

**Multibio Authentication of Online
Users in Proctoring
And E-Learning**

Submitted in partial fulfillment of the
requirements for the award of
Bachelor of Technology degree in Information Technology

By

**NITHISH KUMAR C M (Reg.No – 39120077)
VISHAL S (Reg.No – 39120138)**



**DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade “A” by NAAC | 12B Status by UGC | Approved by
JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI – 600119**

MAY - 2023



SATHYABAMA

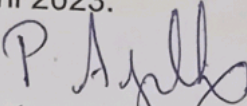
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved by AICTE

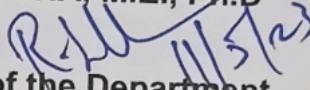
www.sathyabama.ac.in

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **Nithish Kumar C M (39120077)** and **Vishal S (39120138)** who carried out the Project Phase-2 entitled "**Multibio Authentication of Online Users in Proctoring And E-Learning**" under my supervision from January 2023 to April 2023.

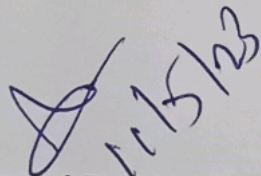

Internal Guide

Dr. P. AJITHA, M.E., Ph.D


Head of the Department

Dr. R. SUBHASHINI M.E., Ph.D

Submitted for Viva voce Examination held on 11/5/2023


Internal Examiner

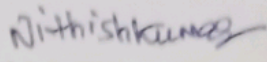

External Examiner

DECLARATION

I, Nithish Kumar C M (Reg.No- 39120077), hereby declare that the Project Phase-2 Report entitled "Multibio Authentication of Online Users in Proctoring And E-Learning" done by me under the guidance of Dr. P. Ajitha, M.E.,Ph.D is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology degree in Information Technology.

DATE: 11/5/2023

PLACE: Chennai


Nithish Kumar C M

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph. D, Dean**, School of Computing, **Dr. R. Subhashini M.E., Ph.D.**, Head of the Department of Information Technology for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. P.Ajitha M.E., Ph.D.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my phase-2 project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

ABSTRACT

To Identify the verification and proctoring of online students are two of the key challenges to online learning today. Especially for online certification and accreditation, the training organizations need to verify that the online students who completed the learning process and received the academic credits are those who registered for the courses. Furthermore, they need to ensure that these students complete all the activities of online training without cheating or inappropriate behaviours. The COVID-19 pandemic has accelerated (abruptly in certain cases) the migration and implementation of online education strategies and consequently the need for safe mechanisms to authenticate and proctor online students. Nowadays, there are several technologies with different grades of automation. In this paper, we deeply describe a specific solution based on the authentication of different biometric technologies and an automatic proctoring system (system workflow as well as AI algorithms), which incorporates features to solve the main concerns in the market: highly scalable, automatic, affordable, with few hardware and software requirements for the user, reliable and passive for the student. Finally, the technological performance test of the large scale system, the usability privacy perception survey of the user and their results are discussed in this work.

TABLE OF CONTENTS

Chapter No.	TITLE	Page No.
	ABSTRACT	v
	LIST OF FIGURES	vii
1	INTRODUCTION	8
2	LITERATURE SURVEY	10
	2.1 Inferences from Literature Survey	11
	2.2 Open problems in Existing System	12
3	REQUIREMENTS ANALYSIS	15
	3.1 Risk Analysis of the Project	15
	3.2 Feasibility Study	16
	3.3 Software Requirements Specification Document	17
4	DESCRIPTION OF PROPOSED SYSTEM	18
	4.1 Selected Methodology or Process Model	18
	4.2 Architecture / Overall Design of Proposed System	22
	4.3 Subsystem response reliability	23
	4.4 Fusion schema	24
	4.5 Integration in e-learning platforms	25
	4.6 Integration methodology	25
	4.7 Temporal windowing of the authentication process	26
	4.8 Global system reliability response	27
5	IMPLEMENTATION DETAILS	28
	5.1 Testing plan of the Proposed Model/System	28
	5.2 Algorithm	32
6	RESULT RESULTS AND DISCUSSION	39
	6.1 Screen Shots	39
7	CONCLUSION	42
	7.1 Future Scope	43
	REFERENCES	44
	RESEARCH PAPER	46

LIST OF FIGURES

Figure No.	FIGURE NAME	Page No.
4.1.1	Integration schema	21
4.1.2	A sample use of temporal windows for biometric authentication	21
4.2.1	The reference architectures Face recognition	22
4.2.2	The reference architecture for Voice recognition	22
4.2.3	The reference architecture for Touch recognition	22
5.2.1	CNN Components	34
5.2.2	RGB Pixel Values	34
5.2.3	Input image size 3*3 and 6*6	35
5.2.4	Feature map	36
5.2.5	Filter Pass	36
5.2.6	Filter pass through stride of 1	37
5.2.7	Applied Max Pooling of 2*2 size	38
5.2.8	The complete process of a CNN model	38
6.1.1	Registring the user's information	39
6.1.2	Capturing User's Face for verification and Matching purpose	40
6.1.3	Comparing the Voice Files for Voice Authentication	40
6.1.4	Result for Face Recognition Authentication	41
6.1.5	Authorization Results of the Project	41

CHAPTER 1

INTRODUCTION

In this project, online courses have emerged as a flexible way to educate large groups of students in distance learning settings. However, as the demand increases, educational institutions are facing the challenge of assessing the integrity of their initiatives, without classroom attendance. In this context, possible threats include impostors taking an online examination as well as the dissimulation of the identity credentials to other users. In order to minimize such threats, institutions should (i) verify the identities of online students, (ii) guarantee they take exams without cheating, and (iii) assess their performance adequately. In this paper, we focus on the first task aimed to prove that the student who is certified is the one who performs the e-learning activities.

In general, the existing solutions are usually designed to proctor students only during online exams. They do not tend to consider the rest of the course participation. The common procedure allows students to perform exams online while a person monitors them remotely (e.g. Kriterion1 and ProctorU2). It is non-scalable and depends on the ability of the human proctor. Other systems replace human with algorithms to achieve the same goal via post or realtime analysis, but at lower costs, as they eliminate the human effort (e.g. ProctorFree3 and RemoteProctorNow4). In that case, several risks come due to the variability of their accuracy and the limited supported scenarios. Furthermore, hybrid solutions involve people only for suspicious situations (e.g. Proctorio5).

Given the nature of the problem, the authentication method should be continuous. In fact, a system based only on passwords (something the user knows) or devices (something the user has) assumes that the student will not provide them to other users. Even more, a biometric authentication (something the user is or does) at the point-of-entry does not consider that the student can login to the system and let an impostor continue. These methods are not valid whenever the students are interested in cheating, especially during exams. In addition to being continuous, the authentication method should also be transparent, without affecting the normal student's activities.

In this context, several academic and industrial research groups have proposed different solutions. Among them, uni-biometric systems usually aim at capturing face and/or body cues. Monitoring them alone cannot stop cheating, since they lack interaction with the student.

In other cases, multiple biometrics are combined, such as face with fingerprint or fingerprint and vocal traits. Behavioral biometrics, such as keystroke and mouse patterns, try to accomplish transparent authentication while the students perform activities, but they are not sufficiently reliable without combining a physical biometric trait. Moreover, they tend to target a specific type of interaction.

For instance, keystroke patterns can be recognized only when the student is typing, Over the course period, students can learn from different devices and their interactions also include selection, navigation, speaking, and more. Task models, such as, usually help to represent and describe them.it seems that student authentication in e-learning platforms during different activities on different devices can be improved.

In this paper, we propose a multi-biometric system aimed at continuously and transparently authenticating online students in e-learning platforms. We combine different biometric traits based on the type of interaction and the type of device used at a specific moment. The system is able to capture raw data of face traits, voice traits, touch behavior, mouse dynamics, and keystroke patterns during the utilization of the e-learning platform.

For each combination of interaction and device, we try to control both something the student is and something the user does, since only face recognition is effective but lacks interaction, while the other biometrics recognize the interaction, but they are not sufficiently accurate alone. In addition, almost all the existing devices are equipped with sensors to track these biometrics. The result is a device/interaction-agnostic multi-biometric system.

CHAPTER 2

LITERATURE SURVEY

RICARDO VEA is currently the CEO and the Business Development Manager of Smowltech. He has worked more than twenty years in the world of HR in different organizations, where he has developed director and consultant roles. He is also a Professor-Collaborator with the Deusto Business School and previously with the UPV. Before entering in Smowltech, he was developing a Cyber- Security Certification Agency for a multinational computing security company. He is an Expert in e-learning and an enthusiast of modern technologies for teaching training.

NAIARA AGINAKO collaborated the Signal Processing and Communication Group, Electronics and Telecommunications Department. She developed and managed research projects with Digital Media Department, Vicomtech, from 2005 to 2015. Since 2015, she has been teaching at the Polytechnic School of Donostia and the Faculty of Informatics. Her work as a Researcher includes a number of publications and two patents.

BASILIO SIERRA is currently a Full Professor with the Computer Sciences and Arti_cial Intelligence Department, the University of the Basque Country. He is also the Director of the Robotics and Autonomous Systems Group, Donostia-San Sebastian. He is a Researcher in the fields of robotics, computer vision and machine learning, and he is working on the development of different paradigms to improve classi_cation behaviours. He has written more than 25 journal articles in those fields, more than 100 conference contributions, and more than 30 book chapters.

MIKEL LABAYEN researches in the automatic facial and voice recognition area developing applications for online user authentication based on human biometrics. In the same period, he also was an Associate Teacher with the Electronic Technology Department, University of the Basque Country. He is currently working in the field of intelligent transport systems (ITS) designing computer vision and machine learning-based solutions for autonomous train operations in the railway sector with the CAF Group. His work as a Researcher includes a number of publications and four patent.

2.1 INFERENCES FROM LITERATURE SURVEY

The general security goals of computer a system are known to include confidentiality, integrity and availability (C-I-A) which prevent critical assets from potential threats. The C-I-A security goals are well researched areas; however they may be insufficient to address all the needs of the summative e-assessment. In this paper, we do not discard the fundamental C-I-A security goals; rather we define security goals which are specific to summative e-assessment security.

