Automated Video Surveillance System for Detection of Suspicious Activities during Academic Offline Examination

G. Sandhya Devi, G. Suvarna Kumar, S. Chandini

***Abstract*—**This research work aims to develop a system that will analyze and identify students who indulge in malpractices/suspicious activities during the course of an academic offline examination. Automated Video Surveillance provides an optimal solution which helps in monitoring the students and identifying the malpractice event immediately. This work is organized into three modules. The first module deals with performing an impersonation check using a PCA-based face recognition method which is done by cross checking his profile with the database. The presence or absence of the student is even determined in this module by implementing an image registration technique wherein a grid is formed by considering all the images registered using the frontal camera at the determined positions. Second, detecting such facial malpractices in which a student gets involved in conversation with another, trying to obtain unauthorized information etc., based on the threshold range evaluated by considering his/her mouth state whether open or closed. The third module deals with identification of unauthorized material or gadgets used in the examination hall by training the positive samples of the object through various stages. Here, a top view camera feed is analyzed to detect the suspicious activities. The system automatically alerts the administration when any suspicious activities are identified, thereby reducing the error rate caused due to manual monitoring. This work is an improvement over our previous work published in identifying suspicious activities done by examinees in an offline examination.

***Keywords*—**Impersonation, image registration, incrimination, object detection, threshold evaluation.

I. Introduction

MANY researches are emerging in the field of image processing, with advancement in technology video surveillance has wider applications and plays a key role in tracking human activities. The primary focus of a video surveillance system is to extract video sequences and then analyze the obtained information for any suspicious activities if involved [2]. Visual information is the key source for identification [8] of the human face and its behavioral pattern. Detection of suspicious activities in an Academic Examination [5] hall by video surveillance is an important and real-time application. There are various factors causing malpractices [3] and students are adapting different techniques involved in malpractice [1] during the course of an examination. The suspicious activities include student's abnormal head motion [12] and student swapping his/her place with another student, asking for answers, passing incriminating material. Image registration technique is most useful in feature detection and motion sensing [9]. A front view camera is required to identify impersonation; a top view camera feed with image registration technique is required to identify several other malpractices [11]. An efficient face detection framework is required which is capable of processing images extremely rapidly at high detection rates [7]. Detection of faces and tracking facial features in video sequences is required in which, face detection is a necessary step for face recognition [10] to identify impersonation in an examination hall. Facial features [6] like eyes and lips play an important role to identify a person communicating with others, and as such, required features are extracted from frames of input video. The state of the mouth, whether open or closed, is important information to recognize human interaction [4].

II. Problem Statement

In the existing system during an academic offline exam, manual monitoring of students through invigilators and surveillance videos is performed throughout the world. Such monitoring of examination halls may be prone to error during human supervision. An observer cannot monitor all the students all of the time and may lose focus over time, which gives an opportunity for the students to indulge in malpractices. Monitoring the activities of students during an exam is a very challenging task in terms of manpower. Thus, there is the need for an 'automated video surveillance system', which helps in detecting and minimizing suspicious activities. Moreover, the probability of error can be reduced greatly, thereby increasing the quality of academic examination system.

III. Related Work

This research work presents a real time system for the detection and tracking of suspicious activities in an examination hall which includes three modules. The first module deals with performing an impersonation check which involves verifying whether the legitimate person is sitting in the examination hall. This is done by cross checking his/her profile with the database using a PCA-based face recognition

G. Sandhya Devi and G. Suvarna Kumar are Assistant Professor, Associate Professor with the Department of Computer Science and Engineering, Faculty of Maharaja Vijayram Gajapathiraj College of Engineering, Vizianagaram, India (corresponding author, phone: 9885000708, e-mail: email.gsd@gmail.com, suvarna.cse@mvgrce.edu.in).

S. Chandini was a Post Graduate at the Computer Science and Engineering Department, Maharaja Vijayram Gajapathiraj College of Engineering, Vizianagaram, India (e-mail: chandinisans@gmail.com).

method. In order to determine the presence or absence of a student, we need to obtain the position of an examinee through front and top view camera, using image registration technique. From the registered images of the grid formed, the exact positions of the examinees are calculated. Hence, at a particular position of examinee, if he/she is absent, then it will be updated in the records. Second, detecting such facial malpractices in which a student gets involved in conversation with another, trying to obtain unauthorized information etc. by considering the height of the mouth and the threshold range evaluated to find out whether his/her mouth is open or closed. The third module deals with the identification of unauthorized material or gadgets used in the examination hall from the video captured by a surveillance camera.

