Smart Examinee Authentication System using Fisherface Algorithm

Anjali Yadav[1], Surykant[2], Utkarsh Sharma[3], Sindhu Thakur[4], Samiksha Sengar[5]

[1,2,3,4,5]*Department of Computer Science and Engineering, Raj Kumar Goel Institute of Technology, Ghaziabad*

***Abstract* - In the quickly developing universe of Information and Communication Technology (ICT), verification of human appearances with least human intercession has a more prominent interest in different areas. As HFR (Human Face Recognition is a notable procedure for verifying clients or partners. Biometric as a predominant branch for check, HFR has its applications in video observing/observation frameworks, HCI. This paper is proposed to introduce a strategy for perceiving an Examinee utilizing the procedure called face acknowledgment wherein Python programming D-Lib and other related libraries/conditions are utilized. This model Biometric system requires an approval machine.**

The proposed work comprises two steps: enrollment and authentication. The enrollment process is done in two phases: online registration in which students /examinees feed their information according to the filled databases and face detection. An authentication image analysis process is carried out with the help of Fisherface algorithm which is used for further processing.

***Index Terms* - Biometric, Fisherface, face recognition, ANN, PCA, LDA.**

I.INTRODUCTION

The target of this paper is to introduce a model which outfits a simpler and easy to use human-machine connection to validate the Examinee by his facial highlights which are separated utilizing the photograph which he/she submitted during the enlistment interaction of the tests. A machine can distinguish and perceive an individual's face, bringing about the confirmation of the up-and-comer. A customized login page having the capacity to investigate client's access will be designed for the admin module with the highlights of facial acknowledgment.

The objective of this work is to introduce a bunch of Programs that can be subsequently bundled in an effectively convenient structure among the diverse processor designs, which we find in machines (PCs) today. It has gotten harder for face location considering some eccentric ascribes. For instance, changing highlights like eyeglasses and facial hair growth will have an impact for recognizing viability. Moreover, unmistakable points of lighting will follow the face and produce disparate brilliance on the face, which will hold the ID interaction. To create a code for right and certifiable facial acknowledgment to have proficient utilization of equipment, a well inbuilt library and a complete investigation of D-Lib stage was defined [7]. The task, overall, has a great deal of uses in different shifting manners utilizing face acknowledgment to confirm, notwithstanding, our extent of exploration is centered around utilizing the face acknowledgment to confirm the Examinee with insignificant human connection. This task centers around the communication of screen outlines acquired from the live video feed and deciding if the caught outline has a human face and afterward face-acknowledgement is set off after human face identification [9].

Information and Communication Technologies (ICTs) continue to grow at a rapid pace and have changed the way people live, work, and learn. The integration of ICT tools in education and training has created new ways of delivering, accessing, and processing useful knowledge, and has provided support to knowledge sharing between different actors and to lifelong learning. In addition, technological development and the growth of the Internet have resulted in the emergence of online learning as an important learning approach. Online-learning provides innovative methods for educating people. Moreover, the online-learning market is growing because of its many advantages over offline education. E-learning is also highly flexible, scalable, a fast-learning method, less expensive, and proven to be effective compared with traditional offline education. The three main drivers for the increasing global importance of online learning methods are:

- Movement toward a knowledge-based economy;
- Paradigm shift in education delivery;
- Technological developments and Internet growth.

The development of online learning mode and online assessment systems is increasing rapidly, both globally and locally, with many universities and corporations investing significant capital in online learning programs and initiatives. This growth is also seen in the report by Ambient Insight, which was published in 2010, indicating that the online learning market has reached US$ 27.1 billion in 2009 and will surpass $49.6 billion by 2014. The growth of the online-learning industry requires new services to ensure reliability and effectiveness of these systems, especially during the examinations process, by handling the issue of cheating in online examinations and identity theft. E-learning is prospering on global and local levels.

Online examination malpractices like cheating and identity theft should be considered, while the privacy of examinee data and more importantly, their images is guaranteed. The major problem that occurs in the examination system is malpractices. This is recognized due to the absence of a credible identity verification system for online and for offline examinations. To overcome the above problem researchers have focused on the use of artificial techniques and use of biometrics. In the past, work has been done on bad testing habits. ANN programming is used for similarity measures between trained and experimental features. Monitoring can be done using verification techniques. Image quality testing with a similarity detection process is used to detect fake biometrics. The biometric system must have variability, stability, compactness, performance, and acceptance and build resistance. On image quality of our real and fake users. Multimodal biometric is also performed where more than one biometric is grouped together and compared with existing data. Our program uses a face recognition system for automatic student visits to the study area.

