International Journal of Engineering Research and Applications *www.ijera.com*
ISSN: 2248-9622, pp. 01-11

RESEARCH ARTICLE OPEN ACCESS

A Review Paper on Examinee Authentication System using various Biometric Methods

Suryakant[1], Utkarsh Sharma[2], Sindhu Thakur[3], Samiksha Sengar[4]
Department of Computer Science and Engineering,
Raj Kumar Goel Institute of Technology, Ghaziabad

ABSTRACT
One of the major problems faced in online examination conduction is candidate impersonation. With the developing technology every part of the examination process has been automated, but the candidate verification processes are obsolete. These days biometric based authentication is one of the most opted methods. This paper presents a comparative analysis of various face detection methods that can be used for candidate's verification. 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 Fisher face algorithm which is used for further processing.

I. INTRODUCTION

Nowadays, online learning and online examination systems have become important components in the education and training domains. Several countries are constantly working to overcome the Knowledge Divide. Through education and training, countries are able to develop the skills of their citizens, consequently bridging the Knowledge Divide within the country and with more developed ones. Success in the Knowledge Economy is based on qualified and skilled citizens, therefore effective education and training systems are required.Parallelly, 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. In Saudi Arabia, the government is focusing on the education sector in general and e-learning in particular in responding to the increasing number of male and female students enrolled in educational institutions. Many universities in Saudi Arabia have already implemented this online learning system and are offering distance learning programs for the desired courses and degrees. Hence, ensuring online learning systems, especially during examinations, are highly crucial. 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 also for offline examinations. In order 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. Iris recognition method based on natural open eyes. In order to see exactly the similarities, you have to remove these items using pre-image processing. Processing of the image of the Iris includes the location of the iris, inserting the eyelid, finding the foreskin and getting used to it. Image quality testing with a similarity detection process is used to detect fake biometrics. The biometric system must have variability, stability, compactness, performance, acceptance and build resistance.On image quality of our real and fake user. 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. Face recognition is an important part of biometrics. In biometrics the basic human characteristics are compared with existing data and it depends on the result of identifying the person being compared. Face features are extracted and applied by active algorithms and some changes are made to improve existing algorithm models.In many articles, there are advantages and disadvantages to online tests. The main advantage is that it can be conducted for the nominees and the test answers can be done automatically for the MCQ questions and other essay type questions can be assessed manually or systematically, depending on the type of questions and requirements. Disadvantages of e-examination inability to input power. There are a number of methods used in these tests, in enrolling students and presenting questions, to test students' knowledge and skills.However, for a limited time, a baptismal candidate cannot fully trust in references or support. Another downside is that 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 forgotten. We therefore decide to use other authentication methods to improve the security of the online release system. In all biometric indicators, fingerprints have one of the highest levels of reliability and are widely used. In the Automatic Fingerprint Identification System (AFIS), the aim is to identify the probe fingerprint similarities in a database of registered printers, which may number millions. The split is used in AFIS to reduce the size of the search space and take fingerprints of the same category before attempting to match exactly. The ID is used in AFIS to indicate whether these fingerprints are the same or not.The platform uses a combination of biometric finger verification and dynamic encryption techniques. Although the technology used is quite sophisticated, making sure that baptism candidates who respond to trials are good people is a challenge and a challenge. 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 [6]. The mobile agent is free to navigate between strangers on the network. Created in a single execution location, it can move its status and code to another network location, where it is initially activated. The mobile agent will have a trip, which is a list of nodes they need to visit, along with. Mobile agents offer a number of reasons, such as reducing network load, overcoming network latency, consolidating contracts, acting independently, and adapting powerfully, naturally. In addition, applications with complex components that are complex and flexible and distributed locally can benefit greatly from using mobile agent design. This program aims to solve the problems of the test system and to change the existing paper-based system [6].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 mainly 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 iris of each eye is different. There are no two identical irises in their mathematical detail, not even between the same twins or between his left and right eyes. Unlike the retina, however, it appears at a distance, allowing for easy image detection without penetration. The sensor device used to detect iris features is a digital camera, very convenient for the user. The iris remains stable throughout human life, preventing rare diseases or trauma. The irregular patterns of the iris are similar to the intricate “human barcode”, created by the bound fabric of connecting tissues and other visual elements. In the proposed format this "personal barcode" is used as a password during testing, to ensure the authenticity

