Impersonation Detection in Online Examinations

Pooja Mahesh
Student, ECE – Design & Manufacturing
IIITD&M - Kancheepuram
Chennai, India
poojamahesh6895@gmail.com

K Selvajyothi
Assistant Professor, ECE - Design & Manufacturing
IIITD&M - Kancheepuram
Chennai, India
ksjyothi@iiitdm.ac.in

***Abstract*—In today's world that witnesses an ever-changing scenario in the technical fields, the concept of an "examination" too has changed. From the traditional methods of pen-and-paper and Optical Mark Recognition (OMR), it has evolved into 'Online Examinations', which are a lot more flexible, time-saving as well as require much fewer resources. However, they have certain drawbacks too. While the uncertainties involved in the working of the electronic equipment and 'server break-down' do affect the examination, the developments in technology have helped overcome these. However, the most important problem faced by online examinations is the authenticity of the student who is taking it. Impersonation, as it is called, is in fact, due to the negligence (or in certain cases due to the cooperation) of the human factors that are present at the examination centre. In this paper, the aim is to eliminate these human factors, to ensure that impersonation, if any, can be easily detected, and the impersonator is not allowed to take the examination. For this purpose, two- step biometric verification of the candidate is done, one of which extends throughout the duration of the examination. In this manner, impersonation can be avoided.**

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

I. INTRODUCTION

Online examinations have slowly begun gaining popularity and are taking over the traditional methods of pen-and –paper and OMR response sheets in India. Initially, however, it did face numerous challenges. Back in the year 2009, when the Delhi Common Admission Test (DCAT) went online, the organizers were forced to offer examinees another chance at answering the paper as there were computers getting crashed and numerous candidates were unable to complete the test [1].

Almost a decade after the DCAT incident, online examinations have become a trend. Most organizers prefer online examinations over offline examinations due to factors like cost effectiveness as well as time and energy conservation. Students too have begun adapting to the new method, though gradually. The advantages of an online examination over the offline one, from a student's perspective include the ease of changing a selected answer, the flexibility to choose a date of examination as well as the timer set at the server, which helps them manage their examination time effectively [2].

Various proposals have been made to eliminate impersonation in online examinations. However, most of them involve only a one step biometric verification [3], or verification of behavioral characteristics [4, 5], which are not always reliable.

Various types of impersonation challenges that are faced in an online examination are discussed in [6]. In this paper, a method is designed and implemented to eliminate these impersonation types. Here, a system of impersonation detection is proposed that consists of a two-step biometric verification to completely eliminate the chances of impersonation. The first step is an already existing fingerprint verification, and the second step is a face detection and recognition done throughout the duration of the examination, to avoid any form of impersonation.

The paper is organized as follows. The proposed method of avoiding impersonation with minimal human interference has been discussed in Section II. In Section III, the implementation methodology of the proposed system is discussed, followed by results and conclusions.

II. PROPOSED METHOD

A. Existing System of Online Examination

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.