This paper proposes a trustworthiness model for the design of secure learning assessment in on-line web collaborative learning groups. Although computer supported collaborative learning has been widely adopted in many educational institutions over the last decade, there exist still drawbacks which limit their potential in collaborative learning activities. Among these limitations, we investigate information security requirements in online assessment, (e-assessment), which can be developed in collaborative learning contexts.

Despite information security enhancements have been developed in recent years, to the best of our knowledge, integrated and holistic security models have not been completely carried out yet. Even when security advanced methodologies and technologies are deployed in learning management systems, too many types of vulnerabilities still remain opened and unsolved. Therefore, new models such as trustworthiness approaches can overcome these lacks and support e-assessment requirements for e-Learning.

online courses and other forms of remote education continue to increase in popularity and reach. The ability to efficiently proctor remote online examinations is an important limiting factor to the scalability of this next stage in education. Presently, human proctoring is the most common approach of evaluation, by either requiring the test taker to visit an examination center, or by monitoring them visually and acoustically during exams via a webcam. However, such methods are labor intensive and costly.

In this paper, we present a multimedia analytics system that performs automatic online exam proctoring. The system hardware includes one webcam, one wearcam, and a microphone for the purpose of monitoring the visual and acoustic environment of the testing location. The system includes five basic components that continuously estimate the key behavior cues: user verification, text detection, voice detection, active window detection and gaze estimation. By combining the continuous estimation components, and applying a temporal sliding window, we design higher level features to classify whether the test taker is cheating at any moment during the exam.

E-learning systems represent a new form of learning and are becoming more and more popular everyday. Hence security in e-Learning has become a fundamental requirement. But the problem of e- learning systems is that only little money is invested for security. Also to authenticate an e-learner especially in case of e-exams is a major challenge in an e-learning environment. The role of authentication techniques to prevent unauthorized access by malicious users becomes more significant.

User authentication methods can be classified into three categories: (1) methods based on human memory such as passwords, (2) methods based on physical devices such as magnetic or IC cards, and (3) methods based on biometrics such as fingerprint, iris, etc., As the first two categories cannot escape vulnerabilities caused by forgetfulness or losses, the third category attracts much attention these days. A major problem of biometrics authentication is that it is not free from an error in the process of extraction of human characteristics and comparison of biometrics data.

2.2 OPEN PROBLEMS IN EXISTING SYSTEM

It is a live proctoring system in which the proctor guides students through the entire process of an online exam, and also monitors them using the webcam. Proctors are required to ensure that no unauthorized materials are present before the start of the exam.

They are also required to verify the student's identity by asking them to present their ID cards. Students are required to maintain an uninterrupted audio-visual connection to the proctor throughout the session. Kryterion, a widely-used commercial OPS uses an approach very similar to the one used by ProctorU. The AI module of ProctorU, however, isn't highly secure and can be deceived, which is why the company recommends using their hybrid solution to maintain high security.

This hybrid solution augments automated proctoring with professionally trained live proctors, who have the ability to interrupt the test and intervene in case they suspect something. The PSI Bridge platform makes use of a proprietary lockdown browser and a self-authentication scheme, to ensure proper compliance, while also maintaining student privacy and minimizing security risks.

It is a highly secure platform that doesn't need any access to the student's computer to verify the exam's integrity, hence making it non-invasive. The exam session is recorded and stored in an LMS server that is integrated with a cloud-based Software as a Service (SaaS) Exam logs and flagged violations are also stored along with it, where the proctor can review it later.

In ProctorExam, spatial controls are augmented by utilizing a highly innovative 360-degree monitoring. This monitoring includes webcam, screen-sharing, and a smartphone camera positioned in such a way so as to view everything around the test-taker. It also uses facial recognition to flag cheating attempts.

A brilliant multi-factor authentication scheme specifically designed for securing online examination services without comprising user-friendliness has also been proposed. It is a three-fold scheme featuring face-recognition, OTP verification, and fingerprint authentication modules. The system deploys a hierarchical structural methodology where the user starts off with a proper Registration process.

The registration process involves the user registering themselves with a unique ID provided by the institution, right forefinger impression and phone number verified using OTP. The system then proceeds to the login module, that screens users trying to access the system.

Although computer supported collaborative learning has been widely adopted in many educational institutions over the last decade, there exist still drawbacks which limit their potential in collaborative learning activities. But the problem of e- learning systems is that only little money is invested for security.

Also to authenticate an e-learner especially in case of e-exams is a major challenge in an e-learning environment. A major problem of biometrics authentication is that it is not free from an error in the process of extraction of human characteristics and comparison of biometrics data.

2.2.1 Disadvantage:

- A new normalization function, the mapping function, able to not overcome the limitations of commonly used techniques.
- As students have to look at screens continuously, it can strain their eyes.
- The classroom environment is lively in nature, whereas sitting in front of a computer or smartphone to listen to the classes will be boring.

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 RISK ANALYSIS OF THE PROJECT

A risk is the probability of the occurrence of a particular threat and the expected loss. E-risk involve the risk at the time of electronic transaction, whereas threat means an anticipated danger. Common threats for computers are viruses, network penetrations, theft and unauthorized modification of data, eavesdropping, and non-availability of servers and personal computers.

During transaction original documents may be modified ,tampered or destroyed by the hackers' active and passive attacks . Therefore knowledge of risk would be given priority in E-Learning. In this paper, our emphasis is laid on different risks faced by the participants and their remedies to make the system reliable and efficient.

The second section explains common threats, followed by different risks faced by the participants and necessity of risk analysis in E-Learning. Section three elaborates how these risks can be minimized by different tools and techniques. The fourth section offers a brief conclusion.

Some cyber security issues related to e-learning system such as corrupted or lost communications, messages, grades, data or work; a compromised the users and the teachers identify; stolen personal information and corrupted social technical systems. The most concern is that instructors and students use the e-system for their education purposes but they don't know the threats behind that system.

E-learning not only offers a lot of benefits for the users but also carries some cyber security threats making data vulnerable. Therefore, we need to ensure the security and the safety of the users in e-system.

3.2 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are,

- **ECONOMICAL FEASIBILITY**
- **TECHNICAL FEASIBILITY**
- **SOCIAL FEASIBILITY**

ECONOMICAL FEASIBILITY :

This project is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY:

This project study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources.

This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY:

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity.

The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

3.3 SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT

Software Requirements

- Front End : PYTHON
- Back End : SQLLITE
- Operating System : Windows 07
- IDE : PYTHON IDE
- ALGORITHM : CNN+LSTM

While you take the exam, the proctoring software monitors your computer, including any software that is running, and streams the exam data to the proctoring software via the cloud. The software also records video and audio from your webcam.

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

4.1 SELECTED METHODOLOGY OR PROCESS MODEL

In this section, we describe the system for continuous student authentication proposed in this paper. The system integrates five biometric subsystems which recognize face, voice, and touch respectively. Each one of them returns a pair of values: the first one is a distance resulting from the comparison of the template of the claimed student and the template of the probe; the second one is the reliability level associated to the distance provided by the subsystem. The global authentication response is computed by adding the matching scores from all the subsystems, weighted with their reliability measures. Finally, the global authentication response is compared with an acceptance threshold if it is lower, the student continues the learning session, otherwise the system raises the access control.

Biometric authentication subsystems

In the following sections, we describe how each subsystem implements its own modules depending on the type of biometric.

Face-Based authentication subsystem

Almost all the existing devices, mobile or desktop, are equipped with an on-board camera. Throughout the learning experience, the student is generally in front of it, so we are able to easily capture face images with no effort for the student. During a temporal window, the subsystem captures face images randomly.

Once the temporal window ends, it performs the recognition of the samples in parallel. For that purpose, we implement a framework based on the approach. The Viola-Jones algorithm is applied to identify the subregion of the image containing the face.

If the number of retrieved faces is not equal to one, the subsystem returns a response of $SRR1 = 1$ and $T1 = 1$. Otherwise, it performs a pose normalization step based on Active Shape Model (ASM), one of the algorithms that balances accuracy and computational time. This is necessary because the student is authenticated transparently without requiring him/her to always remain in front of the camera; so, a pose variation often happens.

In our context, anti-spoofing countermeasures should be integrated due to the possibility of cheating. We implement the technique of 3D geometric invariants stated in. Then, the subsystem uses a matching technique based on a localized version of the spatial correlation between the face template of the claimed identity and the face probe analyzed.

Voice-based authentication subsystem

To record audio clips, a microphone is used. Almost all the existing devices are equipped with this sensor and they provide procedures to capture data coming from it. Given the nature of our problem, the subsystem is able to perform a text-independent authentication, since it does not know in advance which phrases the student says.

A voice activity detector is used to remove the silence and other non-informative segments from the audio clip. The speech input is sampled at a rate higher than 10.000 Hz to minimize the aliasing effects in the analog-digital conversion and cover almost all the energy sounds generated by humans.

To obtain a parametric representation from the speech waveform, the subsystem extracts the Mel Frequency Cepstral Coefficients (MFCCs), one of the most common techniques in modern automatic speech recognition systems. The frequency bands are equally spaced on the Mel scale, so that it approximates human auditory system response. The feature extraction is done on short times, assuming that a small segment of speech is much stationary for a better modeling phase and a better representation of the sound features.

The MFCCs vector extracted from the probe is compared with the template of the claimed identity in the database. For that purpose, the subsystem uses vector quantization codebooks due to their ease of implementation and their high accuracy. The process maps acoustic vectors to a finite number of regions in the space. Each region is a cluster represented by its center (i.e. codeword); each one of them is associated to one student. The set of all the codewords is called codebook.

Touch-based authentication subsystem

In literature, touch-based authentication systems are gaining popularity due to the good compromise between security and usability and the massive use of mobile devices. The existing mobile operating systems provide standard APIs to get raw data related to touch behavior. Other libraries are developed for touch detection on mobile web sites, mainly in JavaScript.

We integrated the algorithm in, since it is able to consume raw data about primary touch gestures (tap and slide). It also requires data only from the claimed student, differently from other state-of-the-art algorithms such as. This speeds up the training phase and provides a fast way to update the student's template, as needed. The algorithm captures six raw touch features for each gesture (timestamp, vibration, rotation, pressure, touch size, and position).

During the enrollment phase, two classifiers based on three hidden markov models are built for the student. This approach fits better our system requirements due to the high enrollment speed and the high accuracy. The trained classifiers represent the touch template that our system stores for each student.