of the actual students. The iris recognition system consists of an automatic separation system based on the Hough transform, and is capable of locating a circular area and a student region, including eyebrows and eyelashes, and display. The iris region extracted and sorted into a rectangular box with a constant size to account for the inconsistency of thought. Finally, the Gabor filter here is used to insert a unique iris pattern into a biometric template[3]. An analogy is used between the two grades of irises hamming. 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 different factors that can be used for recognition. The term, often referred to as a biometric type of behavior, is actually 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 is able to add biometric authentication to the process of higher levels of authenticity and security. Voice verification technology uses a variety of human voice features to discriminate between speakers. Speech recognition allows you to provide input into the voice app.

II. RELATED WORK

The Online Test Program is a state-of-the-art technology to simplify test tasks such as defining test patterns by question banks, defining test time, targeted / specific query categories, computer-based computer or mobile tests.The Online Examination System is an inexpensive, awesome way to turn traditional and paper tests into online and paperless mode. Applicants can appear in the trial using any desktop, laptop, or mobile device with a browser. Test results can be done quickly with the type of questionnaire.Election verification was a major procedural problem. Proof of authenticity can be divided into three types:

1. Authenticity: Authentication is a widely used system. Users must disclose his or her identity to access the service. User ID, password and challenge questions are often used. In the event of Knowledge-Based Verification students can share their login details to third parties to increase their marks. It is one of the major problems of Knowledge Based Authentication.

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 performed at a specific location such as university labs or accredited institutions, etc. In the unlikely event that the test is performed in an unregulated area it is useless as it is possible that the token was stolen or doubled by complex means.

3. Biometric-based authentication: Biometric is a fast technology used to improve security in many types of applications. 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 thermograms), hand (fingerprints, hand geometry, palm print, IR hand thermograms), eye (retina and -iris), ear, skin, smell, teeth and DNA. Some of the most commonly used features are: voice, fingerprints, face, signature, mouse movement, 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 are very safe but not widely accepted due to violations of user privacy. The saved template can be used for malicious activities. Other authentication methods can help with the authentication process such as location, time stamp, IP address and time of trying to access.

Other strategies now used to overcome bad habits or unauthorized access to information:
1. Safe Browser: Secure Browser Technology prevents users from opening any other window while the online scanning process is in progress. Users are only allowed access to the test window. Access to copy keyboard shortcuts, attachments and screen shots is completely blocked.

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.

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.

3. Audit Testing: A detailed login area where tasks such as Login, Logout, Exam Access, Query Navigation, Answers, etc.

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.

Proposed Solution/System

Voice authentication
Since the user voice is the only verified business authorization, the proposed method creates voice templates with the user's initial registration and also verifies the user with the recognition of the generated voice template. After recognition and authentication, the process proceeds to the next stage, e.g. the question answer module. Therefore, the proposed system can be divided into the following sections:

Voice Recognition:
Speech recognition is a process in which a computer (or other type of machine) identifies spoken words. Basically, it means talking to your computer, and knowing exactly what you are saying. A voice or speech recognition is a machine or program that accepts and interprets a call, or understands and executes spoken commands. section, the following steps must be followed:
i) Initially, we should provide user details such as input by the voice prompted by the system.
ii) The program will then generate a ".wav" file and the generated file will be stored in a database for future reference.
iii) During user login, the user is required to provide the same information provided during registration and the system compares the recorded voice with that stored in the database. If both are compatible, the user logs in successfully, if not[4].

Comparing voice recording:
One can easily recognize a familiar word. However, getting a computer to distinguish a word from others is a daunting task, since the magnitude of the problem lies in the fact that it is almost impossible to pronounce the word in the same way on two separate occasions. a person's expression of how quickly the word is spoken, emphasizes different parts of the word, and so on. In addition, suppose the word can be pronounced the same way on different occasions, and then we are left with another major problem[4], in order to analyze two audio files in a timeline, the recording will need to be properly aligned so that both recordings begin at the same time.We start comparing by storing two words in .wav files. Then we edit both signals and try to match them. Comparison made here by producing wav files by sampling by calculating its Fourier conversion. Next, we adjust its power output and reduce it to recreate the energy spectrum by variations such as noise and peaks to be standardized resulting in We use mathematical functions, compound and edit measurements of electricity that we often compare to two voices that give us the results we want.