978-1-5386-3864-4/17/$31.00 © 2017 IEEE

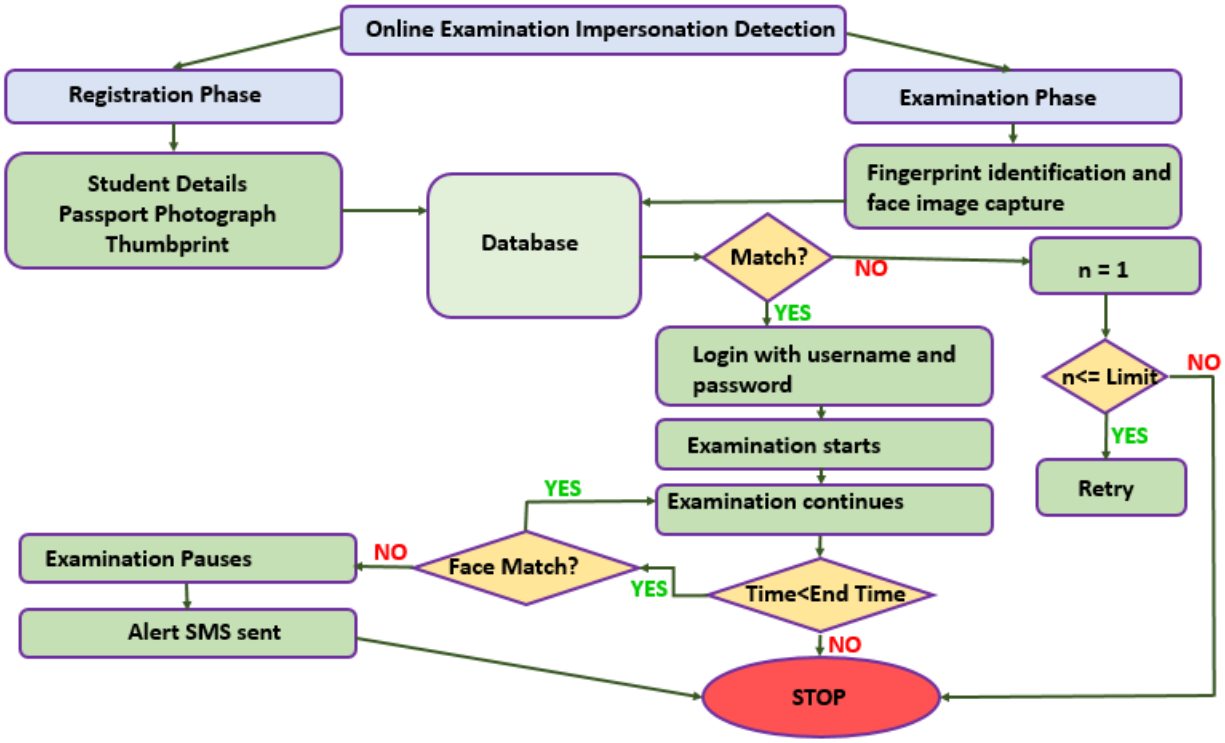

Fig. 1. Flowchart of the proposed impersonation detection method.

B. *Proposed System of Online Examination*

The major problem that is faced by the online examinations is impersonation as already mentioned. The aim of this paper is to introduce an online examination system that can tackle the issue of impersonation with very little human factors involved. This is necessary as the trustworthiness of the invigilators cannot always be guaranteed.

There are two phases involved in the process of conducting the online examination (Fig.1):

- The Registration Phase, and
- The Examination Phase

C. *The Registration Phase*

At the time of Registration, the candidate is required to fill in personal details like name, date of birth, gender and educational qualifications to prove eligibility to take the examination. The Aadhaar Card information is also collected along with a passport sized photograph of the candidate.

D. *The Examination Phase*

The following are the sequence of events at the examination center:

- The candidate must verify his/her examination center and check for the system allotted.
- Upon entering the examination hall, on the monitor that is allotted to each of the candidates, a list of instructions would be displayed, as shown in Fig. 2.

Fig. 2. Page showing instruction for the verification procedures.

- After fingerprint verification (during which an image of the candidate is also captured), the screen moves onto the login page, as shown in Fig. 3.

Fig. 3. Login page with photograph verification.

- The candidate has to verify if the photograph matches with that of his/her own. If it matches, then the candidate can enter the username and password and login to the

page displaying instructions to take the examination (Fig. 4).

- If the photograph is not matching, then the invigilator has to be contacted.
- From the instructions page, the user/candidate is taken to the examination page, at a pre-set time. The clock would be set at the server.
- Once the examination starts, the image of the student is compared to that of what was captured while the fingerprint was entered. If the image matches, the examination continues. Else, after a set number of limits of impersonation threat, the examination pauses, and an alert is given as shown in Fig. 5.Along with the examination being paused, a message will be sent to the examination in-charge (or the higher authorities of the body conducting the examination), warning them of an impersonation attempt (Fig. 6).
- The candidate would not be able to resume the exam until his/her candidature is verified by the concerned authorities.
- If the candidate is found to be fraudulent, then stringent actions are taken.
- If the alert is found to be false (due to system errors, which may occur sparingly), after a thorough verification by the higher officials, the examination can be resumed.

Fig. 4. Instructions for the examination.

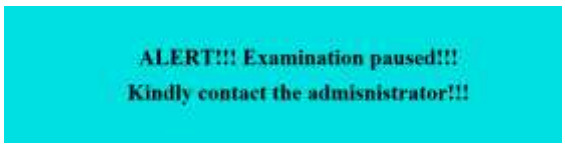

Fig. 5. Alert Message displayed on the screen.

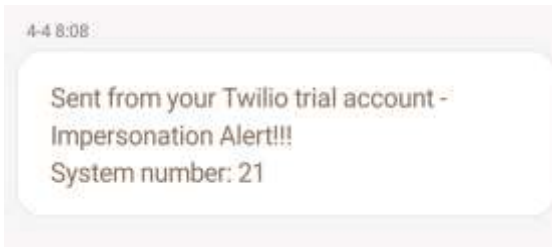

Fig. 6. Alert message sent.

