Fraudulent Detection in Examination Department

Sagar M Rao[1], Poonam[2], Bhavana Girish[3], Shivam Pandey[4], Dr.Srividya B V[5]

[1-4]Department of TCE, Dayananda Sagar College of Engineering, Bangalore, Karnataka- 560078

---***---

Abstract: Candidate impersonation is a fundamental problem often referred to as malpractice within the examination system. The proposed model focuses on the image/video of the candidate for the detection of fraud. In this paper, an attempt is made to develop automated face detection and recognition for detecting impersonation of the candidate in the examination system using facial feature extraction. Automated face detection and recognition can further be used in identity verification and attendance monitoring in the examination system. The proposed work constitutes of two steps: Enrolment and face recognition. The enrolment process is divided into two stages: detect face & extract features. Face recognition is performed with OpenCV, Python, and deep learning by using Support Vector Machine (SVM) learning model and Helen dataset.

Keywords: Face Detection, Face Recognition, Feature extraction, OpenCV, Deep Learning, Support Vector Machine (SVM) and Helen dataset.

1. Introduction

The major downside that happens within the examination system is malpractices. Malpractice is known because of the absence of a reputable biometric authentication system for offline and conjointly for online examinations. To beat the downside, researchers have centered on the employment of artificial techniques.

Generally, frauds are detected with the help of outlier analysis. Face detection is often performed very reliable with open CV phase detector working effectively from 90-95% of clear pictures of an individual looking forward at a camera. Face recognition has been a long goal of computer vision, but only in the recent area near reliable automatic face recognition has become a sensible target of biometric research. The matter of face recognition is often stated as recognizing an individual from the image and encompasses a variety of variations aside from the foremost similar applications. The most focus of this is often to detect fraud within the examination system by taking input as video. The goal of this is often to develop a replacement algorithm for a strong pose-invariant face recognition that overcomes many of the limitation found within the existing face recognition system. The researcher is curious about addressing the matter of detecting a face within the color images within the presence of the varied lightning condition and sophisticated background also as recognizing faces under variation in pose, lighting and expression. The system eliminates student identification like student names, or checking the respective identification card, which not only interferes with the teaching process but can also be stressful for the scholars during the examination session. It's extremely important to use various pre-processing techniques to standardize the image that you simply supplied to a face recognition system. There are some ways during which facial appearance is interpreted for the popularity by an automated system.

Once the face is detected, the facial features are extracted and stored in the database with other details of the student/candidate using facial feature extraction. Facial feature points represent the key facial parts which make major contributions to facial expression recognition, such as eyes, eyebrows, mouth, etc. With much less calculation and more accurate feature, we obtained an ideal recognition rate through rigorous experiment

2. Existing Systems

In the existing system almost all the system uses similar techniques. Our main motto is to improve those drawbacks so that they can be utilised effectively.

Fraud Detection in Examination: This model focuses on the image/video for analysis. In this paper, an attempt is made to develop automated face detection and recognition for detecting impersonation of the candidate in an examination system. Automatic face detection and recognition can further be used in identity verification and attendance monitoring in the examination system. The proposed work comprises of two Steps: the enrolment process which is divided into two stages online registration and face detection authentication. Image analysis is carried out with the help of local binary pattern which is used to convert an image into an array for the processing.

A Fraud Detection based Online Test and Behavior Identification Implementing Visualization Techniques: Now a day's online exam has become one of the prominent and most important aspects of our lives, but there is no guaranty of genuinely of the result in the online examination processes. In many of online examinations, the location of the proctor varies from the location of the examinee, there is no guaranty in the authorization of users to the examination and no guaranty in trusting the examination center head that monitors the students during the examination process. Due to the increase in the distance, chances of doing malpractice and misbehaving during the examination increases. To avoid such situations, the examinee must be constantly monitored and should able to stop the examination based on learner's behavior during the examination. Many techniques were proposed for providing security during the conduct of exams. This paper studies various authorization and authentication techniques namely unimodal, multimodal, hardware interaction and data visualization techniques. The paper also proposes a Fraud Detection based Online Test [FDOT] and Behavior identification through Visualization Techniques [BIVT] that avoids and performs more effectively compared with the existing systems.