Voice authentication:
To ensure continuous voice analysis and continuous signal performance based on DFT, the Fast Fourier Transform (FFT) method is adopted. Fourier transform transformer (FFT) is an efficient algorithm for dynamic calculation of Fourier transform (DFT) and its inverse. Fast Fourier Transform (FFT), the fastest mathematical algorithm. FFT eliminates unwanted statistics in Fourier Transform and is therefore much muchspeedier[4]. FFT is used to process speech to detect spectra in complex sounds. In the speech analysis, the FFT converts speech, which is in the time zone, has gone to the frequency range. Thanks to Fourier it has developed mathematical concepts, leading to FFT, which is very important in voiceprint technology. In the context of Fast Fourier transform algorithms, the butterfly is part of a calculation that combines the effects of small Fourier transformations (DFTs) into larger DFT, or vice versa. (breaking the main DFT into subtransforms).

Iris visibility
With the recognition of Iris, the first test was the generation of iris patterns[3]. The second test confirms the uniqueness of iris patterns. Examining the uniqueness of iris patterns is important, because the complete system relies on iris patterns from different eyes to be completely independent.

Generation Iris Pattern:
In this process, the goal is to determine the iris and student boundaries. After that you know exactly where the iris is, the removal of the iris pattern is made easier. The Haugh circle is used to modify circular detection. Prior to application Haugh modified the outer edge of the iris found. Canny's operator with a certain limit value is used[3] To determine the internal circle of the

cannabis limit value is selected according to size. If the iris is black the lower border is used to mark the inner circle. If the iris is simple the maximum limit is applied After finding the iris, a feature removal can be performed. The iris should be opened for sampling and receive an information signal that will be used to construct the iris template in binary form.

Code comparisons between Iris templates:

The Iris code is compared to the iris code stored in the source folder corresponding to the given Student Identification Number.Iris comparisons are based on Daugman's algorithm. To compare two irises, the algorithm incorporates iris templates, hides areas that do not have valid iris data (light, eyelashes, eyelashes, etc.) and makes small comparisons of unspecified template regions, including Hamming distance[3]. Grade 0 shows the perfect match, and grade 0.5 shows the completely random match of bits.Grade 1 corresponds to one iris which is a negative image of another.To determine if two irises are the same, we use the boundary range: samples with a distance below the threshold were taken from the same user, while samples with higher distances are thought to come from different users.

Image Acquisition and Tracking System:

Web based Graphical User Interface, specially designed for image capture is used for real-time photography. A standard webcam is used for photography and iris extraction. Eventually an online system was created for automatic tracking, which could automatically take a student's photo without notifying him. The level and position are automatically adjusted and the whole image is traced and the process described above is targeted to the user.

Face recognition

Face recognition technology works by scanning a person's face against a stored image.By face recognition system is a program that records prominent facial features and stores the template on the server. monitoring in the testing system. Fraud regarding hall tickets and the creation of an automated system of impersonation or checking of hall tickets using photographic processing methods. online testing programs. Sometimes face recognition systems are used for authentication and default presence programs. The solution to this problem is a test system designed based on face detection and verification technologies that incorporate security capabilities for testing and accuracy.

Three basic steps are used to improve the firmness of the face: (1) facial recognition, (2) feature removal, and (3) facial recognition. Face detection is used to detect and retrieve a person's face image obtained by the system. The element removal step is used to remove the vectors of the features of any human face in the first place. Finally, the face recognition step incorporates features extracted from a person's face to compare it with all the details of the template face information to determine a person's facial identity.

Face detection: The process of facial recognition begins with the making of a person's face in a particular image. The purpose of this step is to determine whether the inserted image contains a human face or not. Variations in brightness and appearance of the face may prevent proper face detection. Many techniques used to obtain and obtain a photograph of a human face, for example, Viola-Jones Detector, Gradient Focus Gradient (HOG), and key object analysis (PCA).