The authentication of the online identity system is still using user / password mode. This mode cannot accurately identify the chosen ones when fraudsters are present, moreover the password may be Theft or forgotten. We therefore decide to use other authentication methods to improve the security of the online release system. In this study, a new method of applying facial recognition was introduced as an improved guarantee for e-Exam participants. An early warning will be generated to notify any suspicious movements of the system. Produces Web Application Programming Interface (API) authentication, image, and video with the same feature removal action. Nowadays, most computer-aided testing methods are tested on the Web and use a customer paradigm. Such methods often do not measure well and do not fully support features such as independent solution testing, dynamic content delivery, and network traffic. Mobile Agents technology has been developed rapidly and extensively as a useful paradigm to overcome the above limitations [8]. Web-based learning or e-learning is growing by the day. But the inspection system is always asked by the authority when it is done remotely. Questions arise about the inspector's accuracy and fairness during the test. In this paper a biometric verification and tracking system is suggested. Here iris recognition is used as a biometric verification tool. The proposed solution is cheaper and more efficient. This solution will help the supervisor to authorize the inspector and to track the inspector during the inspection. The use of biometrics for personal identification has many advantages because the tested features are part of personal information, in many cases, impossible to cheat, share or forget, such as passwords or PINs. The way a person speaks is one of those several factors that can be used for recognition. The term, often referred to as a biometric type of behavior, is a combination of a moral and ethical body. Biometric voice is an example of individual numbers, patterns, and rhythms of an individual's voice. The biometric of the voice or "voice printing," differs from person to person such as finger or palm print. Any authentication system that uses a voice channel during the authentication period can add biometric authentication to the process of higher levels of authenticity and security.

II. RELATED WORK

The Online Test Program has many benefits. Here are some benefits such as increased security, get rid of examination centers, reduced administrative burden, quicker to mark and issue results, more scalable, reduced examination cost, remote supervision and with proper time limit [1]. The Online Examination System is an exceptionally effective way to change our old traditional and paper tests into online and paperless mode. It made the test taking system much easier. Applicants can go through with the trial using any desktop, laptop, or mobile device with a browser. One main reason why applicant prefer Online Test Program is instant evaluation for faster results. They do not have to wait too much for their results. Proof of authenticity can be divided into three types:

2.1 Authenticity: Authentication is a widely used system in online Assessments. Users must disclose his or her identity. User ID, password, challenge questions and any kind of verification are often used. In Knowledge-Based Verification, applicants can share their login details to third parties to increase their marks. It is one of the significant issues of Knowledge Based Authentication.

2.2 Manual Verification: Authentication is based on the user's personal belongings such as memory cards, smart cards, dongles, and keys. Manual certification can be useful if tests are taken at a specified location such as university labs or accredited institutions, etc. If the test is performed in an unregulated area, it is pointless as it is possible that the token was stolen or doubled by complex means.

2.3 Biometric authentication: Biometric is a security process which compares a person’s characteristics through unique biological traits such as face characteristics, retina and fingerprints. It is used to verify a user’s identity when that user accesses his or her account. Biometric-based authentication is more secure because this data is unique for every individual user [2]. User identification depends on physical or behavioral factors. Behavioral factors are considered to be learned movements. Physical features include face (2D / 3D facial images, IR facial thermo grams), hand (fingerprints, finger length, palm print, IR hand thermo grams), eye (retina and iris), ear, signature, and DNA (Deoxyribonucleic acid). Some of the most used features are: voice, fingerprints, face, signature, key, and heartbeat. This type of authentication system consists of two phases: registration (user biometric detection) and authentication (by comparing recorded data into a stored template). Biometrics is very safe but not accepted due to violations of user privacy. The saved template can be used for malicious activities [3].

Other strategies now used to overcome unpleasant habits or unauthorized access to information:

2.3.1 Safe Browser: As students are giving tests from different remote locations which make supervision difficult. The supervisor could not remain physically present to monitor the students all the time which increase the chances of cheating or any kind of malpractices during Online Examinations. The user is allowed to access only the exam window other than this will block the other tabs. Secure Browser Technology prevents the students from opening any other window or switching between different tabs while the online scanning process is in progress. Users are only allowed access to the test window. This features also blocks access to shortcuts like cut, copy and paste. It can also stop the software running in the background [4].