IV. Methodology

Initially the live video is processed through the surveillance camera, embedded into the system and then each frame is extracted from the video and analyzed for further actions. The procedure involved is depicted through Fig. 1.

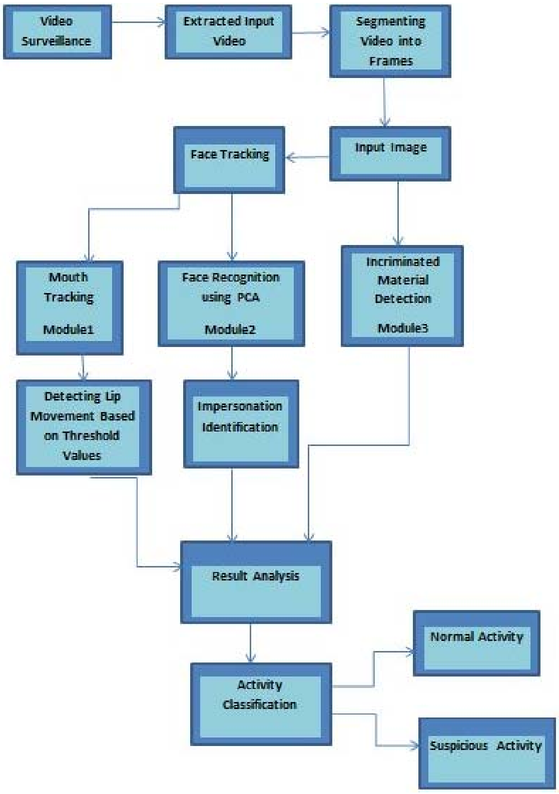

Video Surveillance
Extracted Input Video
Segmenting Video into Frames
Input Image
Face Tracking
Mouth Tracking Module1
Face Recognition using PCA Module2
Incriminated Material Detection Module3
Detecting Lip Movement Based on Threshold Values
Impersonation Identification
Result Analysis
Activity Classification
Normal Activity
Suspicious Activity

Fig. 1 Architecture of proposed system

The first and foremost step in any automated face recognition system is face detection. Its reliability enhances the performance and usability of the system. When any image or a video frame is given as an input, an ideal face detector should be efficient in locating all the faces in the image, regardless of their position, facial gestures and variations in orientation. Viola-Jones [7], which is used to detect the face and to localize the mouth region within the face, is extremely rapid in achieving high detection rates. Once the input is given the computer traces all the faces in the given image with high accuracy. The detected faces are processed in another folder for further analysis. The surveillance camera captures 30 frames per second. If malpractices are identified in 70-80 (or higher) continuous frames, then the activity performed by the examinee (at a position) can be suspected, and then, reported as suspicious.

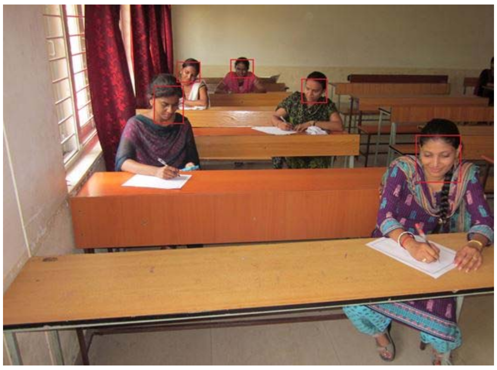


Fig. 2 Face Detection

A. Face Recognition Using PCA for Identifying Impersonation

In this research paper, we implemented the Principal component Analysis based face recognition [10] to confirm the identity of a person by collating the video sequences obtained through surveillance, and the extracted data are embedded into the system and then analyzed by extracting the frames initially, and then applying the Viola Jones algorithm to obtain all the identified faces of the students in the examination hall. The obtained faces are the test images which are to be compared with the trained images in the database using PCA-based face recognition which is called Eigen face. Principal Component Analysis (PCA) is a popular and useful linear transformation technique that is used in numerous applications. The main goal of a PCA analysis is to identify patterns in data and detect the correlation between variables.