Feature removal: The main function of this step is to remove the features of the facial images found in the acquisition step.Many techniques include removing the shape of the mouth, eyes, or nose to identify the face using size and size. HOG, Eigenface, Independent Component Analysis (ICA), Equal Discrimination Analysis (LDA), Haar wavelets, and binary location pattern (LBP) techniques are widely used to exclude facial features.

Face recognition: In this step it looks at the features that have been released in the background during the feature removal step and compares them with known faces stored in a particular database. There are two common uses for face recognition verification and validation, in the face-to-face screening test compared to a face-to-face test that aims to determine the potential match during the face-to-face verification test compared to known faces in the database to decide acceptance or rejection. Correlation filters (CFs), convolutional neural network (CNN), and close neighbors k.

Separation of face recognition system

While people can see faces without much effort, facial recognition is a challenging problem to see a pattern on a computer. Compared to other biometric systems such as asiris, voice, or finger recognition systems, the face recognition system is less efficient and more reliable. Face recognition programs attempt to identify a person's face, which is three-dimensional and varies in appearance and facial expressions, based on its two-dimensional image. benefits. Depending on the acquisition and recognition methods, face recognition systems distinguish three modes: (1) local, (2) complete, and (3) hybrid methods. The first method is categorized according to certain facial features, not looking at

the whole face. The second method uses all faces as input data and projectiles into a small area or integration plane. The third method uses local and international features to improve the accuracy of facial recognition.

Local Approaches

In the context of facial recognition, local methods address only certain facial features. They are very sensitive to facial expressions, certain expressions, and positions[5]. The main purpose of these methods is to find different features. Local routes are further divided into two categories:

(1)Local appearance-based techniques: They are used to extract local features, and the image of the face is divided into smaller regions. It is a geometric method, also called an element or process of analysis. Local appearance-based techniques focus on sensitive areas of the face such as the nose, mouth and eyes to produce more detail. In addition, these techniques describe local features in the direction of pixels, histograms, geometric structures, and compound planes.

● Local Binary Pattern (LBP) is a picture operator used to convert images into identical members. LBP is a widely used operator for image analysis and various computer viewing functions. Adaptability to the LBP operator has made LBP a success in many computer-aided programming and adapted to the need for a program.

● A histogram of targeted gradients (HOG) is one of the best definitions used for structure and line definition. The HOG process can define facial contours using a straight edge distribution or gradient light intensity. The process of this process is done by sharing the whole image of the face to the cells (sub-region or area); a histogram of the direction of the pixel edge or cell gradients in each cell; and, finally, histograms of all cells combined to extract a feature of the facial image.

Algorithmic description of the LBPH method:

A more official description of the LBP provider can be provided as:

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} 2^p s(i_p - i_c)$$

and (xc, yc) as a powerful middle pixel ic; and on the pixel power of the neighbor. s signal function defined as:

$$s(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{else} \end{cases}$$

This description enables you to capture well-written details in photos.In fact, the authors have been able to compete with the state of the art effects of texture classification. Soon after the publication of the operator it became known that the fixed location failed to enter the details with different details on the scale. The operator is therefore extended to use the variable location in [2]. The idea is to align the number of neighbors indiscriminately with a dynamic radio circle, which allows you to capture the following locations:

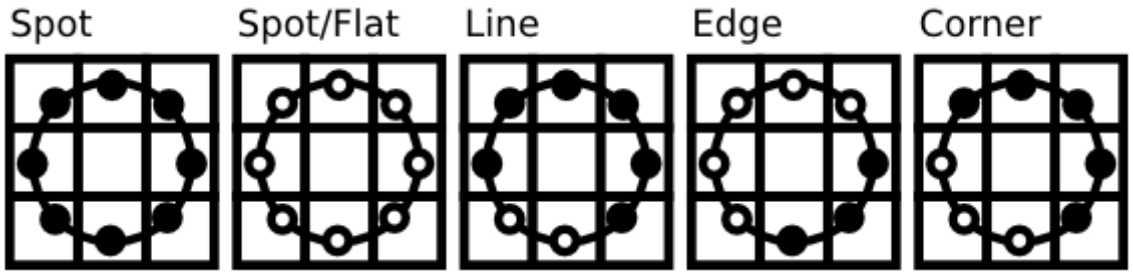

Fig.1: LBP Dynamic Radio circle

With a given Point (xc, yc) a neighbor's position (xp, yp), p∈P can be calculated by:

$$x_p = x_c + R\cos(\frac{2\pi p}{P})$$

$$y_p = y_c - R\sin(\frac{2\pi p}{P})$$

Where R is the circumference of the circle and P is the number of sample points [7].

