DETECTION OF IMPERSONATION IN REMOTE ONLINE EXAMINATION

Shubha.G.Sanu[1], Pushpa.S.Tamase[2]
[1]Asst.Prof, Department of IS, G.I.T, Belagavi,
[2]Asst.Prof, Department of IS, G.I.T, Belagavi

Abstract
Online Examination faces many security threats. The threats are of two types, intrusive and non-intrusive. Non-intrusive is the prominent threat faced in remote online examinations. Collusion is a type of non-intrusive threat, where a student invites a third party for impersonation or assistance during the examination. Collusion is comparatively difficult to detect and prevent because of the lack of efficiency and integrity on the part of the external invigilator. So an efficient invigilation mechanism is the need of the hour to ensure the standard of examination and to maintain authentic conduct of examination. We propose to employ Facial Recognition using PCA (Principal Component Analysis) to build such system that overcomes this threat of collusion and perform live identification and authentication of candidate throughout the examination to avoid impersonation.
Keywords: Collusion, Facial Recognition, Impersonation, Online Examination, Principal Component Analysis..

I. INTRODUCTION

A 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 [1]. 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. Collusion is when the candidate invites any third party for impersonation or for aid/help the candidate in the examination.

Currently authentication of the user before taking up the examination is carried out using biometric authentication and manual verification of credentials by the invigilator. This process ensures authentication at entry level. 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.

This paper proposes an approach to overcome this disadvantage. Facial recognition with PCA is a simple approach that can embedded to the existing system to conduct dynamic authentication of the candidate. Candidate registration photograph is used for comparison with the picture recorded while the candidate enters the examination hall. 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.

This entire process is secured and conducted in those corresponding systems to avoid any intrusion and modification of crucial data

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 confirm the violation.

II. EXISTING SYSTEM

Existing system has an efficient identity check when the candidate appears for the examination by manual verification of credentials, biometrics, and image matching by the corresponding invigilator. But the system does not perform any check during the course of examination.

This lack of presence of a invigilating mechanism has led to increase of collusion. Lack of integrity of the invigilator also contributes to collusion.

III. PROPOSED SYSTEM

ARCHITECTURE—

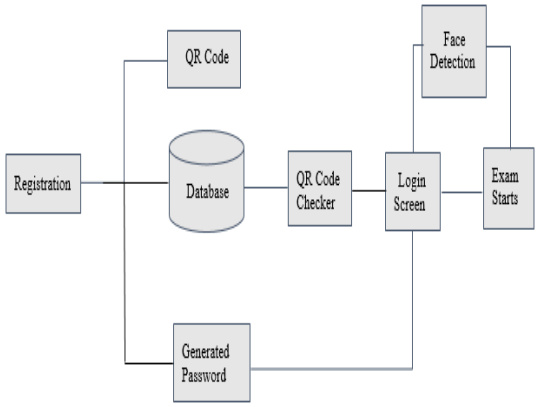

Fig.1. Architecture Diagram

IV. COMPONENTS

A Registration

Registration module involves registration for administrator and student. Administrator registration provides the admin with questionnaire framing facility and can view the students who registered for that corresponding examination.

Candidate is asked to register using necessary details and recent photograph. An unique QR code is generated for each candidate registered and is used for authentication of the candidate and generation of unique question set for that candidate.

B. Database

SQL database is used for storing and retrieving data. The database contains details of the candidates, administrators and the set of questions. These details are used for verification during login attempts by the administrator/candidate and for selection of set of questions.

C.QR Code

QR code (abbreviated from Quick Response Code) is the brand name for a type of matrix barcode (or two-dimensional barcode) first designed in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data.\

QR code gained popularity outside the intended automobile industry because of its quick readability and greater storage capacity than that of standard UPC barcodes. QR code is employed for various commercial and industry based applications such as product tracking, item identification, document management and marketing.

QR code has a square grid with white background on which a series of black squares are arranged, which can be read using any imaging device such as a camera and processed using Reed-Solomon error correction to interpret the image correctly without any noise or error. The data are extracted from the patterns formed by vertical and horizontal components of the image.

D.QR Code Scanner

One-dimensional barcodes were designed for reading by mechanically scanning using a narrow beam of light. QR code is detected by a 2-dimensional digital image sensor and then digitally analyzed by a programmed processor. The processor locates the three distinctive squares at the corners of the QR code. A smaller square at the last corner of the image is used to normalize the image for size, orientation and angle of viewing. The small dots throughout the QR image are then converted to binary numbers and validated with an error correcting algorithm.

E. Facial Recognition

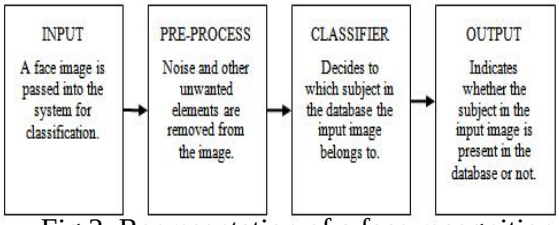

Fig.2. Representation of a face recognition system

Intensity is the main characteristic that should be used to distinguish human faces rather than chrominance. Intensity or grayscale representation is used in the recognition stage. This image is compressed using 2D-DCT for further processing [2][3]. The intensity value for each skin pixel is stored in this grayscale image. We use grayscale image because of the factor that skin color varies from human to human.