During the authentication phase, the multiple consecutive gestures performed by the user are provided to the classifiers previously trained for the claimed student. T3 score is represented by the average likelihood obtained from the two classifiers. The value is normalized in the range [0,1] and then converted in a distance in the same range by subtracting it from 1.

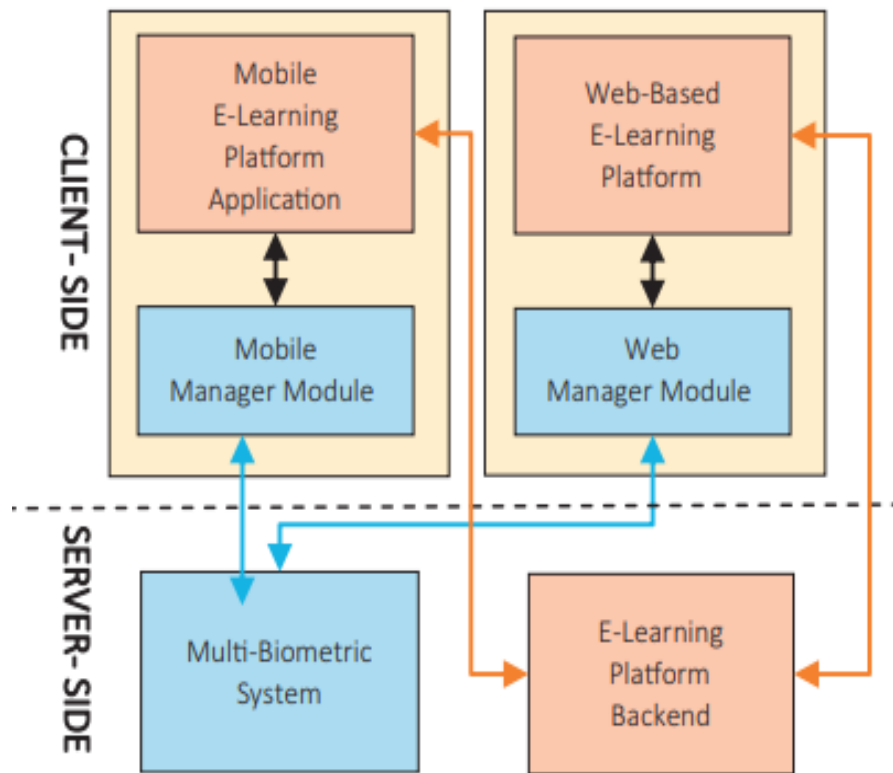


Fig 4.1.1. Integration schema between an e-learning platform and our system.

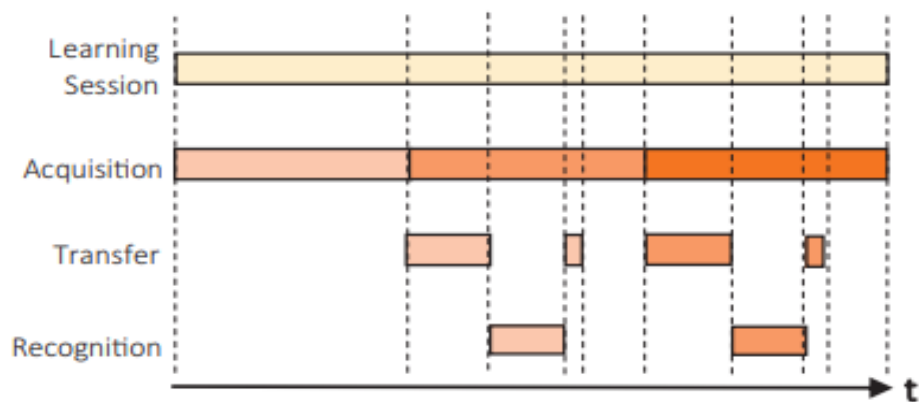


Fig.4.1.2. A sample use of temporal windows for biometric authentication.

4.2 ARCHITECTURE / OVERALL DESIGN OF PROPOSED SYSTEM

The system architecture for Multibio Authentication of Online Users in Proctoring and E-Learning would typically involve multiple components working together to ensure secure and reliable authentication of online users during proctoring and e-learning activities. Here is a high-level overview of the potential system architecture:

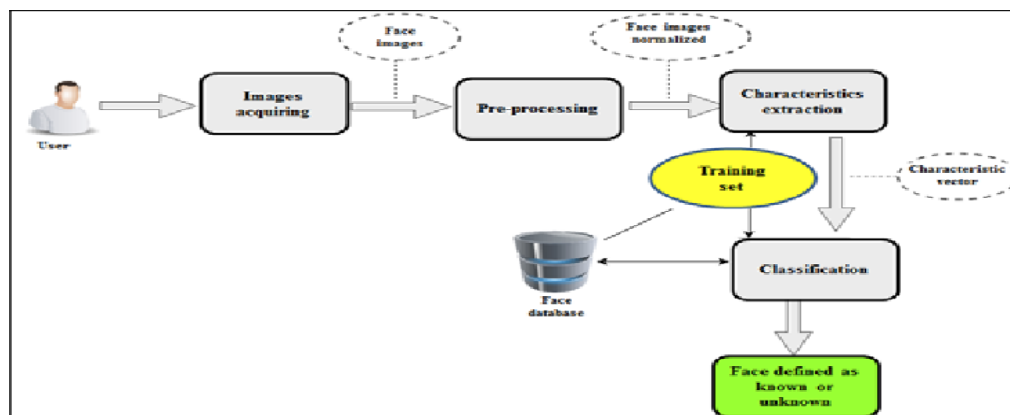


Fig 4.2.1 The reference architectures Face recognition.

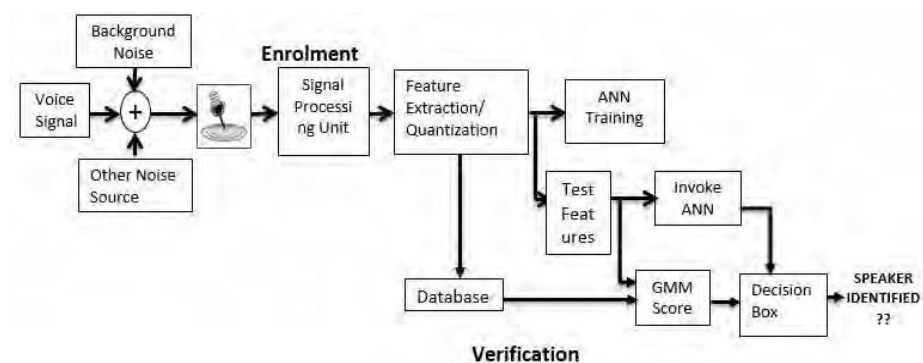


Fig 4.2.2 The reference architecture for Voice recognition.

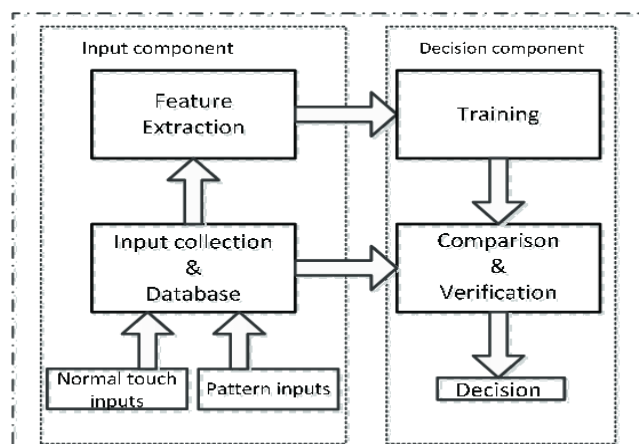


Fig 4.2.3 The reference architectures for Touch recognition.

4.3 Subsystem response reliability

In the authentication response, each subsystem returns (i) the matching score and (ii) the reliability level associated with it. As analyzed in Section 2.5, a reliability measure which considers the context in which the matching score is computed rather than the quality of input data is proved to return better performance. In, the authors defined a biometric-independent reliability function for an identification system which depends on the gallery.

They consider the sorted list of identities returned in an identification process as a cloud; the more the points are near to the first returned identity, the more unreliable is the answer. The density ratio ϕ can be used to model this concept. In our contribution, each subsystem addresses the computation of the score reliability by applying a variation of that idea.

Since each subsystem contains a gallery with all the students' templates, the system uses the template of the claimed student as unique genuine sample (i.e. as the first returned identity in the identification case) and the other templates as impostors' templates. The idea is formalized as follows. Given a probe p_i claimed by the student s_k with the enrolled template g_{ik} and an authentication subsystem A_i with a gallery of impostors G_i , the density ratio ϕ_i for p_i in A_i is defined as follows:

$$\phi_i(p_i, s_k) = 1 - |Nb|/|G_i| \longrightarrow (1)$$

Where:

$$Nb = |\{g_{ij} \in G_i | d(p_i, g_{ij}) < r * d(p_i, g_{ik}) \wedge j \neq k\}| \longrightarrow (2)$$

where r is the value of the radius. Once computed the value ϕ_i , some more steps are required to pass from it to the value of SRR for the probe, namely SRR_i . For this purpose, with the density ratio ϕ_i as confidence measure. The result is normalized in the range $[0, 1]$ through the QLS function. In this way, we can manage the high variability of the responses caused by the context in which the data is acquired.

4.4. Fusion schema

The system proposed in this paper implements a fusion scheme where five biometric traits are combined at score level to improve authentication performance. This is widely accepted as the best compromise between the level of complexity and the amount of information available to the fusion process. In our system, each subsystem returns a pair of values.

The first one is a distance in the range [0,1] resulting from the comparison of the template of the claimed student and the template of the probe. The second one represents the level of reliability associated to the score provided by the subsystem in the range [0, 1]. We assume that the reliability level becomes 0 when no data is received for the corresponding biometric, so that the associated matching score can be discarded in the computation of the global response.

It is proved that a high distance, which generally implies that a user is not who s/he claims to be, should be weighted with the reliability level associated to the response for a better recognition result. The same principle is also valid when the distance is low. The fusion schema adopted by our system exploits SRR measures produced by the subsystems to weight the matching scores.