3. Proposed System

Our main aim is to develop a system for automatic fraud detection in an Examination.

Face detection and recognition system for identity verification and attendance monitoring in the examination system. Fraud concerning to the hall tickets and designs an automated system for impersonation or cross-checking hall tickets using image processing techniques. The major problems occur in examination systems are malpractices. The fundamental Problem identified is the absence of a credible identity verification system for offline and for online examination system. The solution for this problem is an examination system designed based face detection and verification technology incorporating the security strength of examination and the accuracy.

Impersonation is nothing but to pretend to be for purposes of fraud or to assume the character or appearances of especially fraudulently, which is one of the main problems to be addressed in our project. Secondly in case of impersonation is detected whether the candidate is authenticated or not. If the person is authenticated his attendance is also recorded and the message is sent to the authority.

The main objective of our system is to:

1. This is implemented in both online and offline examination.
2. It makes use of ciphers and steganography.
3. The proposed system not only detects face but also locates important facial features such as eyes and mouth. This feature are crucial to the performance of face recognition.
4. Image segmentation is used to locate objects and boundaries in the image it will assign to label to every pixel in an image. The result of segmentation is set of segments that will collectively cover the entire image.
5. Use of RSA algorithm to provide authentication.
6. Collection of database for comparison and verification to provide fraudulent.

Figure 1: Overview of Application Architecture

4. Algorithm

Support Vector Machine Algorithms

Support vector machine (SVM) [2], which uses the SVM classification combination in series and introduces the type weight factor and sample weight factor. The model not only solves the shortcomings of a small sample, high dimension, nonlinear and local minima in the traditional model but solves the wrong classification question caused by the number imbalance of training samples and data interference. Classification of objects has been a significant area of concern in machine vision applications. In recent years, Support Vector Machines (SVM) is gaining popularity as an efficient data classification algorithm and is being widely used in many machine vision applications due to its good data generalization performance [2].
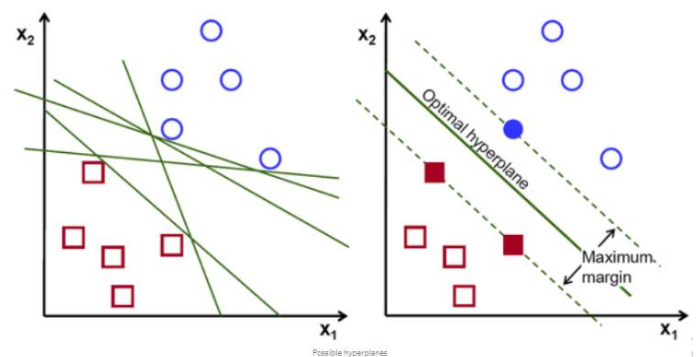
The objective of the support vector machine algorithm is to find a hyperplane in N-dimensional space(N — the number of features) that distinctly classifies the data points. To separate the two classes of data points, many possible hyperplanes could be chosen. Our objective is to find a plane that has the maximum margin, i.e. the maximum distance between data points of both classes. Maximizing the margin distance provides some reinforcement so that future data points can be classified with more confidence.

Cascaded classifier

Haar cascade

Face detection can be used to find and index pictures and videos with background, size and position. There are some methods of face detection. One of these is haar cascade. It allows the system to recognize people's face with varied illumination [3].