The operator is an extension to the original LBP codes, so it is sometimes called Extended LBP (also called Circular LBP). If a point connection to a circle does not match the image link, a point is entered. Computer science has a host of clever translation schemes, the launch of OpenCV makes two translations [7]:

$$f(x,y) \approx [\,1-x \quad x\,] \begin{bmatrix} f(0,0) & f(0,1) \\ f(1,0) & f(1,1) \end{bmatrix} \Big|$$

By definition the LBP operator is stronger compared to the conversion of a larger gray scale. We can easily confirm this by looking at the LBP image of the manipulated image (so you can see what the LBP image looks like)[2]:

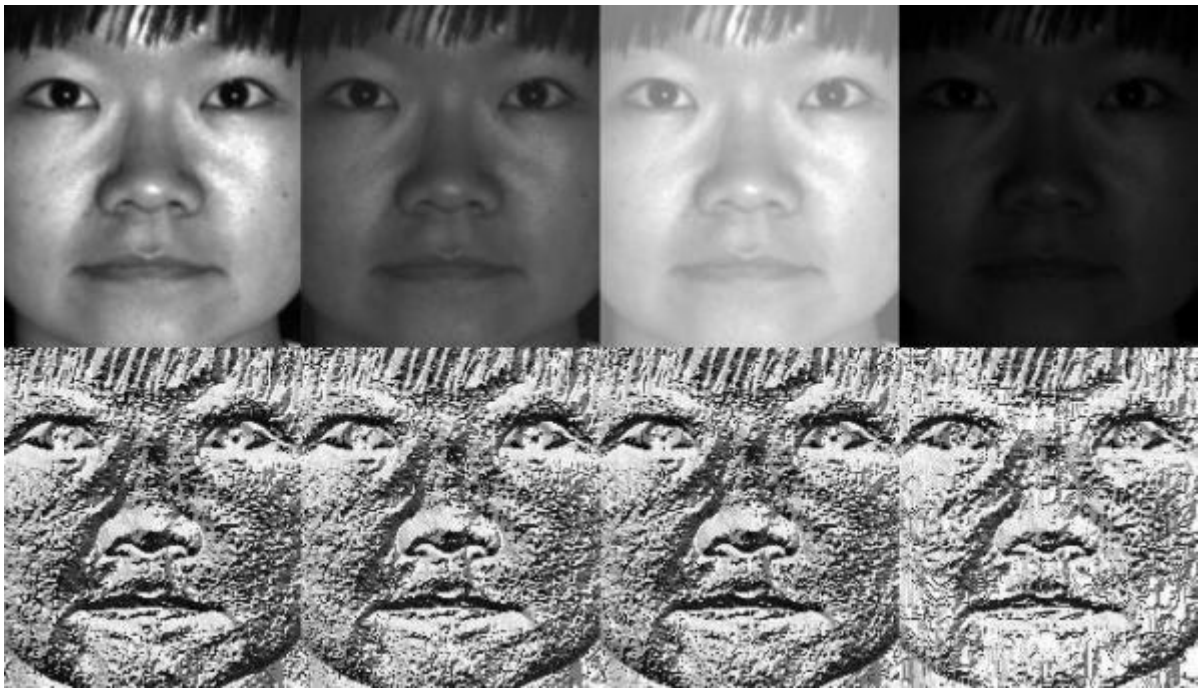

Fig.2: LBP modified image to grayscale

(2) Key point-based strategies: Key-based strategies are used to find interesting points in a facial image, after which the elements for these points are removed. According to some geometric details of the face (e.g., the distance between the eyes, the width of the head). The second step focuses on the display of information accompanied by the features of the key points of the face image.

Flexible Flexible Scale Scale (SIFT): SIFT is an algorithm used to locate and define local image attributes. This algorithm is widely used to link two images by their local descriptions, which contain details to create similarities between them. The main idea of the SIFT definition is to convert an image into a presentation made up of points of interest. It is widely used today and is fast, which is very important in real-time use, but one of its disadvantages is the critical point time algorithm. , and the definition of a point of view.