More specifically, we can identify five different reliability values, respectively SRR1 for the face, SRR2 for the voice, SRR3 for the touch, SRR4 for the mouse, and SRR5 for the keystroke.

They are used as weights to produce a weighted sum which corresponds to the global distance produced by the system. To make consistent the result, the sum of the weights must be 1. SRRi values are normalized with respect to their sum.

$$SRR_{\sigma} = \frac{\sum_{i=1}^5 SRR_i}{\sum_{i=1}^5 SRR_i} \longrightarrow (3)$$

Moreover, we have five matching scores, respectively T1 for the face, T2 for the voice, T3 for the touch, T4 for the mouse, and T5 for the keystroke.

With an extension on the formula provided in, the global score T for the whole system is obtained as follows:

$$T = \sum_{i=1}^5 SRR_i / SRR_{\sigma} * T_i \longrightarrow (4)$$

The global authentication response is compared against a specific acceptance threshold if it is lower, the student continues the learning session, otherwise the system raises the access control.

4.5. Integration in e-learning platforms

In this project, we describe how the multi-biometric system presented in this paper can be integrated in an e-learning platform. we show how the components are distributed on the client side and the server side. we describe how they communicate each other; since the integration method raises the problem of defining how much data should be captured before starting the recognition, we introduce and explain the concept of temporal authentication window. we propose global reliability measures related to the ability of the system to recognize a given student during a specific type of interaction on a specific type of device.

4.6. Integration methodology

The integration methodology is depicted in On the client side, it is necessary to integrate the web/mobile client of the elearning platform with a manager module. On the server side, there are both the multi-biometric system and the e-learning platform backend. The manager module acts as an intermediary between the e-learning platform client and the multi-biometric system running on the server. It is responsible for the acquisition of raw data for each biometric trait and the sending of data to the multi-biometric system. In addition, it processes the global authentication response returned by the multi-biometric system. On the server side, no dependencies are required between our system and the e-learning platform backend. The multi-biometric system receives raw data, performs the recognition and returns the global authentication response to the manager module. The reader notices that we decided to avoid the inclusion of the entire multibiometric system into the client side, so that we can obtain major

4.7. Temporal windowing of the authentication process

The existing biometric systems we reported in typically perform continuous authentication by instantly capturing a new probe (e.g. a touch gesture or a face image) and recognizing it immediately. This is quite complex in the context of our system due to (i) the computational weight derived from the execution of feature extraction, matching, and fusion steps whenever a probe is acquired, (ii) the reduced amount of information available for a biometric recognition cycle, especially for behavioral biometrics which need data acquired over an interval of time to provide a better matching, and (iii) the instability and the minor contribution of the fusion step which derive from the problems at second point. Our multi-biometric system tries to minimize them through the use of temporal authentication windows.

The acquisition of raw data is carried out on the manager module along consecutive time intervals of fixed duration (i.e. temporal windows). Once a temporal window expires, the raw data captured in that temporal window is sent to the multi-biometric system for the recognition process. At the same time, the manager module starts to capture data for the next temporal window.

The multi-biometric system returns the authentication response to the manager module that reacts accordingly to it, enabling the student to continue the learning session or raising the access control. The temporal window size mainly depends from (i) the time required to send the raw data, (ii) the computational time that the multi-biometric system requires to compute the authentication response, and (iii) the time required to send back the authentication response to the manager module.

If the sum of the times at the first and the second point is lower or equal to the temporal window size, the multi-biometric system is able to consume the data captured for a given window before the data acquired for the next window is sent to it. The main limitation of this approach is that an impostor can perform any interaction with the e-learning platform between the end of a temporal window and the moment in which it is received the global authentication response.

4.8. Global system reliability response

In our multi-biometric system, the reliability measures for each subsystem are computed from the probes. Consider a learning session Is of t_s seconds on the device d and a temporal window size of t_w seconds. Assume each T_k subsystem was executed $M = t_s / t_w$ times producing $\{T_k(1), T_k(2), T_k(M)\}$ matching responses with the corresponding reliability measures $\{SRR_k(1), SRR_k(2), SRR_k(M)\}$.

For the learning session Is , the system stores a set of records composed by three attributes: the ID of the device where Is is performed, the ID of the student who performed the learning session, and a list of averaged SRR values, one for each biometric subsystem; each averaged SRR represents the average of all the SRR measures returned by the corresponding biometric subsystem during Is session.

They model the reliability of the subsystems T_k on the session Is for a given student. By using the information stored in these session records, we can also measure (i) the reliability of the system to recognize a student on a given device and (ii) the reliability of the system to recognize a student during a specific type of interaction on a given device. The first one can be the average of all the SRR values stored in all the session records. The second one can be calculated from the average of the SRR values from only a subset of biometric subsystems; its elements should be selected with respect to the type of interaction and the type of device considered.

The above reliability measures can be suitable to identify on which device the system can perform a better authentication of the student. This support is crucial, especially to evaluate which student's device should be used to perform online exams that normally require a higher security level than course attendance. However, the reader notices that a trade-off probably exists between reliability and user's preference related to the type of device.

In combination to the above techniques, the discovery of user or even group preferences, such as [50], can help to integrate users' acceptance, maintaining uniformity

CHAPTER 5

5.1 TESTING PLAN OF THE PROPOSED MODEL/SYSTEM

SYSTEM TEST:

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS

Unit testing:

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated.

It is the testing of individual software units of the application. It is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive.

Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing:

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional test:

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

- Valid Input : identified classes of valid input must be accepted.
- Invalid Input : identified classes of invalid input must be rejected.
- Functions : identified functions must be exercised.
- Output : identified classes of application outputs must be exercised.
- Systems/Procedures : interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

System Test:

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An

example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing:

White Box Testing is a testing in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing:

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

Unit Testing:

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test objectives:

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

Integration Testing:

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Acceptance Testing:

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

We can summarize the most representative characteristics of the proposed multi-biometric system as follows.

- The system is able to verify the student's identity on almost all the existing devices since they are equipped with sensors and provide routines to track such biometrics.
- The subsystems work in parallel, so that the global response is computed with the execution time of the slowest recognition algorithm. This mitigates the global authentication time.
- The system is able to integrate off-the-shelf algorithms, since each subsystem has no knowledge about the other ones and the matching scores are normalized by applying the QLS function.

- The system uses an adaption of the SRR measure, exploiting the template gallery with data of all the students. The reliability values are normalized with the QLS function.
- The system implements a score-level fusion, balancing the computational cost of the fusion operation and the amount of information available to perform authentication.

5.2 ALGORITHM

Convolutional Neural Network (CNN)

Introduction to CNN

Convolutional Neural Network is a Deep Learning algorithm specially designed for working with Images and videos. It takes images as inputs, extracts and learns the features of the image, and classifies them based on the learned features.

This algorithm is inspired by the working of a part of the human brain which is the Visual Cortex. The visual Cortex is a part of the human brain which is responsible for processing visual information from the outside world. It has various layers and each layer has its own functioning i.e each layer extracts some information from the image or any visual and at last all the information received from each layer is combined and the image/visual is interpreted or classified.

Similarly, CNN has various filters, and each filter extracts some information from the image such as edges, different kinds of shapes (vertical, horizontal, round), and then all of these are combined to identify the image.

There are some disadvantages with ANN:

- It is too much computation for an ANN model to train large-size images and different types of image channels.
- The next disadvantage is that it is unable to capture all the information from an image whereas a CNN model can capture the spatial dependencies of the image.
- Another reason is that ANN is sensitive to the location of the object in the image i.e if the location or place of the same object changes, it will not be able to classify properly.

COMPONENTS OF CNN

The CNN model works in two steps: **feature extraction and Classification**. **Feature Extraction** is a phase where various filters and layers are applied to the images to extract the information and features out of it and once it's done it is passed on to the next phase i.e **Classification** where they are classified based on the target variable of the problem.

A typical CNN model looks like this:

- Input layer
- Convolution layer + Activation function
- Pooling layer
- Fully Connected Layer

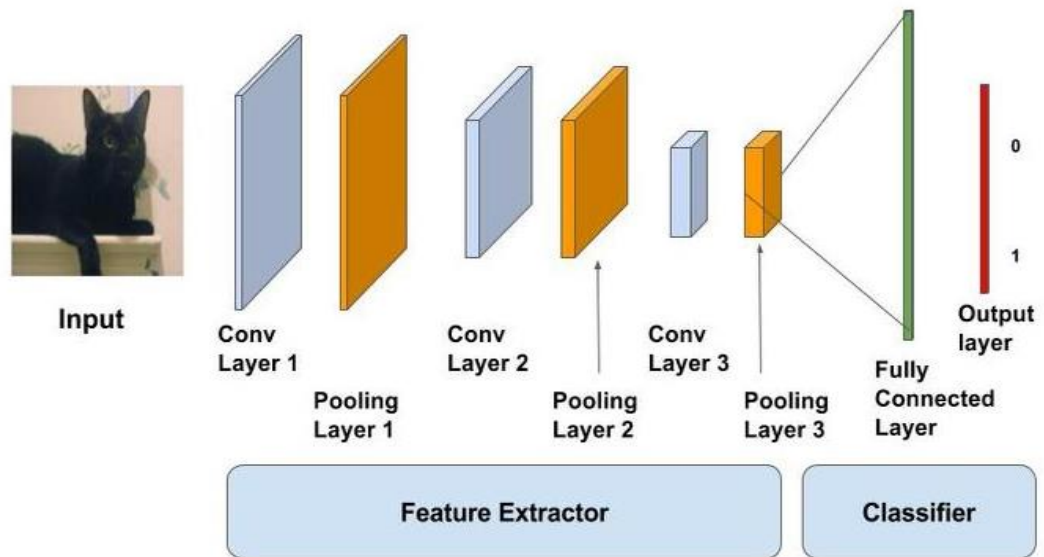
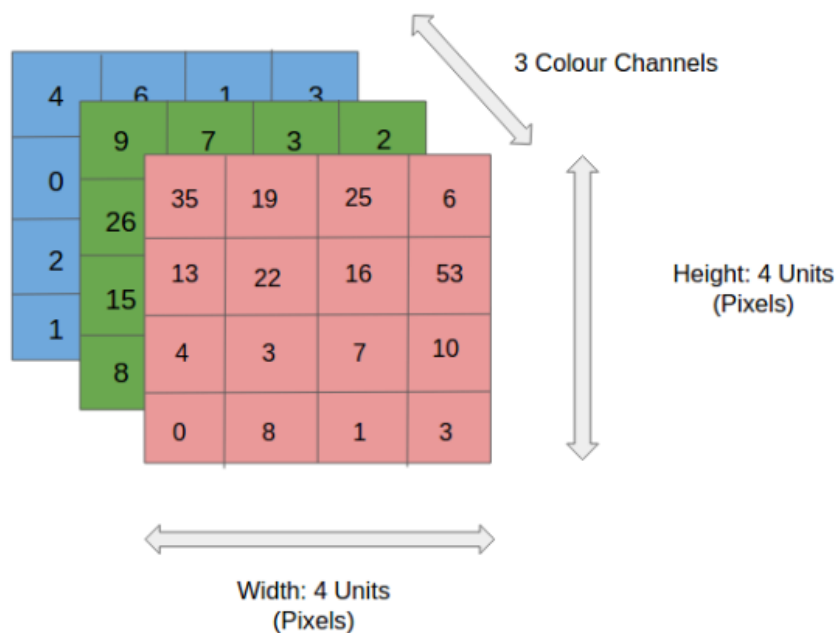


Fig 5.2.1 CNN Components.

