved CNN with Context and Texture Information",Chinese Journal of Electronics (Volume: 28 , Issue: 6 , 11 2019).