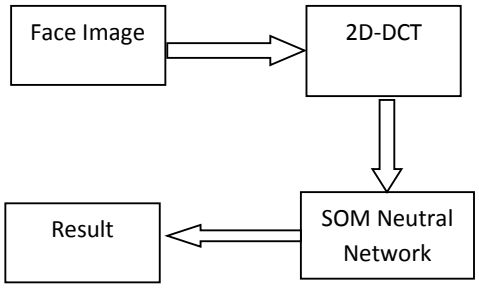

Fig.3. Technique for face recognition system

Fig.3 represents the technique for facial recognition system [4]. Each image is processed to form a 2D-DCT [5] and feature vectors are formed from the DCT (direct cosine transform) coefficients. SOM (self-organizing map) [6] [7] is an unsupervised learning technique. It is used to classify the vectors into groups. These groups are used to recognize if the subject in the input image is "present" or "not present" in the image database. If a match is found in the database then the best match image is displayed from the training database else the result displays that the subject is not found in the database.

E. Examination System

Examination system is a normal online examination system with facial recognition system integrated to it. Questions for the examination are randomly selected from a question pool that produces a unique pattern/set of question for the candidate.

V.PROCESS

Initially the process begins with the candidate registering for taking up the examination. Essential details such as name, age, and course are received from the candidate. In addition to this a recent photograph of the candidate is to be uploaded during registration. After successful registration a unique ID, password and a QR code is generated for each candidate. These credentials are used by the candidate while appearing for the examination. The QR code has a recorded pattern which indicates the pattern of questions for the candidate. These credentials are used for preliminary authentication of the user before taking up the examination.

In step 2, the candidate is recorded using a photograph device at the entrance of the examination center after successful authentication. This photograph is uploaded to the database and appended to the candidate's data. This photograph is used for comparison with the one that was uploaded during the registration process. This is next level of authentication to ensure that the candidate appearing is the one who enrolled for the examination. This second photograph is then stored in the database and the result of the comparison is logged in the central server.

In step 3, the candidate is required to scan their corresponding QR code on the system in which the candidate is going to take up the examination. After scanning the QR code the central server acknowledges the pattern in the code and selects the questions according to that pattern and displays those questions. Transparency is to be ensured during this process because the candidate should not feel that questions have been shuffled for each candidate.

In Step 4, during the examination period, the algorithm triggers a "image capture" signal to the system which invokes the photographic device connected to the system. The peripheral is activated when the candidate switches between questions because the probability of capturing the full face image without any inclination or distraction of the candidate face is very high only when the candidate is switching between questions.

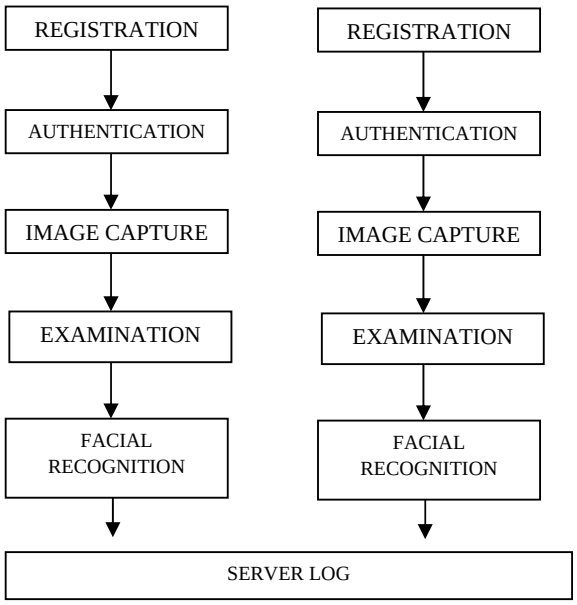

Fig 4. Impersonation detection process using facial recognition

In step 5, the captured image is compared with the photograph that was recorded during the candidate's entry into the examination center to detect violation. If the feature matching exceeds the mismatch threshold then the algorithm outputs mismatch and indicates violation to the central server and they are recorded in a log for that candidate.

If a violation alert is produced by the algorithm then the examination is paused and the invigilator and the center invigilation team is alerted and the examination is invalidated.

IV. ADVANTAGES

The advantages of employing facial recognition system to detect collusion are

- Easy to implement.
- Sophisticated authentication process.
- Higher accuracy.
- Affordable.
- Reduced effort on human factor.
- Reliability.

VII. APPLICATIONS

This concept can be applied not only in remote online examinations but also can be applied to all other online examinations to prevent these threats.

This system can also be applied to other examination systems to avoid impersonation in any examination. The ease and less expensive nature of the system makes it an affordable system in all examination systems.

VIII. REFERENCE

[1]. Abrar Ullah; Hannan Xiao; Trevor Barker 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) "A classification of threats to remote online examinations"

[2] A. Abdallah, M. Abou El-Nasr, and A. Lynn Abbott, "A New Face Detection Technique using 2D DCT and Self Organizing Feature Map" in Proc. of World Academy of Science, Engineering and Technology, Vol. 21, May 2007, pp. 15-19.

[3]. A.Ghadamyari, A A Safavi. "Self organizing Map(SOM) Neural network based on novel Fuzzy Wavelet for non linear function approximation " , 2nd International Conference on Control, Instrumentation and Automation(ICCIA), 2011.".

[4]. Jawad Nagi, Syed Khaleel Ahmed, Farrukh Nagi "A MATLAB based Face Recognition System using Image Processing and Neural Networks.

[5]. Derzu Omaia, Jankees V D, Leonardo V B,"2D=DCT Distance Based Face Recognition using a Reduced number of co-efficients", IEEE, XXII Brazilian Symposium on Computer Graphics and Image processing,2009.

[6]. Swati Jadon, Mahendra K, Yogesh R,"Face recognition using SOM neural network with Ddct facial feature extraction techniques", IEEE ICCSP-2015 conference 978-1-4799-80881-9/15.

[7]. P Abouzar, S Yousefi, S K Setarehdan, "Hybrid WT Based DCT Based face recognition",IEEE, ICSPC 2007.