As some malpractices cannot be identified only using front view camera, both top mounted camera and front view camera when used together give a better performance. The first module of the research work is impersonation identification which is done by cross-checking the student face in the stored college database. Using Principal Component Analysis technique, the faces are extracted and then validation is performed to confirm their identity. Now from the top view video feed, frames are extracted to analyze and detect the presence or absence of a student through a technique called Image registration. Image registration is a process of transforming different sets of data to one co-ordinate system. It is used to determine top view position of examinees by forming grids. A grid is formed through the faces identified from the video frames. The main idea of forming these grids is to ensure that each and every student is tracked and writing the exam fairly. Two grids are formed from frames extracted through the front view and top view camera, respectively, which are overlaid by using affine transformation. From the registered images after control point registration [11], individual positions of all the students are calculated and stored. While registering for the absence or presence of a student, if at any particular position the student is not present, then we can consider his absence in the records, and while validating for the student details it helps in identifying impersonation.

$$\text{Real time image} = \begin{cases} \text{Closed if } \text{black}_{\text{pixels}} < \text{Threshold}_{\text{mouth}} \\ \text{Open Mouth} \quad \text{other wise} \end{cases}$$

(a)

$$\text{Real time image} = \begin{cases} \text{Closed if } \text{black}_{\text{pixels}} \ <1000 \\ \text{Open Mouth} \quad 1000\text{-}2000 \end{cases}$$

(b)

Fig. 3 (a) Formula to identify state of Mouth, (b) Threshold Range evaluated

B. State of Mouth State Detection Based on Evaluated Threshold Range

The next module in our research work is to identify whether any student is involved in conversation with others trying to obtain unauthorized information. Once the face is detected, the second step is to detect the mouth in the face area. The detected mouth area is extracted from the input image; the next step is to analyze his/her mouth status whether open or closed. To do so, we evaluated the threshold range by considering a large set of frames extracted and stored in the database. Since every person has a different mouth size and height of mouth for every person varies during a conversation, a dynamic threshold value is required to compare the size of the mouth of a particular person. We now compare the state of the mouth for every series of incoming 30 frames with the threshold value. The centroid of the mouth is extracted and height of the mouth with the threshold range is evaluated based on the number of pixels present at the centroid region considering the black and white pixels in that region by converting the image to black and white. This approximate pixel ratio is used to calculate a threshold value which can be used in the coming frames to determine the state of the mouth. In the case that the ratio of black and white pixels in the coming frame is greater than the threshold value i.e., 1000, it means the mouth is open, and if the ratio of black pixels in the coming frame is less then threshold value range 1000, then we consider the mouth is closed. The mathematical representation of closed mouth detection is given in Fig. 3.

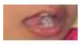
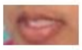
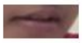
Mouth State	Detected Mouth	Threshold Range of Mouth
Closed mouth		<1000
		<1000
Open mouth		2000
		2500
		1800
		1400

Fig. 4 Analysis of state of Mouth based on threshold ranges evaluated

C. Detection of Incriminated Material

Initially, frames are extracted from the video obtained from the top view camera. The object detector detects objects in images by sliding a window over the image. The detector then uses a cascade classifier to decide whether the window contains an object of interest by searching for the region of interest. Thus, we need to train the detector for each orientation of the object. Region of Interest (ROI) can be selected from any area of our choice from the image selected, thereby creating a binary mask in which selected region pixels are set to 1 and all other pixels set to 0. We can define more than one ROI in an image. The cascade classifier consists of various stages of training depending on the positive samples considered. In every stage the classifier labels the region defined as either positive or negative. Positive indicates presence of the object and negative indicates no objects were found.