III. Implementation of Proposed System

A. Webpage Development

The front end of the system proposed has been developed ensuring that it is user-friendly and simple to implement. Clear instructions are given to the candidates in order to ensure that there is no ambiguity and discomfort to the candidates appearing for the examination.

The detailed front-end process is already discussed in Section II. The front-end is made user-friendly and easy to comprehend. Also, the system is so designed that any external device (or another system), cannot be connected to it either in the wired, or the wireless form. This is done to avoid any possibility of wireless accessibility to the online examination by an impersonator who is located elsewhere, while the actual candidate is present before the original system in order to prove the candidature authenticity.

B. Fingerprint Recognition

A simple optical fingerprint sensor is connected to the laptop or the personal computer using a serial to universal serial bus (USB) convertor.

Here, while implementing, the fingerprints have to be enrolled. However, in the actual examination scenario, fingerprint data can be extracted from the database of Aadhaar Card.

Using the Aadhaar Card details, the identity of the person can be verified. Hence, Aadhaar card forms an integral part of this method of impersonation detection, as it reduces the resources required during the enrolment phase as well.

Fig. 7 shows the process of finger verification, where a finger is placed on the optical fingerprint scanner. Fig. 8 shows the software that recognizes the fingerprint as a valid one and returns its identification (ID) as the result. When the fingerprint recognition is successful, a system is allotted to the student and the student has to take that system.

Fig. 7. Fingerprint verification system.

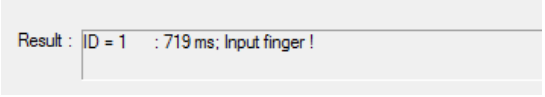

Fig. 8 .Result of fingerprint identification.

C. *Face Recognition*

Face recognition is the step after face detection. Here too, a face has to be detected and distinguished from the background. After face detection, the face has to be recognized to check if it is the actual student.

1) *Viola-Jones Face Detection*

The algorithm that is used here for the purpose of face detection is Viola-Jones Face Detection algorithm. It mainly consists of four stages: Haar features detection, finding the integral image, adaptive boosting (AdaBoost) to reduce the computational complexity and Cascade classifying the image using combinations of weak and strong classifiers so as to eliminate the chances of false rejections as much as possible. An example of face detection using this algorithm is shown in Fig. 9.

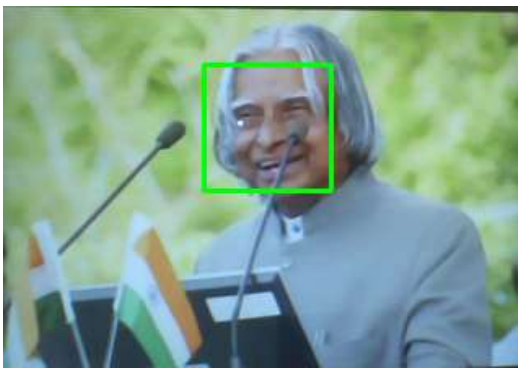

Fig. 9. Face Detection (an example).

2) *Local Binary Pattern Histogram (LBPH) Recognition*

Of methods like the Eigen Faces (based on Principal Component Analysis), Fisher Faces (based on Linear Discriminant Analysis) and LBPH, LBPH is chosen as it is more robust and focuses on important features of the face, rather than taking the entire face as a single entity [7,8].

LBPH is less affected by the pose variations and the light intensity variations. During an examination, pose variations and light intensity variations are inevitable, hence LBPH would be an appropriate face recognition algorithm. An example of face recognition using LBPH is shown in Fig. 10.

Fig. 10. Face Recognition (an example)

As shown in Fig. 11, a set of images of the face of the candidate is captured when fingerprint verification is done. This is stored as the dataset against which the face of the candidate is compared during the course of the examination.

Fig. 11. Dataset of the Face image captured when fingerprint is verified.

In Fig. 12, the registered candidate is shown taking the examination. When an unknown face is found to be in view for more than a minute, then the examination is paused, as shown in Fig. 13. Once the examination pauses, the alert message is sent to the higher authorities.

Fig. 12. Face recognition system recognizes the trained face and allows the examination to continue.

Fig. 13. Face recognition system does not recognize the untrained face and pauses the examination. The screen shows an alert

IV. Results and Discussions

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 a screen 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.

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)