The fast dynamic features (SURF) SURF process is inspired by SIFT, but it uses wavelets and Hessian resolution measurements to achieve better performance repetition, contrast, and durability compared to the SIFT definition. The main advantage of SURF performance time, which is less than that used by the SIFT adjective To obtain feature points, SURF seeks to obtain the maximum size of the Hessian matrix using integrated images to significantly reduce processing time.

Holistic Approach

Key point-based strategies: Key-based strategies are used to find interesting points in a facial image, after which the features for these points are removed. According to some geometric details of the face (e.g., the distance between the eyes, the width of the head). The second step focuses on the display of information accompanied by the features of the key points of the face image.

- Scale invariant feature transform (SIFT): SIFT is an algorithm used to locate and define local image attributes. This algorithm is widely used to link two images by their local descriptions, which contain details to create similarities between them. The main idea of the SIFT definition is to convert an image into a presentation made up of points of interest. It is widely used today and is fast, which is very important in real-time use, but one of its disadvantages is the critical point time algorithm. , and the definition of a point of view[5].

- Speeded-up robust features (SURF) SURF process is inspired by SIFT, but it uses wavelets and Hessian resolution measurements to achieve better performance repetition, contrast, and durability compared to the SIFT definition. The main advantage of SURF performance time, which is less than that used by the SIFT adjective[5] To obtain feature points, SURF seeks to obtain the maximum size of the Hessian matrix using integrated images to significantly reduce processing time.

Algorithmic description of the Eigenfaces method:

Let X = {x1, x2,…, xn} be a random vector with xi∈Rd recognition.
1.Compute the meaning of μ

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

2.Count the Covariance Matrix S

$$S = \frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)(x_i - \mu)^{T_i}$$

3.Compute the eigenvalues λi and eigenvectors vi of S

$$Sv_i = \lambda_i v_i, i = 1, 2, \ldots, n$$

4. Order eigenvectors decrease according to their statistics. The main elements of k are the eigenvectors corresponding to the largest eigenvalues. The key elements of the visible vector x are provided by:

$$y = W^T(x - \mu)$$

where $W = (v_1, v_2, \ldots, v_k)$.
PCA reconstruction is provided by:

$$x = Wy + \mu$$

where $W = (v_1, v_2, \ldots, v_k)$

Eigenfaces approach and create face recognition with:

- Incorporating all training samples into the PCA subspace.
- Inserting a query image into the PCA subspace.
- Find the nearest neighbor between the proposed training images and the questionnaire that emerged.

However, there is one problem left to solve. Suppose we are given 400 image sizes per 100 × 100 pixel. Key Analysis analyzes the matrix of covariance S = XXT, where size (X) = 10000 × 400 in our example. You will end up with a matrix of 10000 × 10000, about 0.8GB. Solving this problem is not possible, so we will have to use a strategy. From your algebraic line studies you know that the M × N matrix with M> N can have e val 1 in non-zero eigenvalues. It is therefore possible to take the decay of eigenvalue S = XTX in size N × N instead:

$$X^T X v_i = \lambda_i vi$$

then find the original eigenvectors of S = XXT with the left-hand multiplication of the data matrix:

$$XX^T(Xv_i) = \lambda_i(Xv_i)$$

Emerging orienters of orthogonal eigenvectors, to find orthonormal eigenvectors need to be made standard at unit length.

- Fisherface (LDA): The Fisherface method is based on the same principle similar to the Eigenfaces method. The purpose of this approach is to reduce the image size of a high-resolution image based on discriminatory analysis (LDA) instead of PCA 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 [1]. PCA is an unregulated process, while LDA is a supervised learning method and uses data.

Algorithmic description of the Fisherfaces method [2]:
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:

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

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

When μ means the total value:

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

And μi 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 almost 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.
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:

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

● Independent component analysis (ICA): The ICA technique is used for the calculation of the basic vectors of a given space. The goal is to separate independent sources from a mixed-signal. Unlike PCA (Principal Component Analysis) which focuses on maximizing the variance, the ICA (Independent Component Analysis) focuses on independence, i.e., independent components. ICA represents the data in terms of statistically independent variables due to which we obtain greater efficiency. ICA provides more powerful data than PCA.