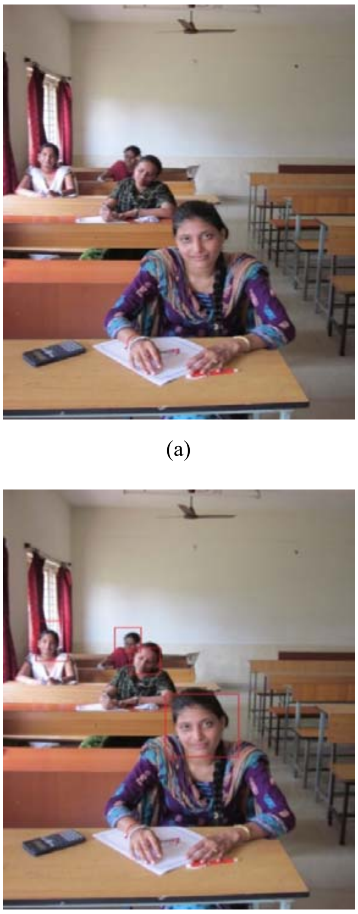
Training an object is done through N stages using cascade classifier. The Object training is done as follows:

1. Initially we store all the positive samples in one folder and negative samples in another.
2. The positive samples are converted into a mat file by loading them into Image Training Labeler App and then the ROI is selected from all the positive dataset and then the positive instances are loaded.
3. We now add the full Image directory path of the positive data samples.
4. Specify the folder with negative images and train the detector.
5. Now the training is done in N stages based on the number of samples and an .xml file is created.
6. Use the newly trained classifier to detect an object in an image.
7. Read the test image as input, and then the Object Detector detects the sign and finally displays the object.

V. Experimental Results

Fig. 5 (a) is a frame extracted from the video processed for further analysis. In Fig. 5 (b) faces are detected and the extracted faces are stored in another folder for further analysis.

This is positive sample of an image where no impersonation is identified.



(a)

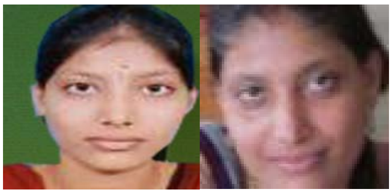
(b)

Fig. 5 (a) Input Frame for Testing, (b) Face Detection in input Frame

A. Impersonation Identification

The Algorithm works in the following manner:

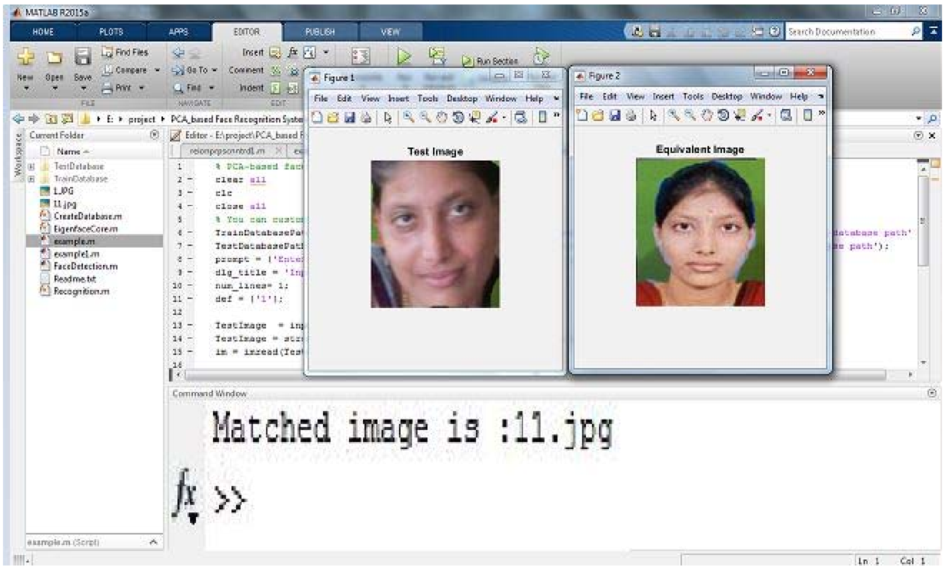
1. First, it contains several images from the training set which are the images of the students stored in the college database.
2. We obtain the test images from the video by processing them to frames and performing face detection.
3. After loading these images, we perform PCA for face recognition in which we find the mean, covariance, eigenvectors and perform comparison with the trained images.
4. Based on the difference from Eigen faces, we confirm the identity of the person.
5. If the test and trained image are matching then there is no impersonation identified.
6. If both the images are not matching then we confirm that there is an impersonation.