INPUT LAYER:

As the name says, it's our input image and can be Grayscale or RGB. Every image is made up of pixels that range from 0 to 255. We need to normalize them i.e convert the range between 0 to 1 before passing it to the model.

Fig 5.2.2 RGB and pixel values.



CONVOLUTION LAYER:

The convolution layer is the layer where the filter is applied to our input image to extract or detect its features. A filter is applied to the image multiple times and creates a feature map which helps in classifying the input image.

Let's understand this with the help of an example. For simplicity, we will take a 2D input image with normalized pixels.

The diagram illustrates a 1D convolution operation. On the left is a 6x6 input matrix (labeled 6*6) with the following values:

0	0	0	1	1	1
0	0	0	1	1	1
0	0	0	1	1	1
0	0	0	1	1	1
0	0	0	1	1	1
0	0	0	1	1	1

This is multiplied (indicated by an asterisk *) by a 3x3 filter (labeled 3*3) with the following values:

1	0	-1
2	0	-2
1	0	-1

The result is a 4x4 feature map (labeled 4*4) with the following values:

0	-4	-4	0
0	-4	-4	0
0	-4	-4	0
0	-4	-4	0

Fig 5.2.3 Input image size 3*3 and 6*6.

In this example, we have applied only one filter but in practice, many such filters are applied to extract information from the image.

The result of applying the filter to the image is that we get a Feature Map of 4*4 which has some information about the input image. Many such feature maps are generated in practical applications.

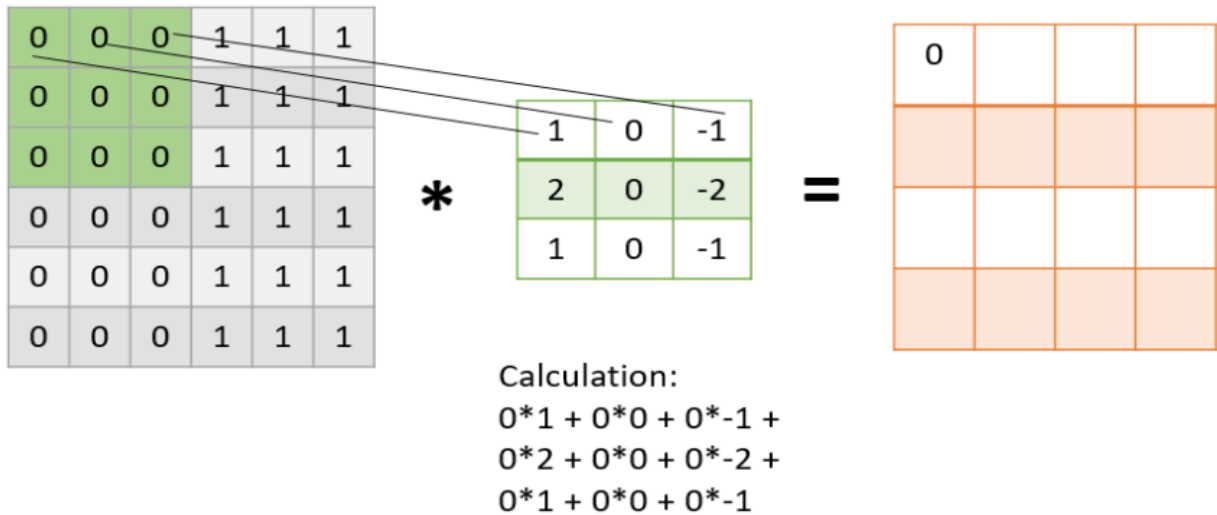


Fig 5.2.4 The Feature Map.

As presented in the above figure, **in the first step** the filter is applied to the green highlighted part of the image, and the pixel values of the image are multiplied with the values of the filter (as shown in the figure using lines) and then summed up to get the final value.

In the next step, the filter is shifted by one column as shown in the below figure. This jump to the next column or row is known **as stride** and in this example, we are taking a stride of 1 which means we are shifting by one column.

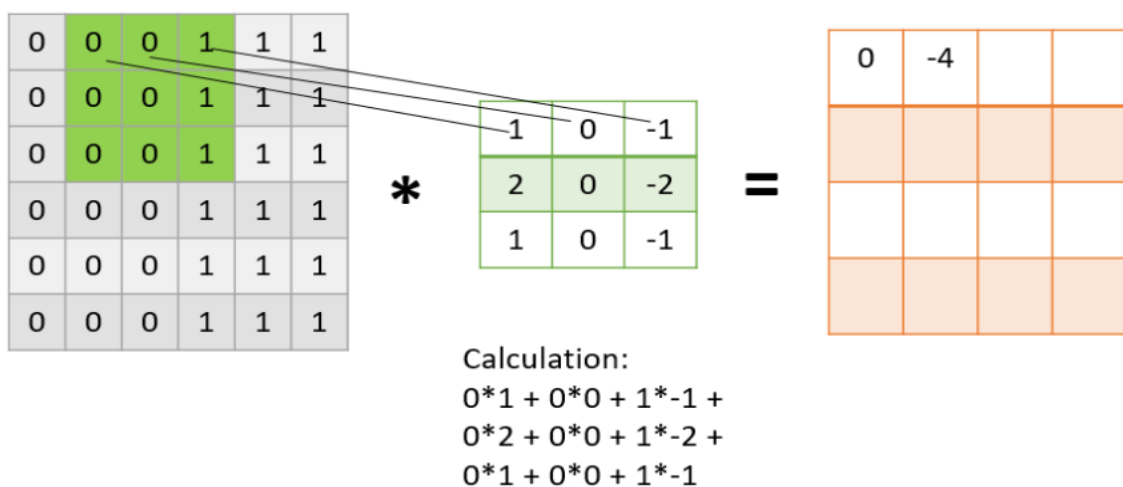


Fig 5.2.5 The Filter Passes.

Once we get the feature map, an activation function is applied to it for introducing nonlinearity.

A point to note here is that the Feature map we get is smaller than the size of our image. As we increase the value of stride the size of the feature map decreases.

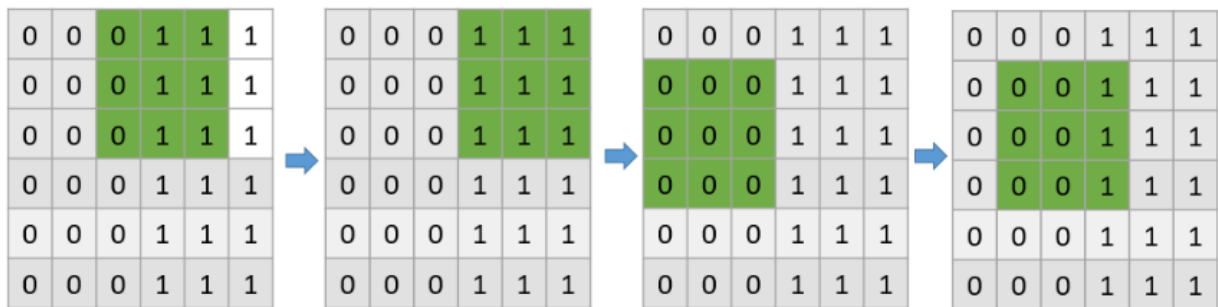


Fig 5.2.6 Filter pass through stride of 1.

Pooling Layer

The pooling layer is applied after the Convolutional layer and is used to reduce the dimensions of the feature map which helps in preserving the important information or features of the input image and reduces the computation time.

Using pooling, a lower resolution version of input is created that still contains the large or important elements of the input image.

The most common types of Pooling are Max Pooling and Average Pooling. The below figure shows how Max Pooling works. Using the Feature map which we got from the above example to apply Pooling. Here we are using a Pooling layer of size 2*2 with a stride of 2.

The maximum value from each highlighted area is taken and a new version of the input image is obtained which is of size 2*2 so after applying Pooling the dimension of the feature map has reduced.

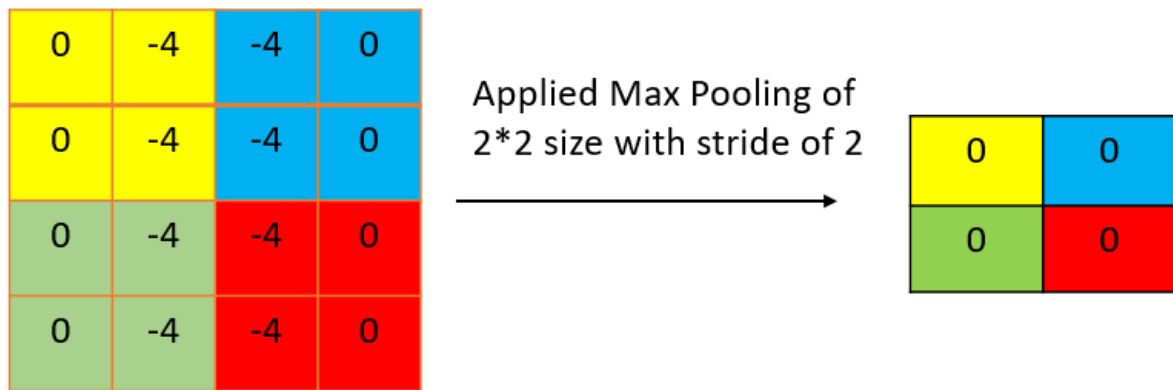


Fig 5.2.7 Applied Max Pooling of 2*2 size.

