International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 6 ǁ 2022 ǁ PP. 975-978

Detecting Impersonators in Examination Centers

Puduru Pavan[1]
PG Scholar
Master of Computer Applications
Madanapalle Institute of Technology & Science, India

Mr. S. Balamurugan[2]
Assistant Professor
School of Computers
Madanapalle Institute of Technology & Science, Madanapalle, Chittoor Dist., AP, India

Mrs.S.Savitha[3]
Assistant Professor
Department of Computer Science
Saradha Gangadharan College, Pondicherry

[1,2,3]*Master of Computer Applications, Madanapalle Institute of Technology and Science, India.*

ABSTRACT :
Detecting impersonators in examination room is critical for providing a better examination handling system that can aid in the reduction of malpractices that occur in examination centres. According to recent news reports, a national testing agency identified 56 JEE candidates who are potential impersonators. To solve this problem, an efficient method requiring less manpower is required. This problem is simple to solve thanks to advances in machine learning and AI technology. In this project, we are creating an AI system in which images of students with names and hall ticket numbers are collected, pre-trained using the KD-Tree algorithm, and the model is saved. When a student enters the classroom, he or she should look at the camera and then enter the classroom.

Keywords: *Impersonation, Online Examination, Face Recognition, Fingerprint Verification, Aadhaar Card.*

Date of Submission: 02-06-2022 Date of acceptance: 14-06-2022

I. INTRODUCTION

The threat is any factor that poses any form of harm to the proper functioning and satisfying the objective of the system in a secure way ensuring confidentiality, authenticity and other necessary features. An Online Examination is a critical asset in the fast-growing online learning environment. In order to assess the threats, we should understand the nature of the system and must analyze the environment where the system is deployed. Collusion is identified as the highest rated threat in an online examination. Intent of most threats backtracks to the motive of cheating by the candidates for obtaining assistance during examination to enhance their chances in the examination amongst the competitors.

As we already discussed lack of integrity of the invigilator may increase the chance of collusion in an examination. The only way to address this issue is to conduct a runtime dynamic authentication during the online examination. Then this recently recorded image is compared with the images captured during random intervals for identification of violations. Violation here refers to mismatch of features above a certain degree which drives to the decision that the person currently taking up the examination is not the corresponding candidate. Violations identified by the algorithm is logged in a centralized repository under control of the examination authority. Manual verification by the invigilator is triggered to conform the violation**.** This entire process is secured and conducted in those corresponding systems to avoid any intrusion and modification of crucial data 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-7, 2017 62 resulting in failure of the system to meet the intended functionality. Violations identified by the algorithm is logged in a centralized repository under control of the examination authority. Manual verification by the invigilator is triggered to conform the violation**.**

Most online assessments are hosted on open-source systems that are vulnerable to hacking. With a virtual machine and some insider help, anyone can take control of a student's computer and impersonate them from a remote location. Lately, a string of incidents surfaced where online exam papers for technical and non-technical posts were rigged. For instance, the 2019 IAF recruitment exam was hacked by impersonators who took the test from a remote location. As reported by the Indian express, supervisors of examination centers were lured into installing the "Team viewer software" on their computers. "Supervisors switched off CCTV cameras while hacking the server. On the day of the examination, the candidates would sit at the center but the impersonator, sitting in their room, would take the tests for them"

II.LITERATURE REVIEW

Face detection is a computer technology that determines the location and size of human face in arbitrary (digital) image. The facial features are detected and any other objects like trees, buildings and bodies are ignored from the digital image.Face detection, can be regarded as a more general 'case of face localization. In face localization, the task is to find the locations and sizes of a known number of faces (usually one). Basically there are two types of approaches to detect facial part in the given image i.e. feature base and image base approach. feature base approach tries to extract features of the image and match it against the knowledge of the face features.

When of facial features such as the eyes, lips, nose, mouth and eyebrows. In order to achieve the task, a snake is first initialized at the proximity around a head boundary. It then locks onto nearby edges and subsequently assume the shape of the head. The evolution of a snake is achieved by minimizing an energy function, Esnake (analogy with physical systems), denoted as Esnake = Einternal + EExternal Where Einternal and EExternal are internal and external energy functions. Internal energy is the part that depends on the intrinsic properties of the snake and defines its natural evolution. The typical natural evolution in snakes is shrinking or expanding. Energy minimization process is done by optimization techniques such as the steepest gradient descent.

Which needs highest computations. Huang and Chen and Lam and Yan both employ fast iteration methods by greedy algorithms. Snakes have some demerits like contour often becomes trapped onto false image features and another one is that snakes are not suitable in extracting non convex features. Deformable Templates: Deformable templates were then introduced by Yuille et al. to take into account the a priori of facial features and to better the performance of snakes. Locating a facial feature boundary is not an easy task because the local evidence of facial edges is difficult to organize into a sensible global entity using generic contours.