(a) (b)

Fig. 6 Evaluation for Impersonation (a) Trained Database Image, (b) Extracted Input Testing Image

From Fig. 6, we can see the actual trained image of the candidate stored in the database, which is validated, and the testing input image at the allocated position, which is extracted from the video processed during the course of an academic offline examination.



```
% PCA-based fac
clear all
clc
close all
% You can custo
TrainDatabasePa
TestDatabasePat
prompt = {'Ente
dlg_title = 'In
num_lines= 1;
def = {'1'};

TestImage  = in
TestImage = str
im = imread(Tes
```

```
Matched image is :11.jpg

fx >>
```

Fig. 7 Principal component based analysis for face recognition

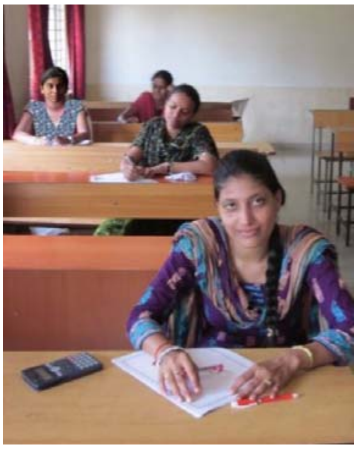
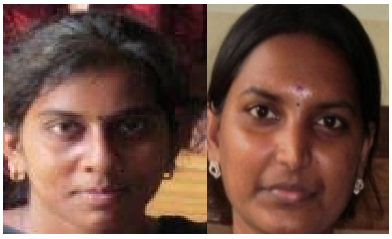


Fig. 8 Test image of Impersonation

From Fig. 7, we can see that the PCA technique is implemented for face recognition, and in this case, the validation is done successfully, wherein the trained image in the database and the test image given as input are matching.

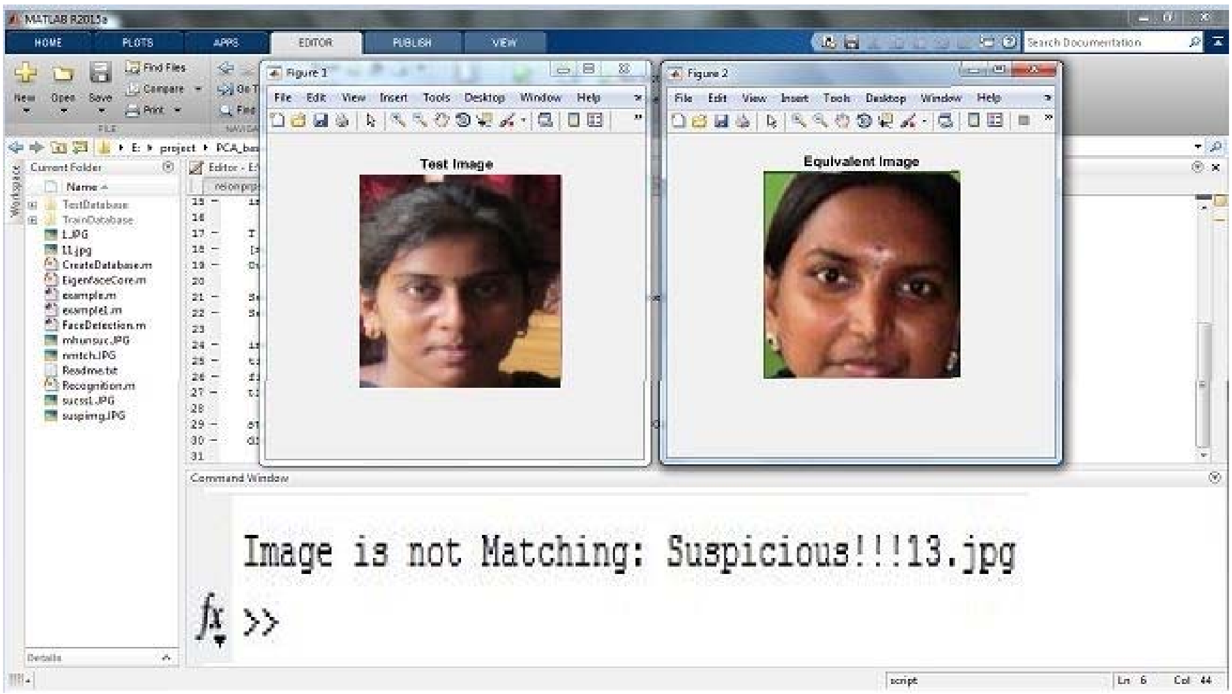
From Fig. 5, we can see that at a specified position certain person has been seated in the left corner. From Fig. 8, after performing the grid evaluation, PCA is applied for face recognition to validate the person and confirm his/her presence in the examination. While performing the validation we obtained a mismatch of image from the database when compared to the test image given as input.