Here we will work with face detection. Initially, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) to train the classifier. Then we need to extract features from it. For this, haar features shown in the below image are used. They are just like our convolutional kernel. Each feature is a single value obtained by subtracting the sum of pixels under a white rectangle from the sum of pixels under a black rectangle.
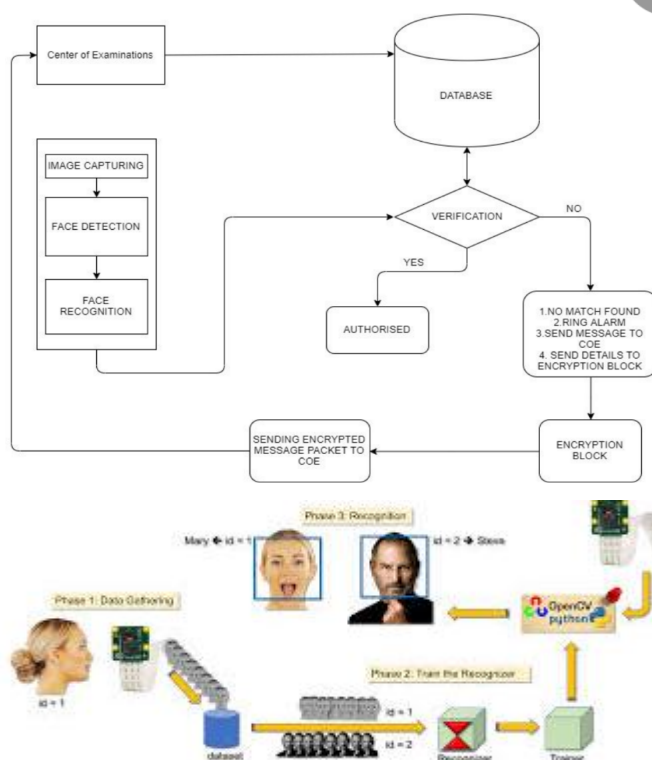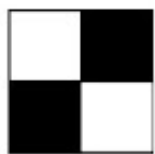
(a) Edge Features

(b) Line Features

(c) Four-rectangle features

$$MouthMap = C_r^2 \cdot \left(C_r^2 - \eta \cdot C_r/C_b\right)^2,$$

$$\eta = 0.95 \cdot \frac{\frac{1}{n} \sum_{(x,y) \in \mathcal{FG}} C_r(x,y)^2}{\frac{1}{n} \sum_{(x,y) \in \mathcal{FG}} C_r(x,y)/C_b(x,y)}$$

5. Expected Results

Enrolment side:

Facial landmarks are used to localize and represent salient regions of the face, such as Eyebrows, Eyes, Jawline, Nose and Mouth. These details are stored in the database with other details of the student like their USN, Name etc.
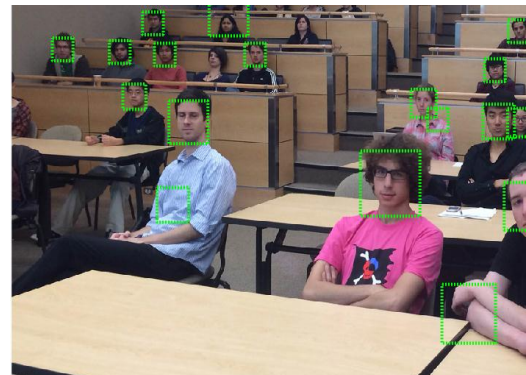
Examination Hall:

The facial features present in the database is made available in the cloud. The surveillance camera in the examination, which is given access to the database makes use of facial features to recognize the candidates present in the examination hall. If any candidates not recognized, they are reported to the center of examination as an unrecognized student/candidate.