Nonlinear Techniques

● Kernel PCA: It is an improved method of PCA, which uses kernel method techniques. Kernel PCA computes the Eigenvectors of the kernel matrix, while PCA computes the covariance matrix. Kernel PCA uses techniques of kernel function which helps to project dataset into high-dimensional feature space.● Kernel linear discriminant analysis (KDA): the KLDA technique is a kernel extension of the linear LDA technique, within the same kernel extension of PCA[5]. There are many

● Evolutionary weighted principal component analysis.
● Kernelized Maximum average margin criterion (KMAMC), SVM, and kernel Fisher Discriminant analysis.
● Wavelet transform (WT), radon transform (RT), and cellular neural networks.
● PCA, local Gabor binary pattern histogram sequence (LGBPHS), and GABOR wavelets: It is a computationally efficient hybrid face recognition system that employs both holistic and local features. The PCA technique is used to lower the dimensionality. Then, the LGBPHS technique describes a face by combining the LBP operator and the Gabor wavelet transforms. It reduces the complexity caused by the Gabor filters.
● PCA and Fisher linear discriminant (FLD): It is a novel hybrid technique for face representation and recognition, which exploits both local and subspace features. To extract the local features, the image we have given is first divided into a sub-area, and then global features are taken out from the whole image.
● (GW-LDA) Gabor wavelet and linear discriminant analysis: GW-LDA is a hybrid approach that combine the Gabor wavelet (GW) and linear discriminant analysis (LDA) for face recognition. The grayscale face image refers to a black and white face image which reduced in dimension. Then the grayscale face image has convolved with a bank of Gabor filters with varying orientation and scales. After that, a subspace technique 2D-LDA is used to maximize the inter-class space and reduce the intraclass space. To classify and recognize the test face image, the k-nearest neighbor (k-NN) classifier is used. The test face image is then compared with each training set features to complete the recognition task. Hence, the result shows how this approach is strong and stable in different conditions.

Result/Experiment or Performance

Face recognition system has become popular in the past decades who have changed our lifestyle completely. In recent times, we are using various types of recognition systems everywhere to ease our life. Based on facial information, we can develop face recognition systems by using different techniques. The proposed intelligent based examination is implemented in such a way that it can be used online and verified for accuracy.

Two surveys were carried out. The first survey targeted students' reliability on e-exam to use, and the second targeted on face recognition as additional security to enhance the previous e-exam schemes. The first was to know how trustworthy is the proposed system and to identify if face recognition should be accepted in an e-exam scheme

as effective to capture any student intending to cheat or be replaced by another student during exams. However, e-exam candidate (N=29) was delivered using explanation of the proposed solution and were asked to rate the following statements using a five-point Likert scale (5- Strongly Agree to 1- Strongly Disagree):

1. I am confident that my grades for online assessment are secure with additional high-security methods.
2. I do prefer face capturing using Biometric technology for the e-exam system.

Illustration Results (Reliability)

This output shown in Table 1 was used to accept the alternative hypothesis in our decision (H0). The output indicates that we have 29 valid and none of the numbers was missing from respondents used in circulating the t-test. The respondents mean 2.72 and standard deviation 1.523. The standard error mean is 2.72 and standard deviation 1.623. The standard error mean is 0.301 (0.301 / square root of 29 = 0.301). The t-test value: (2.72-1) / (1.623 / square root of 29) = 9.036. The df (degree of freedom) column tells us that the t-test has 28 degrees of freedom derived from (29-1 =28). Sig (2-tailed) column indicates that the 2-tailed significance (the 2-tailed p value = 0.000). The mean difference in the population mean is 2.72 and the 95% confidence intervals are 2.11 to 3.34 ("Lower" to "Upper" columns).

Illustration Results (Securities)

Table 2 illustrates the result obtained from the 2-tailed Pearson correlation test. This output was used to accept the alternative hypothesis in our decision (H1) and reject the Null hypothesis (H0). The output indicates that we have 29 valid and none of the numbers was missing from respondents used in calculating the t-test. The respondents mean 2.67 and standard deviation 1.518. The standard error mean is 0.282 (0.282 / square root of 29 = 0.282). The t-test value: (2.67-1) / (1.518 / square root of 29) = 9.471. The df (degree of freedom) column tells us that the t-test has 28 degrees of freedom derived from (29-1 = 28). Sig (2-tailed) column indicates that the 2-tailed significance (the 2-tailed p value = 0.000). The mean difference in the population mean is 2.67 and the 95% confidence interval is 2.82 to 3.23 ("Lower" to "Upper" columns).