The low brightness contrast around some of these features also makes the edge detection process.Yuille et al. took the concept of snakes a step further by incorporating global information of the eye to improve the reliability of the extraction process. Department of ECE Page 6 Deformable templates approaches are developed to solve this problem. This synthesis of ideas from image processing and statistical shape modelling led to the Active Shape Model.

The first parametric statistical shape model for image analysis based on principal components of inter-landmark distances was presented by Cootes and Taylor in. On this approach, Cootes, Taylor, and their colleagues, then released a series of papers that cumulated in what we call the classical Active Shape Model.

III. PROPOSED METHOD

In proposed system initially images of each student are collected and each dataset consists of 50 images of each student. These images are trained using kdtree algorithm using image processing technique and model is saved in system this model can be used for automatic prediction of student in exam halls from live video or images.

The present system of online examinations includes a registration phase where the details of the candidate are entered. A passport size photograph, as well as a thumbprint is taken as proofs of identity. In some cases, a signature, either a scanned copy or a digital signature is collected as well.

The next phase is that of examination. Only those candidates with a valid admit card are allowed into the examination hall. The fingerprint verification of the candidate is done and a system is allotted to the candidate if the document verification yields a positive result. Now, the candidate can enter his/her registration number and a password on a screen which is later redirected to the page of examination. In some cases, the login page also shows the image of the student to whom the specific system is allotted.

K-D TREE ALGORITHM

The *k*-d tree is a binary tree in which node is a *k*-dimensional point. Every non-leaf node can be thought of as implicitly generating a splitting hyperplane that divides the space into two parts, known as half-spaces. Points to the left of this hyperplane are represented by the left subtree of that node and points to the right of the hyperplane are represented by the right subtree. The hyperplane direction is chosen in the following way:

every node in the tree is associated with one of the *k* dimensions, with the hyperplane perpendicular to that dimension's axis. So, for example, if for a particular split the "x" axis is chosen, all points in the subtree with a smaller "x" value than the node will appear in the left subtree and all points with a larger "x" value will be in the right subtree. In such a case, the hyperplane would be set by the x value of the point, and its normal would be the unit x-axis.

ADVANTAGES:

- Student verification process is fast and accurate with least effort. Reduces impersonators issue with live verification.
- Time taken for prediction and processing is less and prediction done automatic using trained model.
- Trained model can be used to track live video and automates process of detecting students at exam centers and display in video.

IV. System Architecture

- Student verification process is fast and accurate with least effort. Reduces impersonators issue with live verification.
- Time taken for prediction and processing is less and prediction done automatic using trained model.
- Trained model can be used to track live video and automates process of detecting students at exam centers and display in video.

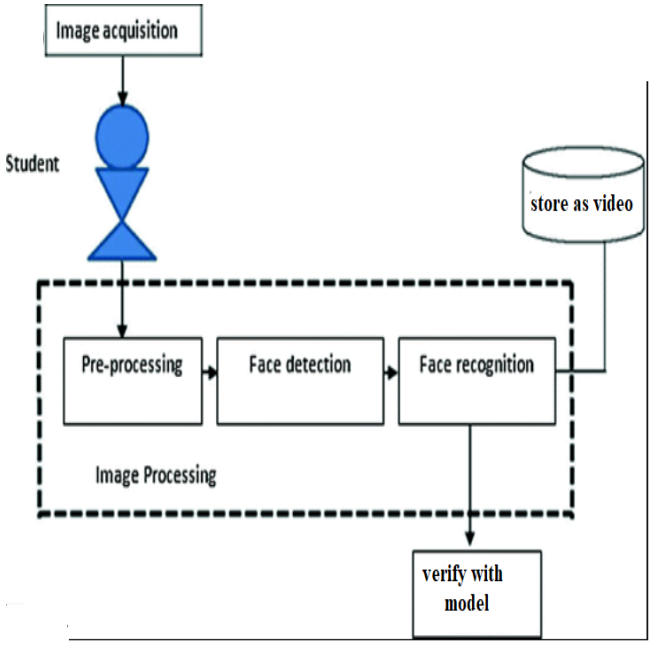

Image Acquisition

Digital **Image** Processing.in **image** processing, it is defined as the action of retrieving an **image** from some source, usually a hardware-based source for processing. It is the first step in the workflow sequence because, without an **image**, no processing is possible.

Pre-processing

Pre-processing is a common name for operations with images at the lowest level of abstraction both input and output are intensity images. The aim of pre-processing is an improvement of the image data that suppresses unwilling distortions or enhances some image features important for further processing, although geometric transformations of images are classified among pre-processing methods here since similar techniques are used.