Fully Connected Layer

Till now we have performed the Feature Extraction steps, now comes the Classification part. The Fully connected layer (as we have in ANN) is used for classifying the input image into a label.

This layer connects the information extracted from the previous steps (i.e Convolution layer and Pooling layers) to the output layer and eventually classifies the input into the desired label.

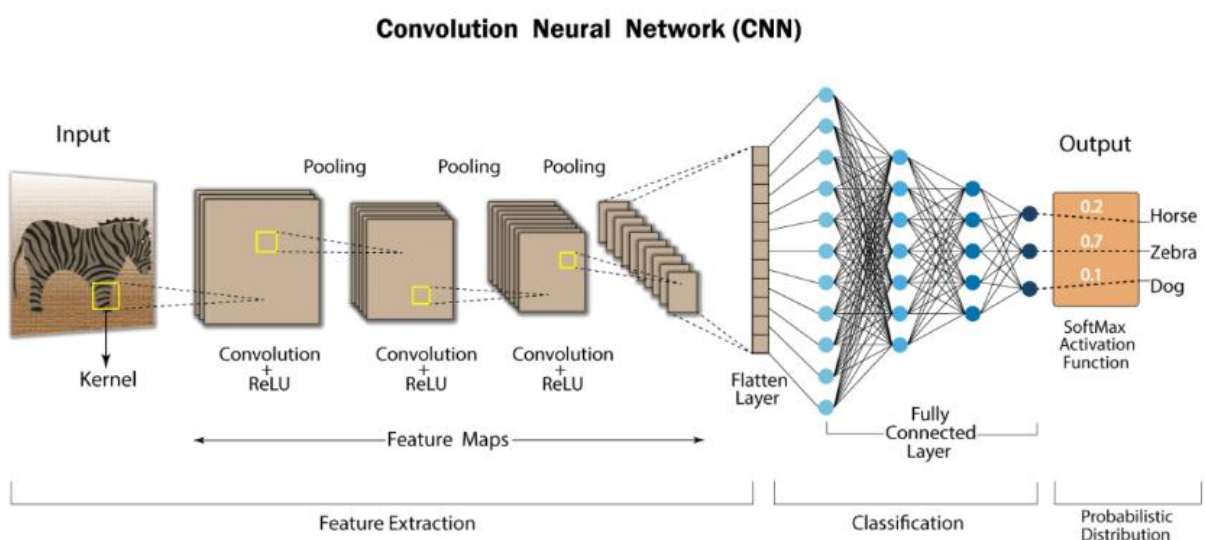


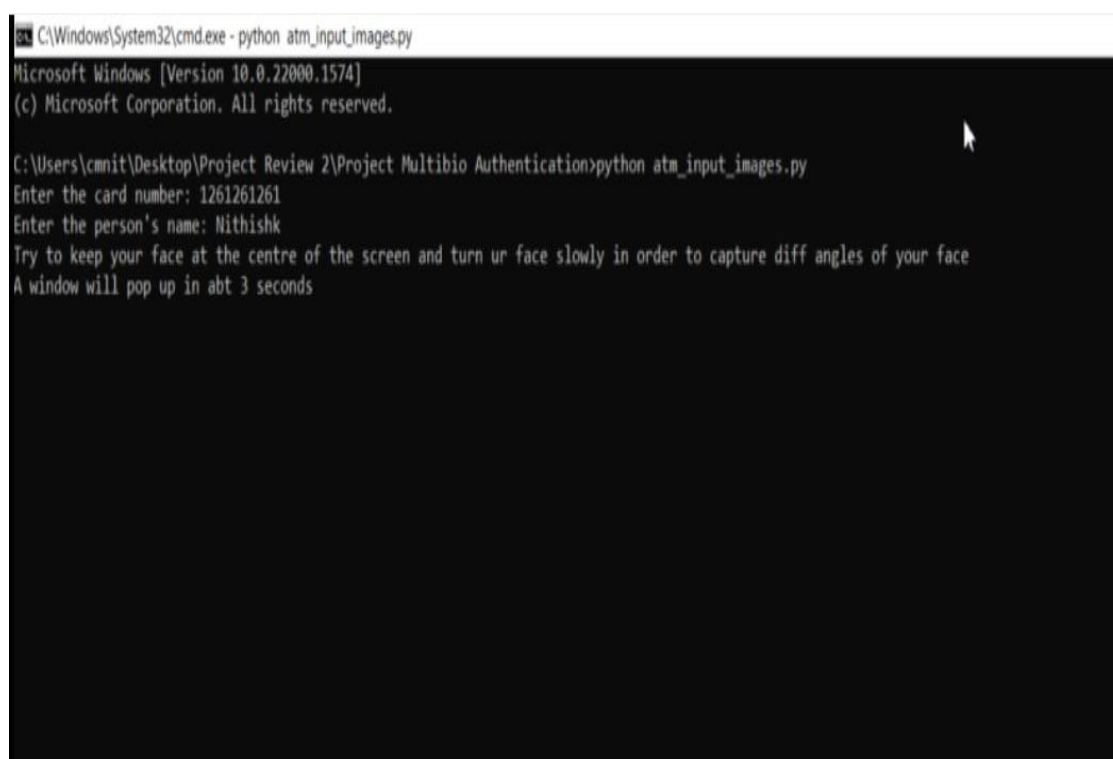
Fig 5.2.8 The complete process of CNN model.

CHAPTER 6

RESULTS AND DISCUSSION

we presented a multi-biometric system for the continuous and transparent authentication of students in eLearning platforms, describing its components and how they work. One of the main goals was to make the system compatible with an as wide as possible set of different devices and learning activities. By exploiting the combination of five biometric traits, the system recognizes students basing on something they are (presence) and something they do (interaction). Furthermore, our system is transparent from the student's perspective, since it does not require additional devices or explicit actions. This has a good potential to pose our system as a usable solution to attest that the student who is certified is the one who performs the learning activities.

6.1 Screen Shots



```
C:\Windows\System32\cmd.exe - python atm_input_images.py
Microsoft Windows [Version 10.0.22000.1574]
(c) Microsoft Corporation. All rights reserved.

C:\Users\cmnit\Desktop\Project Review 2\Project Multibio Authentication>python atm_input_images.py
Enter the card number: 1261261261
Enter the person's name: Nithishk
Try to keep your face at the centre of the screen and turn ur face slowly in order to capture diff angles of your face
A window will pop up in abt 3 seconds
```

Fig 6.1.1 Registering the user's information.

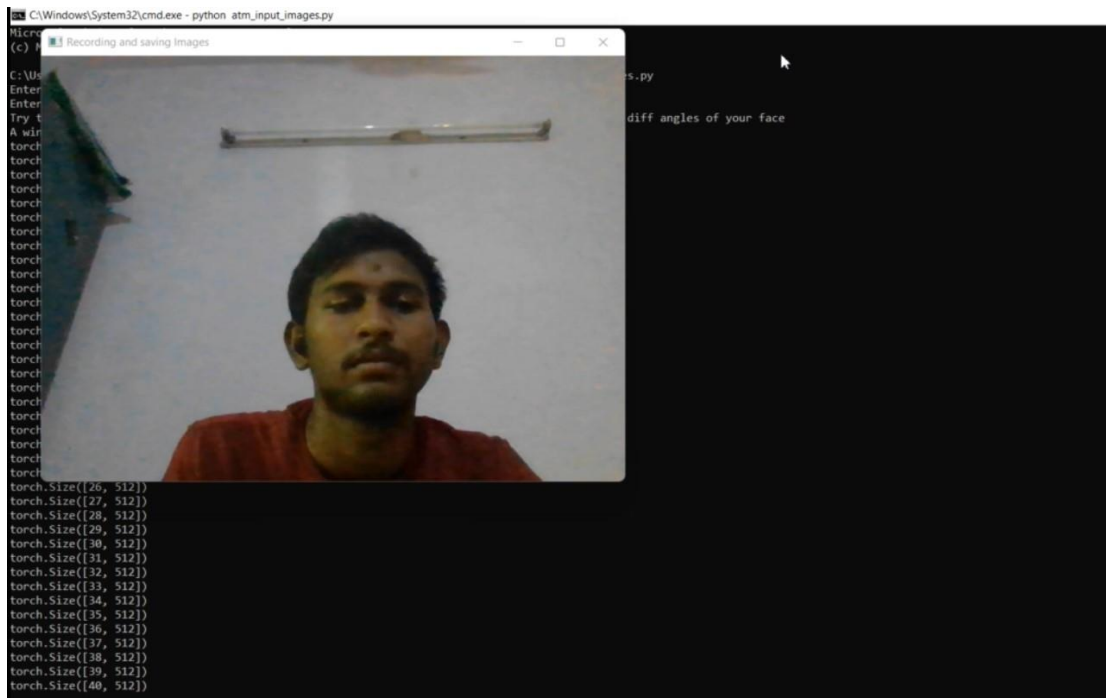


Fig 6.1.2 Capturing User's Face for verification and Matching purpose.