(a) (b)

Fig. 9 Sample Images for Impersonation Verification. (a) Extracted Input Testing Image, (b) Trained database Image

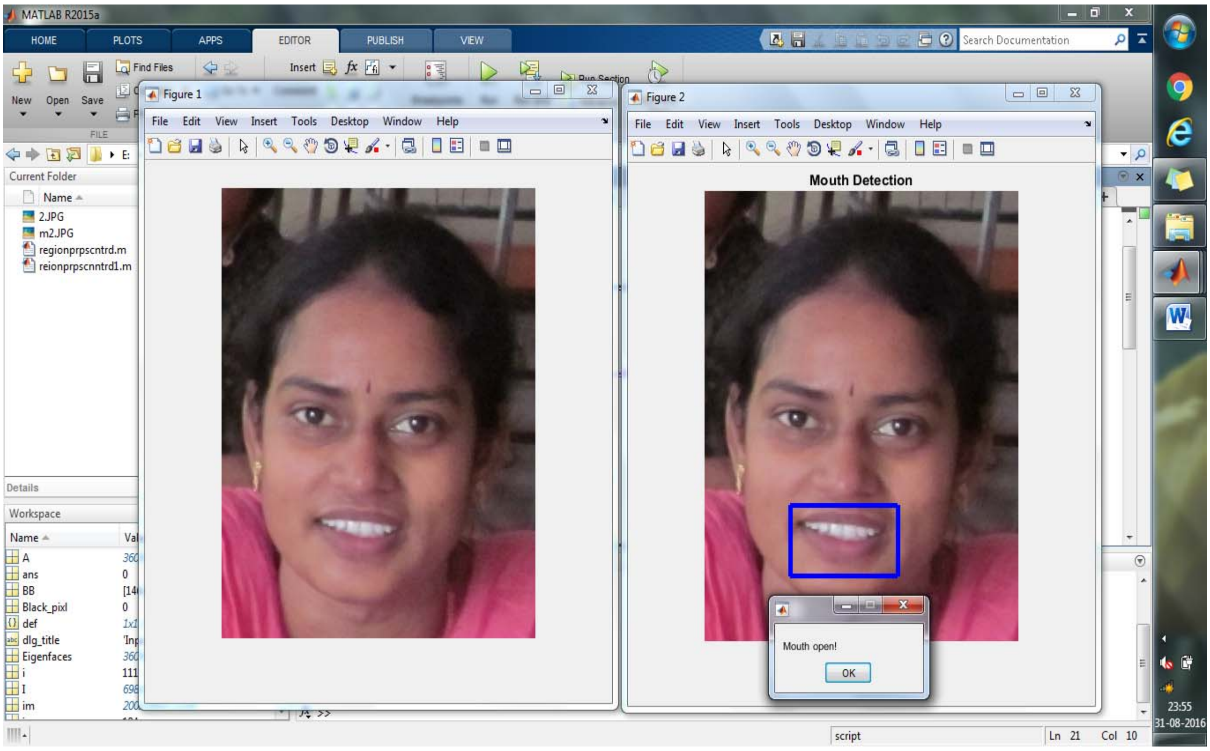
From Fig. 10, we can see that at a specified position impersonation is identified. The test image and trained image of the database are not matching, which means that the person in the trained image has to be seated at a particular position, but instead, another person whose record is not in the database is found seated which clearly indicates an impersonation was done at that particular position.



```
Image is not Matching: Suspicious!!!13.jpg
>>
```