Face Detection

The face is one of the easiest ways to distinguish the individual identity of each other. Face recognition is a personal identification system that uses personal characteristics of a person to identify the person's identity. Human face recognition procedure basically consists of two phases, namely face detection, where this process takes place very rapidly in humans, except under conditions where the object is located at a short distance away, the next is the introduction, which recognize a face as individuals.

FACE RECOGNITION

There are two predominant approaches to the face recognition problem: Geometric (feature based) and Recognition algorithms can be divided into two main approaches: 1. Geometric: Is based on geometrical relationship between facial landmarks, or in other words the spatial configuration of facial features. 2. Photometric stereo: Used to recover the shape of an object from a number of images taken under different lighting conditions. Popular recognition algorithms include: 1. Principal Component Analysis using Eigenfaces, (PCA) 2. Linear Discriminate Analysis, 3. Elastic Bunch Graph Matching using the Fisherface algorithm

V.RESULT

An automated method of detecting impersonation in online examinations has been developed, which requires minimal human intervention and does not depend on the trustworthiness of the invigilators present in the examination hall. After the fingerprint verification is done, the student is allowed to take his/her seat, where ascreen asking for the username and password is displayed. After logging in, at regular intervals, the face detection is done, and if any extra face or any mismatch in the face is found multiple times, then the examination is paused and an alert SMS is sent to the examination authority in-charge of that particular center.

Due to the rapid developments in the field of biometric recognition, especially that of face recognition, wherein, three dimensional identification is being evolved, this method of identification would help eliminate impersonation. In the case of unavailability of proper fingerprint (like accident victims, or certain skin disorders), iris recognition can be done. Aadhar Card has information about the iris and the fingerprint, hence the details can be verified using the same. In the near future, the online examination would replace the pen-and-paper methods, and hence many robust methods to eliminate impersonation could further be developed using biometric and physiological behavior patterns of the individuals.

VI.CONCLUSION

The computational models, which were implemented in this project, were chosen after extensive research, and the successful testing results confirm that the choices made by the researcher were reliable. The only reason for this was the face recognition subsystem did not display even a slight degree of invariance to scale, rotation or shift errors of the segmented face image. Implementing an eye detection technique would be a minor extension to the implemented system and would not require a great deal of additional research.

They would probably be more compliant when a 6'5" policeman is taking their mugshot! In mugshot matching applications, perfect recognition accuracy or an exact match is not a requirement. If a face recognition system can reduce the number of images that a human operator has to search through for a match from 10000 to even a 100, it would be of incredible practical use in law enforcement. The automated vision systems implemented in this thesis did not even approach the performance, nor were they as robust as a human's innate face recognition system. However, they give an insight into what the future may hold in computer vision.

REFERENCES

[1]. Hindustan Times (January 2011), "Online tests gain traction in India" [Online]. Available: http://www.livemint.com/Politics/ 4n7yjM4f t1aa S6fqhl rB4I/Online-tests-gain-traction-in-India.html (Accessed: January 2017)

[2]. Aakash, "The war of offline vs online exams show rising popularity of new trends in education" [Online]. Available: http:/ /aakashinstitute.aakash.ac.in/blog/the-war-of-offline-vs-online exams show-rising-popularity-of-new-trends-in-education/(Accessed: January 2017)

[3]. S. G. Anuradha, B. Kavya, S. Akshatha, K. Jyothi, G. Ashalatha, "Automated face detection and recognition for detecting impersonation of candidate in examination system", International Journal of Scientific & Engineering Research, Vol. 7, Issue 3, ISSN 2229-5518 (March 2016)

[4]. N. A. Karim, Z. Shukur, "Using preferences as user identification in the online examination", International Journal on Advanced Science Engineering Information Technology, Vol. 6, No. 6, ISSN 2088-5334 (2016)

[5]. K. Patrick, Dr. S. O. McOyowo, Dr. H. O. Okoyo, "Addressing impersonation threats in online assessment environment using temporal information and systems interactions", Merit Research Journal of Education and Review, Vol.3, pp. 215-220, ISSN: 2350-2282 (June 2015)

[6]. J. W. Gathuri, A. Luvanda, S. Matende, S. Kamundi, "Impersonation challenges associated with e-assessment of university students", Journal of Information Engineering and Applications, Vol.4, No.7, ISSN 2225- 0506 (2014)

[7]. M. Pietikainen (2010), "Local binary patterns" [Online]. Available: http://www.scholarpedia.org/article/Local_Binary_Patterns (Accessed: February 2017)

[8]. OpenCV 2.4.13.2 documentation, "Face recognition with OpenCV" [Online]. Available:http://docs.opencv.org/2.4/modules/contrib/doc/facerec/facerec_tutorial.html (Accessed: February 2017)