6. Applications

1. For identity verification and attendance monitoring in the examination system
2. Fingerprint recognition: It refers to the automated method of verifying a match between two human fingerprints.
3. Security: Security has two dialogues. Negative dialogue is about danger, risk, threat etc. Positive dialogue is about opportunities, Interests, profits etc. Negative dialogue needs military equipment, armies, police. Positive dialogue needs social capital, Education, social interaction
4. Smart Cards: It makes use of an embedded integrated circuit chip that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone [5]. The range is typically one-half to three inches for non-battery-powered cards, ideal for applications such as building entry and payment that require very fast card interface.
5. Surveillance: Is the monitoring of the behavior, activities, or other changing information, usually of people to influence, manage, directing, or protecting them. This can include observation from a distance employing electronic equipment (such as CCTV cameras). Surveillance is used by governments for intelligence gathering, the prevention of crime, the protection of a process, person, group or object, or for the investigation of crime. It is also used by criminal organizations to plan and commit crimes such as robbery and kidnapping, by businesses to gather intelligence, and by private investigators.
6. Multimedia Others: Multimedia is content that uses a combination of different content forms such as text, audio, images, animation, video and interactive content. Multimedia contrasts with media that use only rudimentary computer displays such as text-only or traditional forms of printed or hand-produced material
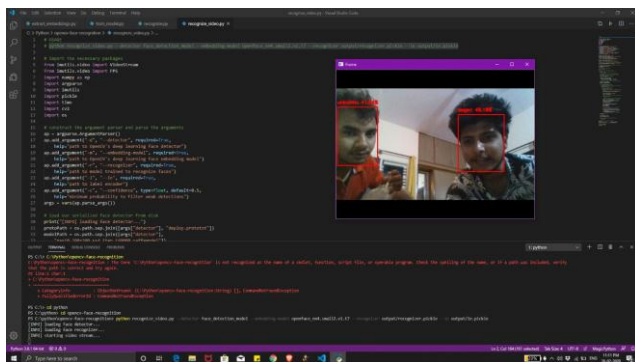
7. References

[1]. Liang, X., Cai, X., Li, L., & Chen, Y. (2017). Facial feature extraction method based on shallow and deep fusion CNN. 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD). doi:10.1109/fskd.2017.8393320

[2]. Suriya Prakash, J., Annamalai Vignesh, K., Ashok, C., & Adithyan, R. (2012). Multi-class Support Vector Machines classifier for machine vision application. 2012 International Conference on Machine Vision and Image Processing (MVIP). doi:10.1109/mvip.2012.6428794

[3]. Tyas Purwa Hapsari, D., Gusti Berliana, C., Winda, P., & Arief Soeleman, M. (2018). Face Detection Using Haar Cascade in Difference Illumination. 2018 International Seminar on Application for Technology of Information and Communication. doi:10.1109/isemantic.2018.8549752

[4]. Face Recognition Across Pose and Illumination (Beveridge, J. Ross, et al. "Factors that influence algorithm performance in the face recognition grand challenge." Computer Vision and Image Understanding113.6 (2009): 750-762.).

[5]. Smart card technology IJSER International Journal of Scientific & Engineering Research, Volume 7, Issue 3, March-2016 157 ISSN 2229-5518 IJSER © 2016.

[6]. An automated fraud detection of hall tickets in an offline examination system using ANN classifier (Shridevi Soma and Vidyashree S.A. Article: An Automated Fraud Detection of Hall Ticket in an Offline Examination System using ANN Classifier. International Journal of Computer Applications 126(8):7-12, September 2015. Published by Foundation of Computer Science).

[7]. Multi-Mode Biometric Solution for Examination Malpractices (Adeoye, Olufemi Sunday. "Multi– Mode Biometric Solution for Examination Malpractices in Nigerian Schools." International Journal of Computer Applications 4.7 (2010): 20-26.).

[8]. Creadit Card Fraud Detection Using Iris Biometrics Techniques (International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2024).

[9]. Face detection system for attendance of class students (Akram, Farida, and Ram P. Rustagi. "An efficient approach towards privacy preservation and collusion resistance attendance system." MOOCs, Innovation and Technology in Education (MITE), 2015 IEEE 3rd International Conference on. IEEE, 2015.).

[10]. An efficient biometric multimodal face, iris & finger fake detection using an adaptive Neuron Fuzzy infernal system (. Wilson, S., and A. Lenin Fred. "An Efficient Biometric Multimodal Face, Iris and Finger Fake Detection using an Adaptive Neuro Fuzzy Inference System (ANFIS)." Middle East Journal of Scientific Research 22.6 (2014): 937-947).

[11]. Implementing biometrics to curb examination malpractices in Nigeria (Center for information security and Network Research, University of Plymouth, United Kingdom).