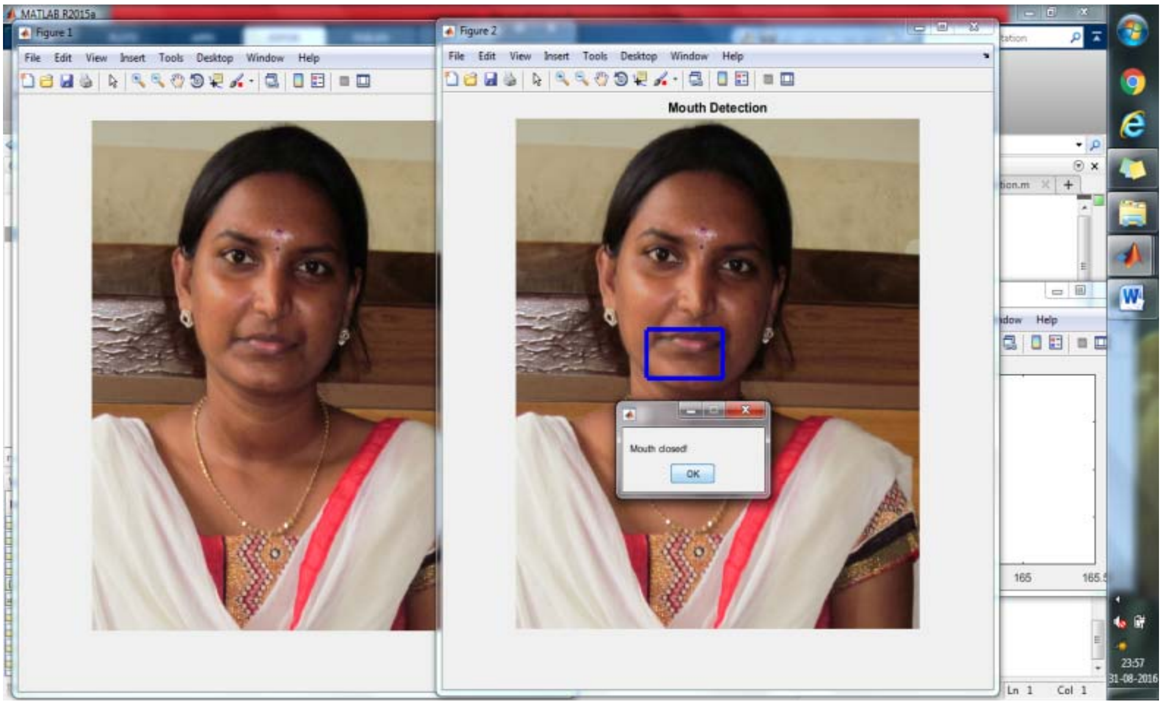
Fig. 10 Impersonation identified after PCA face recognition

B. State of Mouth Detection



Mouth open!

Fig. 11 Detection of open Mouth



Mouth closed!

Fig. 12 Detection of closed Mouth

From Fig. 11, we can see that the threshold range of the mouth is within the range. So it considered as mouth is open.

From Fig. 12, we can see that threshold of the mouth is less than the range evaluated, so in this mouth is considered to be closed.

C. Detection of Incriminated Material

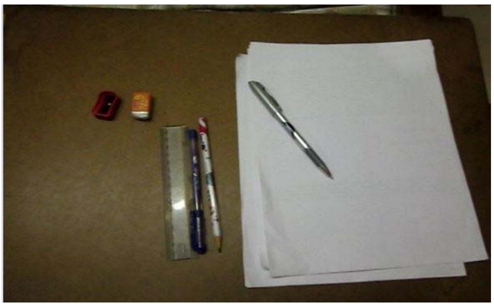
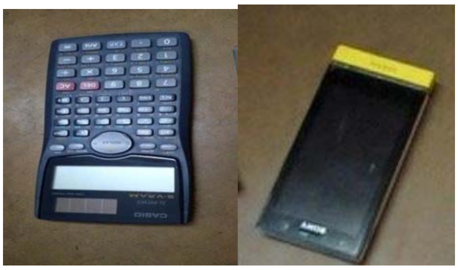


Fig. 13 Frame wherein no incriminated material is found

From Fig. 13, the image is a sample where we can see no incriminated materials are found which indicates no suspicious activities are identified.