2.3.2 Remote Testing: In the Remote Proctoring system, the administrator does not have to be present at the test center. The test can be extended to other remote locations. Candidates can write a test in a far location.

It involves three main processes:

- Photography
- Video streaming
- Screen Capture
- Performing Voice Proctoring

This enables the director to view the page the student is on to avoid any kind of abuse.

2.3.3 Audit Testing: A detailed login area where tasks such as Login, Logout, Exam Access, Question Navigation, Answers Responses, etc. You can the detailed activity of the candidates. It also records details of activities like Section Changes, Internet Speed. We can even track the exact location of the user during online exam activity by using geotagging technique.

2.3.4 Authentication and authentication based on IP: The concept of IP-based authentication and Authentication means that access to and operation of the test system is limited or limited to a specific number of IP addresses.

In the case of Admin login, you may have IP based Authentication so that users trying to sign in from a specific IP are allowed access to the application. This allows access to only specific IP addresses and ensures complete test security [5].

III. PROPOSED SYSTEM

Our main goal is to develop an automated fraud detection system for Examination. Fisherfaces algorithm extracts principle components that separate one individual from another. So, now an individual's features cannot dominate another person's features. The Fisherface method is based on the same principle like the Eigenfaces method. The purpose of this approach is to reduce the image size of a high-resolution image based on discriminatory analysis LDA (Linear Discriminant Analysis) instead of PCA (PRINCIPAL COMPONENT ANALYSIS) process. Linear Discriminant Analysis performed to reduce the magnitude of a certain level and was developed by the great mathematician Sir RA Fisher. He successfully used it to classify flowers in his 1936 paper on the use of multiple scales in tax problems. To obtain a combination of features that differentiate between classes Linear Discriminant Analysis increases the ratio of values between classes to within, without increasing the overall spread. The LDA process is widely used in reducing the size and visibility of the face. PCA is an unregulated process, while LDA is a supervised learning method and uses data. Algorithmic description of the Fisherfaces method [6]: Let X be a random vector with samples taken from classes c:

$$X = \{X_1, X_2, \ldots, X_c\}$$

$$X_i = \{x_1, x_2, \ldots, x_n\}$$

Scattered SB and S_ {W} matrices are calculated as[10]:

$$S_B = \sum_{i=1}^{c} N_i(\mu_i - \mu)(\mu_i - \mu)^T$$

$$S_W = \sum_{i=1}^{c} \sum_{x_j \in X_i} (x_j - \mu_i)(x_j - \mu_i)^T$$

When μ means the total value:

$$\mu = \frac{1}{N} \sum_{i=1}^{N} x_i$$

And μ_i is the meaning of i ∈ {1,…, c}:

$$\mu_i = \frac{1}{|X_i|} \sum_{x_j \in X_i} x_j$$

Fisher's classic algorithm now looks at W predictions, which increase the classification criterion:

$$W_{opt} = \arg\max_W \frac{|W^T S_B W|}{|W^T S_W W|}$$

There is one problem left to solve: SW level is large (N - c), with N samples and c classes. In pattern recognition problems the number of N samples is always smaller than the input data rate (number of pixels), so the scatter matrix SW is singular (see [172]). In [14] this was resolved by conducting Principal Component Analysis data and displaying space samples (N - c) -dimensional. Linear Discriminant Analysis was then performed on reduced data because SW is no longer single [6].

The performance problem can be rewritten as:

$$W_{pca} = \arg\max_W |W^T S_T W|$$

$$W_{fld} = \arg\max_W \frac{|W^T W_{pca}^T S_B W_{pca} W|}{|W^T W_{pca}^T S_W W_{pca} W|}$$

Transformation matrix W, which makes a sample in the space (c - 1) -dimensional and is provided by:

$$W = W_{fld}^T W_{pca}^T$$

Precisely, FisherFaces face recognizer algorithm extracts principal features that differentiate one person from the others. In that sense, an individual's features do not dominate over the others.