Table 1: One Sample T-Test (Reliability)

	N	**Mean**	**Std. Deviation**	**Std. Error Mean**
S5Q7 – I am confident that my grades for online assessments are secure with additional high securities methods	29	2.72	1.623	0.301

One-Sample Test

	Test value = 0					
	t	**Df**	**Sig.(2-tailed)**	**Mean Difference**	**95% confidence Interval of the Difference**	
					Lower	**Upper**
S5Q7 – I am confident that my grades for online assessments are secure with additional high securities methods	9.036	28	.000	2.724	2.11	3.34

Table 2: One Sample T-Test (Securities)

One-Sample Statistics

	N	**Mean**	**Std. Deviation**	**Std. Error Mean**
S5Q7 – I do prefer the face capturing using biometric technology for e-exam system	29	2.67	1.518	0.282

One-Sample Test

	Test value = 0					
	t	**Df**	**Sig.(2-tailed)**	**Mean Difference**	**95% confidence Interval of the Difference**	
					Lower	**Upper**

S5Q7 – I am confident that my grades for online assessments are secure with additional high securities methods	9.471	28	.000	2.675	2.82	3.23

Table 3 summarizes the results of the measurement integration test, confirming a clear interpretation of the results that statistically significant factors are reflected in the TWO-dimensional statistical test in relation to the acceptance recognition face included in the existing e-exam system.According to the student respondent from the results of the hypothesis test showed a very high percentage of firm consent, indicating that facial recognition is a requirement to be added to the e-exam system to make security safer and more reliable in the performance of student results and benefits to the student's use of the system. In addition, this clever approach uses a facial recognition test to enable the detection of theft and fraud in e-exam programs.

The results show that almost all students agree with the statements made.

Table 3: Summary of Hypothesis Test Results

Factors	**Correlation Test Results**
Reliability	Significant
Security	Significant

III. CONCLUSION

The Robust Automated Face Detection & Recognition system is being developed and used for Acquiring Additional Student Self-Determination in the testing system. This paper discusses a variety of modeling techniques that help in the ongoing monitoring of the student.In face detection using a fishing face, face detection, if the face is detected compared to the registration database, then the presence will be a sign. If the face is unknown, then a scam is detected and a message is sent to the chief inspector and the room manager. The ultimate goal is to ensure candidate identity in terms of facial recognition and recognition. Iris identification is the best way to identify people based on different patterns within the ring-shaped region. It provides an adequate Degree-of-Freedom for accurate and secure recognition. Iris provides precise consistent performance as it does not change much as people age. It works whether people wear sunglasses or contact lenses. This program aims to overcome limitations.So the conclusion is that the GUI should be upgraded so that the user can look at the top of the screen where the camera is usually installed.

REFERENCES

[1]. K. Sunil Manohar Reddy 2017, 'Comparison of Various Face Recognition Algorithms' Accessed at http://www.ijarset.com/upload/2017/february/21_IJARSET_sunilreddy.pdf

[2]. https://iq.opengenus.org/face-recognition-using-fisherfaces/

[3]. Aditi Bal, Arunasish Acharya, 2011 "Biometric Authentication and Tracking system for Online Examination System"

[4]. DwijenRudrapal, Smita Das, S. Debbarma, N. Kar, N. Debbarma, 2012 "Voice Recognition and Authentication as a Proficient Biometric Tool and its Application in Online Exam for P.H People"

[5]. Yassin Kortli, Maher Jridi, Ayman Al Falou, Mohamed Atri. "Face Recognition Systems: A Survey", Sensors, 2020

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

[7]. Minh Son Nguyen, Ngo Van Huynh, Dai Duong Tran, Hieu Truong Ngo. "An Approach of Face Recognition Applied for Smarthome Using System – on – Chip Technology", 2019 International Conference on Advanced Computing and Applications (ACOMP), 2019