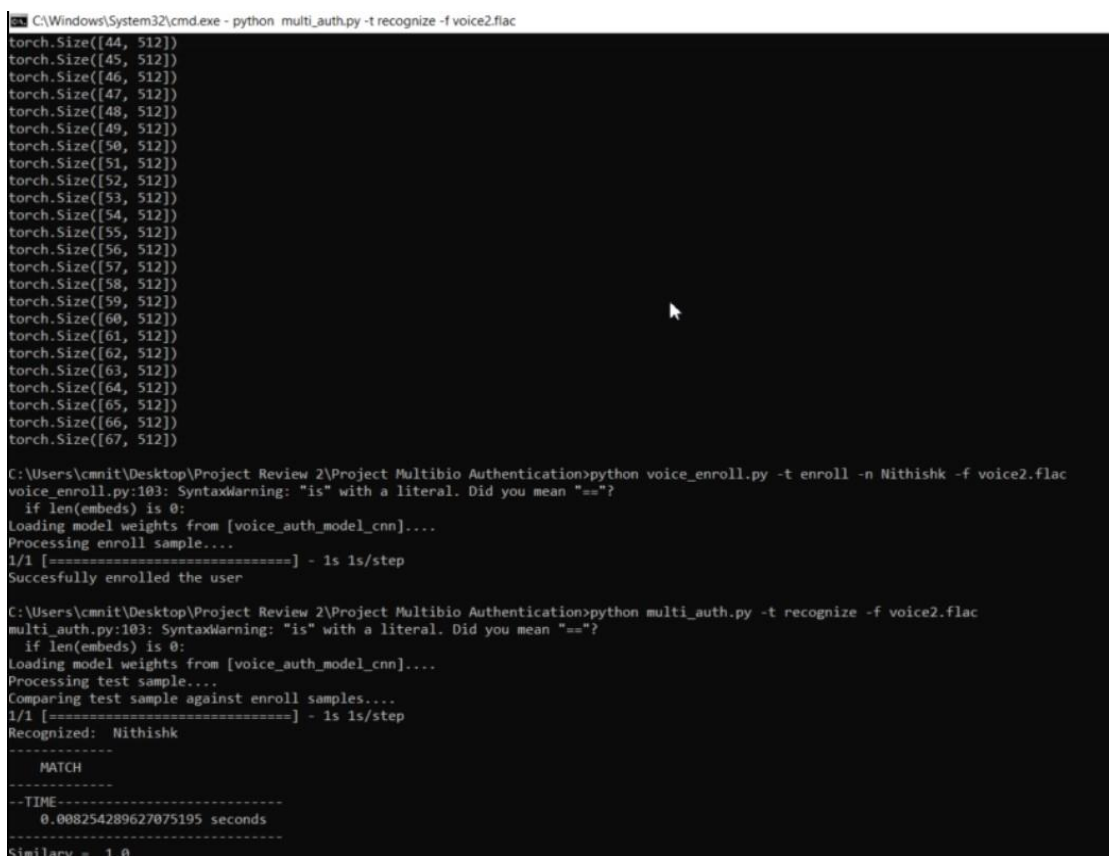


Fig 6.1.3 Comparing the Voice Files for Voice Authentication.

CHAPTER 7

CONCLUSION

In this paper, we presented a multi-biometric system for the continuous and transparent authentication of students in eLearning platforms, describing its components and how they work. One of the main goals was to make the system compatible with an as wide as possible set of different devices and learning activities.

By exploiting the combination of five biometric traits, the system recognizes students basing on something they are (presence) and something they do (interaction). Furthermore, our system is transparent from the student's perspective, since it does not require additional devices or explicit actions.

This has a good potential to pose our system as a usable solution to attest that the student who is certified is the one who performs the learning activities.

In our system, we selected a parallel architecture and a scorelevel fusion which support both speed and accuracy.

In contrast to several state-of-the-art solutions, this dynamic structure is also able to adapt to the type of device used and the type of interaction performed with it. At least one physiological biometric and one behavioral biometric are combined to recognize the student.

To manage such combination, we use the concept of temporal authentication window; the system captures data during a temporal window, then it starts the recognition. It does not perform a recognition cycle whenever a new sample (e.g. a touch gesture) is acquired.

Furthermore, each subsystem can be instantiated with other off-the-shelf algorithms, since the output is quite standard.

Besides a matching score, each one of them returns a reliability measure used to weight the contribution of the subsystem for the global response.

In this way, we can also identify which student's device is the most reliable for his/her recognition. The preliminary comparison with the other existing solutions stimulates us to perform further research.

We plan to test our system in real scenarios and investigate its integration into online proctoring systems in combination with cheating detectors. In this way, we would certify that (i) the students are who they claim to be and (ii) they take exams without cheating.

Even if we consider the e-learning context as case study, the potential applications of our authentication system are opened to other online platforms.

7.1 FUTURE SCOPE

This study examines online assessment systems as a tool, and the results of this study (characteristics of online assessment systems) can guide interpreters, decision makers, experiments and system inventors in the future selection and/or development of online assessment.

system However, since students are the users of online assessment systems, it is important to understand scholars' views on how online assessment systems reflect students and support their literacy. Thus, future research can address the impact of online grading systems on colorful academic factors.

REFERENCES:

- [1] K.M. Apampa, G. Wills, D. Argles, Towards security goals in summative e-assessment security, in: the Proceedings of the International Conference for Internet Technology and Secured Transactions, IEEE, 2009, pp. 1–5.
- [2] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, Security in online web learning assessment, *World Wide Web* 18 (6) (2015) 1655–1676 Springer.
- [3] X. Li, K.M. Chang, Y. Yuan, A. Hauptmann, Massive open online proctor: protecting the credibility of MOOCs certificates, in: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, ACM, 2015, pp. 1129–1137.
- [4] Y. Atoum, L. Chen, A.X. Liu, S.D. Hsu, X. Liu, Automated online exam proctoring, *IEEE Trans. Multimedia* 99 (2016).
- [5] A. Moini, A.M. Madni, Leveraging biometrics for user authentication in online learning: a systems perspective, *IEEE Syst. J.* 3 (4) (2009) 469–476 IEEE.
- [6] S. Asha, C. Chellappan, Authentication of e-learners using multimodal biometric technology, in: the Proceedings of the International Symposium on Biometrics and Security Technologies, IEEE, 2008, pp. 1–6.
- [7] E.G. Agulla, E.A. Rúa, J.L.A. Castro, D.G. Jiménez, L.A. Rifón, Multimodal biometrics-based student attendance measurement in learning management systems, in: the Proceedings of the 11th IEEE International Symposium on Multimedia (ISM), IEEE, 2009, pp. 699–704.
- [8] E. Flior, K. Kowalski, Continuous biometric user authentication in online examinations, in: the Proceedings of the 7th International Conference on Information Technologies, 2010, pp. 488–492.
- [9] A. Morales, J. Fierrez, Keystroke Biometrics for Student Authentication: A Case Study, in: the Proceedings of the ACM Conference on Innovation and Technology in Computer Science Education, 2015, p. 337.
- [10] L.D. Spano, G. Fenu, IceTT: a responsive visualization for task models, in: Proceedings of the 2014 ACM SIGCHI Symposium on Engineering Interactive computing systems, ACM, 2014, pp. 197–200.
- [11] M. De Marsico, D. Riccio, A new data normalization function for multibiometric contexts: a case study, in: International Conference on Image Analysis and Recognition, Springer, Berlin Heidelberg, 2008, pp. 1033–1040.

- [12] M. De Marsico, M. Nappi, D. Riccio, CABALA-Collaborative architectures based on biometric adaptable layers and activities, *Pattern Recognit.* 45 (6) (2012) 2348–2362 Elsevier.
- [13] W. Meng, D.S. Wong, S. Furnell, J. Zhou, Surveying the development of biometric user authentication on mobile phones, *IEEE Commun. Surv. Tutorials* 17 (3) (2015) 1268–1293 IEEE.
- [14] M. De Marsico, C. Galdi, M. Nappi, D. Riccio, FIRME: face and iris recognition for mobile engagement, *Image Vision Comput.* 32 (12) (2014) 1161–1172 Elsevier.
- [15] S. Barra, A. Casanova, F. Narducci, S. Ricciardi, Ubiquitous iris recognition by means of mobile devices, *Pattern Recognit. Lett.* 57 (2015) 66–73 Elsevier.

Multibio Authentication of Online Users in Proctoring And E-Learning

NITHISH KUMAR C M
B TECH INFORMATION
TECHNOLOGY
SATHYABAMA INSTITUTE OF
SCIENCE AND TECHNOLOGY
CHENNAI, TAMIL NADU
nithishmohan2002@gmail.com

VISHAL S
B TECH INFORMATION
TECHNOLOGY
SATHYABAMA INSTITUTE OF
SCIENCE AND TECHNOLOGY
CHENNAI, TAMIL NADU
vishalmuki@gmail.com

Dr P AJITHA
ASSOCIATE PROFESSOR/IT DEPT
SCHOOL OF COMPUTING
SATHYABAMA INSTITUTE OF
SCIENCE AND TECHNOLOGY
CHENNAI, TAMIL NADU
ajitha.it@sathyabama.ac.in

A. *Abstract*— Online courses have become more liked recently as a brand-new method of instructing students in remoteness literacy environment. However, as request grows, educational accademies were faced with difficulty of determining how to verify that online scholars are the persons they say they are throughout learning ventures, particularly examinations. Mortal monitoring is a un-scalable method that calls for someone to oversee every student ever. On the computraized supervisors frequently focus on a certain kind of gadget and confirm the students' attendance without taking into account their interactions with the distance learning platform. In this study, we present a multi- ralistic authentication system that is device/commerce independent and aims to constantly and translucent validate both existance and commerce. Through the use of a score-position emulsion of several realistic authentication response suc as facial, voice, touch based on the gadget The system is suitable to certify to the scholars's identification all over the literacy occurrence depending on how it is used and the commerce that is conducted with it. Our donation has a fair chance of providing workable and dependable carry on a wider range of online system tests when compared to existing alternatives.

Keywords— *Proctoring, Python IDE, SQLLITE, CNN, LSTM.*

I. INTRODUCTION

Online courses have recently become a versatile technique to instruct big teams of researchers in online learning situation. As order to rises, educational academy must contend with difficulty of evaluating its honesty of its operations in the absence of student involvement. In the settings, fraudsters taking part in online surveys and fake

IDs for other pharmaceuticals are potential hazards. Educational institutions should (i) support online students' individuality, (ii) make sure they pass tests honestly, and (iii) evaluate their performance correctly to reduce these issues. The first job, which tries to show that e-learning requirements are met by a certified learner, is the subject of this article. Typically, during online exams, the findings are only meant for academic purposes.

Typically, they do not take into account participation in other courses. Researchers can conduct web-based studies accompanied by ongoing human observation using a standard approach. This was not scaleable and is reliant in operating supervisor's mortal abilities. Other systems, such ProctorFree3 and RemoteProctorNow, do the same thing with post- or real-time analysis but at a lesser cost because they do away with the die problem. These approaches do not always hold true when researchers want to falsify data, particularly when conducting experiments. The authentication process must be visible and continuous without interfering with the student's regular health.