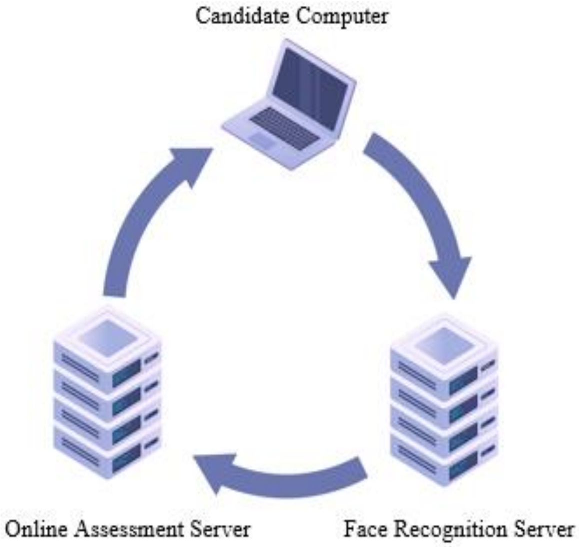

Fig. 1 Proposed system

IV. ALGORITHM

4.1 Retrieve data:

Collection of data is done in the form of face images. Collection can be done using photographs already saved or from a webcam. Face must be fully visible and must be facing forward [11].

4.2 Image Processing:

Preprocessing stage: Getting images using camera or saved images and conversion from RGB to grayscale. Image data is divided into training and test data.

Processing stage: Fisherface method will be applied to generate feature vector of facial image data used by system and then to match vector of traits of training image with vector characteristic of test image using the Euclidean distance formula [11].

4.3 Feature generation:

Features of the faces are extracted.

4.4 Recognition Step:

The next stage is image recognition process, after the training is done. The goal is to successfully recognize the test image.

If training image is the same as the testing image:

In this case, the system can successfully identify the test image correctly up to 100%.

If training image is different from the testing image:

The test image and the training image must come from the image of the same person's face. System can now successfully identify the test image correctly up to 90%.

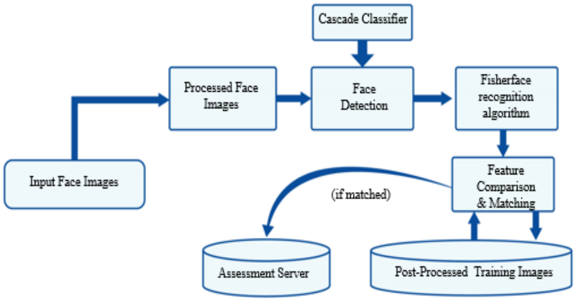

Fig. 2 Flowchart of algorithm

V. CONCLUSION AND FUTURE WORKS

In this paper, we effectively used the Python D-Lib and PCA/Fisherface algorithm and could obtain the satisfactory result in the perspective of recognition and identification for the candidate who is taking the e-exam/online exam. The main goal is to ensure candidate identity in terms of face recognition and identification. In Future we should work upon a fully automated audio/video proctoring system in the configuration of desktop applications and also for mobile devices like android/iOS.

REFERENCES

[1] https://www.testreach.com/benefits-of-online-assessment-testreach.html.

[2] https://www.jumio.com/what-is-biometric-authentication/.

[3] https://recfaces.com/articles/types-of-biometrics.

[4] https://onlineexamhelp.eklavvya.in/what-is-secure-browser-for-online-exams/.

[5] https://blog.epravesh.com/top-5-techniques-to-make-online-examination-system-secure.

[6] https://docs.opencv.org/3.4/da/d60/tutorial_face_main.html.

[7] Fayaz Ahmad Fayaz, Shakir Mohi-ud-din, Irtiza Batool, Satinder Kaur, Mamoon Rashid, “Novel Face Recognition Based Examinee Authentication System using Python D-Lib” Fifth International Conference on Image Information Processing (ICIIP), 2019.

[8] Mie MieThetThwin. "Mobile agent based online examination system", 2008 5th International Conference on Electrical Engineering/Electronics Computer Telecommunications and Information Technology, 05/2008.

[9] S. Yoo, D.-G. Sim, Y.-G. Kim, and R.-H. Park, “Performance Comparison of Principal Component Analysis-Based Face Recognition in Color Space,” Advanced Biometric Technologies, Sep. 2011.

[10] D. L. Swets, and J. Weng, "Using Discriminant Eigenfeatures for Image Retrieval," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 18, no. 8, pp. 831-836, August 1996.

[11] Aakriti Tyagi, Smita Deshmukh, Gayatri Dindokar, Shraddha Kale, Mayur Karale, Bhagyashree Dhakulkar, “IoT Based Smart Home Automation System” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2020.