(a) (b)

Fig. 14 Trained positive samples of (a) Mobile phone and (b) Calculator for object detection

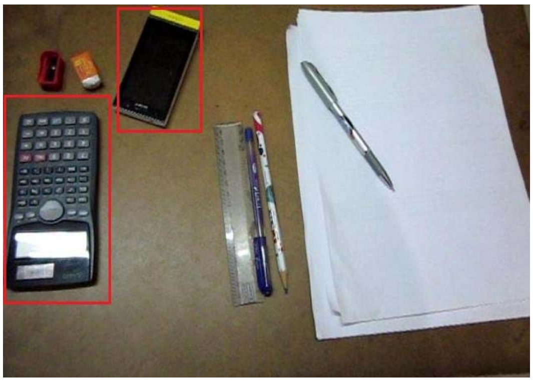


Fig. 15 Incriminated Material Detection

From Fig. 15, we can see that suspicious materials are found, which includes electronic gadgets like calculator and mobile phone indicating malpractice is involved.

VI. Conclusion

The proposed system can be very useful in educational institutions for monitoring students during academic offline examinations; thereby, reducing the burden on the exam administrators. For an educational institution to curb incidents of examination malpractice, surveillance and monitoring system can be a reliable and adequate in providing a conducive and safer environment for the students and staff. The system identifies several malpractices such as impersonation identification, conversation between examinees and identification of incriminated material. The monitoring personnel will be aware of suspicious activities conducted in the class if any. Inputs required are taken from the recorded video during an offline examination. The surveillance system developed is a better approach and helpful to identify incidents of malpractice in an academic offline examination.

References

[1] A. Y. Abdul Kareem, A. T. Alabi, "Curbing Examination Malpractice in the University system", *Nigerian Journal of Educational Research and Evaluation*, Vol. 5, No. 1, 2004.

[2] Ahmad Salihu Ben-Musa, Sanjay Kumar Singh, Prateek Agrawal, "Suspicious Human Activity Recognition for Video Surveillance System", *International Conference on Control, Instrumentation, Communication and Computational Technologies*, Research gate, 2015.

[3] B. C. Amanze, C. C. Ononiwu, B. C. Nwoke, I. A. Amaefule, "Video Surveillance And Monitoring System For Examination Malpractice In Tertiary Institutions", *International Journal Of Engineering And Computer Science*, Vol. 5, January 2016, pp. 15560-15571.

[4] Christian Bouvier, Alexandre Benoit, Alice Caplier, Pierre-Yves Coulon, "Open or Closed Mouth State Detection: Static Supervised Classification Based on Log-polar Signature", *Springer*, Vol. 5259, pp.1093-1102, 2008.

[5] D. Gowsikhaa, Manjunath, S. Abirami, "Suspicious Human Activity Detection from Surveillance Videos", *International Journal on Internet and Distributed Computing Systems,* Vol. 2, No: 2, 2012.

[6] Ijaz Khan, Hadi Abdullah, Mohd Shamian Bin Zainal, "Efficient Eyes and Mouth Detection Algorithm Using Combination of Viola Jones and Skin Color Pixel Detection", *International Journal of Engineering and Applied Sciences*, Vol.3, No. 4, 2012.

[7] Paul Viola, Michael J. Jones, "Robust real Time Face Detection", *International Journal of Computer Vision 57(2)*, pp. 137–154, Kluwer Academic Publishers, 2003.

[8] Pravin Khandagale, Anant Chaudhari, Amol Ranawade, P. M. Mainkar, "Automated Video Surveillance to detect suspicious Human Activity", *International Journal of Emerging Technologies in Computational and Applied Sciences*, pp. 13-128, 2013.

[9] N. Rajesh, H. Saroja Devi, "Emerging trends in video surveillance Applications", *International Conference on Software and Computer Applications*, vol. 9, 2011.

[10] Rajkiran Gottumukkal, K. VijayanAsari, "An improved face recognition technique based on modular PCA approach", *Pattern Recognition Letters 25 (2004),* pp. 429–436, 2003.

[11] G. Sandhya Devi, P. G. V. D. Prasad Reddy, G. Suvarna Kumar, Vijay Chaitanya, "Multiple View Surveillance using Image Registration", *International Journal of Computer Applications*, Vol. 93 – No. 2, 2014.

[12] G. Sandhya Devi, P. G. V. D Prasad, G. Suvarna Kumar, V. Chaitanya, "A Mono Master Shrug Matching Algorithm for Examination Surveillance", *I.J. Information Technology and Computer Science*, 01, pp. 81-86 vol. 1, 2015.