In this setting, numerous academic and commercial research organisations have put forth diverse.) Single-biometric systems among them typically seek to compute face and/or body signals. Because they rationalise trading a student, simply watching them won't stop them from cheating. We seek to confirm both the commodity that the student is and the stone manufacturer in any combination of business and device since facial identification is efficient but reduction of business while some other realistic authentication support business but this are insufficiently accurate on their own. Additionally, nearly all prejudices have detectors that verify their biometrics. The outcome is a multi-biometric system that is independent of device/transaction. Our approach adds a temporal authentication window to take advantage of various biometric emulsions. The association of biometric data occurs throughout a series of fixed-duration time intervals.

The information kept in that screen is address to the multi-realistic authentication system for the identification procedure when temporary window expires. This final step is to compare the overall authentication score to the receiving entrance if the score is lesser, the person can continue their reading time; if not, the system tightens access control. We dissected the reliability metrics and normalisation functions of the important points. We also made the choice to use the Quasi Linear Sigmoid (QLS) purpose to get similar and objective results for various other components. Our solution is ideally positioned to give an workable and trustworthy instrument system for various online education courses (such as participation course, quizzes) that supports the bigger bias along with relationship as compared to the already used ways.

The following benefits are provided by this paper:

- Our proposed multi-biometric system, which is not reliant on a specific gadget and considers both presence and commerce through a combination of facial, voice, and touch biometric responses based on the device used, has the potential to provide flexible and reliable support for a wide range of online tests, surpassing existing alternatives.
- In order to continually verify researchers on Personnel computer and phone while carry on the most popular forms of communication, it propose to combine a multi-biometric system into a single learning platform.
- To compare the proposed approach to the most recent authentication outcomes in the context of e-learning platforms, we map the results.

II. LITERATURE SURVEY

A. Title: *Towards security objectives for summative online assessments*

Author: Gary Wills and Kikelomo Maria Apampa

Year: 2009

Description: Confidentiality, integrity, and availability (C-I-A), which safeguard vital resources from potential dangers, may be part of a computer system's overall security objectives. Although C-I-A's security objects are well-studied, they might not be enough to meet all of the requirements for the entire e-assessment. We do not disparage the CIA's core security goals in this document. Instead, we establish security objectives that are unique to the security of an electronic summary assessment.

B. Title: *Online Exam Proctoring with Automation*

Author: Liping Chen and Yousef Atoum

Year: 2017

Description: Massive open online courses (MOOCs) and additional types of e-learning are enlarged and more well-

known. One significant barrier to the scaling of this next stage of training is the capacity to observe online remote tests efficiently. Human testing, which requires the test subject to visit the testing facility or be observed physically and acoustically through a webcam while taking the test, is now the most popular assessment method. We build more sophisticated features that categorise if a test taking person is cheat at the any point in the test by integrating the elements of continuous assessment and employing a temporal sliding window. Numerous test outcome illustrate the precision, dependability, and potency of the distant learning test shadowing platform.

C. Title: *e-learner authentication leveraging multimodal biometric technologies*

Author: C. CHELLAPPAN AND S. ASHA

Year: 2008

Description: E-learning platforms are a brand-new method of education that are gaining popularity daily. However, the issue with e-learning platforms is that not enough money is spent on certainty. User authenticity techniques can be categorised onto one of 3 groups: 1) based on the human memory store such as passwords pins, 2) based on physical device bias namely magnetic or IC cards and 3) based on realistic authentication datas. Because the first two categories cannot completely eliminate the vulnerability of being forgotten or lost, the third category currently garners a lot of attention. The fundamental issue with biometric authentication is that it contains errors when comparing biometric data and extracting human traits. When a single biometric verification technique is unable to provide the needed degree of reliability, multi-biometrics can be used to increase the reliability of biometric verification. In order to serve diverse e-learning applications that demand user authentication, this article suggests the usage of numerous biometric authentication methods.

D. Title: *Student Authentication Using Keystroke Biometrics: A Case Study*

Author: Aythami_Morales

Year: 2015

Description: In this essay, a case study of the use of biometric technology for student authentication is presented. We analyse the subtleties of a keystroke dynamic algorithm used to authenticate students during a live online exam for a course on basic computer knowledge System Analysis.

3.1 Existing system

Despite the fact that many educational institutions have implemented computer-based collaborative learning during the past 10 years, there are still gaps that restrict their ability to foster collaborative learning. The issue with e-learning systems, however, is that not enough money is spent on security. Additionally, one of the biggest challenges in an

online learning environment is authenticating students, particularly when it comes to e-exams. The fundamental issue with biometric authentication is that it contains errors when comparing biometric data and extracting human traits.

Disadvantages:

- A new mapping function that cannot get beyond the drawbacks of conventional methods is a normalisation function.
- Students' eyes may become fatigued since they must look at screens all the time.
- Why Learning in a classroom is engaging by nature; doing it while seated in front of a computer or smartphone is dull.

3.2 Proposed System

We suggest a multi-biometric system that can continually and transparently validate both presence and commerce, regardless of the device or type of business. The system may establish the identification of the learner during the learning process by performing point-level aggregation of multiple biometric responses (facial, voice, and touch) based on the device in use and contact with it. Our addition has a strong possibility of offering flexible and dependable support for a larger range of web experiences, according to an initial comparison with existing approaches.

Advantages:

- Because nearly all devices have sensors and a process to track such biometric data, the system can use them to validate the student's identification.
- Because subsystems operate concurrently, the overall response is calculated using the speed of the slowest detection algorithm. As a result, global authentication time is shortened.
- Because no subsystem knows anything about any other subsystem and because the matching points are normalised using the QLS function, the system can integrate standard algorithms.

III. METHODOLOGY

The persistent student identification method that is suggested in this paper is described in this section. Three biometric subsystems in the system can recognise touch, voice, and face. Each delivers a couple of values: the 1st is the interval determined by comparing sensor model with purported pupil model, and the second is the subsystem's level of distance-related dependability. The compatibility scores of all subsystems are added and weighted according to their confidence metrics to determine the overall verification response. The global authenticated response is then contrasted to an entrance of acceptability; if it is lesser, the scholar keeps studying; if not, the system tightens access restriction.

We can outline the most typical features of the offers multi-realistic authentication device as follows.

- Since nearly all devices have sensors and algorithms to track such biometric data, the system can utilise these to validate a student's identification.

- The implementation time was the slowest detection method is used to compute the overall response since subsystems operate in parallel. As a result, global authentication time is shortened.

- Because no subsystem knows anything about the others and the matching points are normalised using the QLS function, the system can integrate standard algorithms.

- The approach employs a model gallery of all student data and SRR metric matching. The QLS function is used to normalise reliability data.

- Point-level aggregation is used by the system to strike a balance between the computational cost of the aggregation procedure and the amount of data available for authentication.

4.1. Biometric authentication subsystems

According to the kind of biometric, we discuss in the sections that follow how each subsystem implements its own modules.

4.1.1. Face-Based authentication subsystem

Almost all of today's technology includes an on-board camera, whether it be a desktop or mobile device. We can easily snap facial images because the student is often in front of the tablet while reading. Throughout a temporal frame, the subsystem randomly captures face images. When the time limit runs out, sample discovery happens simultaneously. For that goal, we employ a framework based on the methods. Using the Viola-Jones approach, the area of the image containing the face is found. The subsystem responds with $SRR1 = 1$ and $T1 = 1$ if the number of recovered faces is not exactly 1. In the event that this does not occur, it performs a covert normalisation phase based on Active Shape Model (ASM), one of the techniques that strikes a balance between delicateness and processing speed. This is crucial since the pupil is obviously verified without demanding that he or she continually face the camera; as a consequence, disguise variations often occur. The implementation of anti-spoofing countermeasures is necessary given the possibility of infidelity in our environment. Additionally, we use a matching technique based on a localised interpretation of the spatial connection between the face inquiry analyzed and the claimed identity's face template. The technique makes use of 3D geometric invariants. The subsystem determines that only the asserted student is present in the acquired inquiry samples if all the student's match values for all of the collected inquiry sampling are higher than a predetermined threshold. The typical of all the matched scores are given back as a T1 value which has been corrected within range and translated to a distance metric in the identical range by subtracting 1.

The point on the vector of the inquiry with the associated score that is nearest to the norm is identified. The compatible scores from the face tests are ranked. This point vector is used to determine the SRR1 index.

4.1.2. Voice-based authentication subsystem

To record audio samples, a microphone is used. This detector is present in almost all living creatures, and they all have ways to record the information it generates. Due to the nature of our problem, the subsystem can perform textbook-independent verification as it cannot foresee the student's future choices. Silence and other irrelevant gaps are removed from clips utilising the audio performance sensor. The audio input is tested at a rate exceeding 10,000 Hz in order to minimise aliasing concerns during the analog-to-digital translation and catch nearly all of the energy sounds created by humans. The subsystem extracts a parametric representations from a speech waveform using Mel frequency Cepstral Components (MFCCs), one of the most commonly used approaches in modern automatic speech recognition systems. The Mel scale's inversely spaced frequency bands mimic the response generated by the mortal audile apparatus. The point birth is carried out on short timeframes while presuming that a small member of speech is considerably more immobile in order to improve the modelling phase and the depiction of the sound quality. The vector of the MFCCs that was excluded from the inquiry is contrasted with the design of the claimed identity in the database. Because they are so easy to use and delicate, the subsystem uses quantization of vectors codebooks for that reason. The method allocates acoustic matrices to a select few spatial regions. Each area is a grouping that, symbolically, is symbolised by its core, and each grouping is linked to a specific student. The collection of all the devices is referred to as a codebook. During the registration phase, the subsystem develops a metaphor for each student, and during the verification phase, it determines the distance between the stated pupil's metaphor and the auditory direction that represents the inquiry (a location in a set of devices). To be harmonious, the distance value is corrected in the range and provided by the component to be the T2 value.

4.1.3. Touch-based authentication subsystem

Because they strike a solid balance between usability and security and because mobile devices are so widely used, touch-based recognition systems are becoming more prevalent in the literature. Modern mobile operating systems offer common APIs that may be used to access raw data about touch behaviour. Other libraries have been created to detect touches on mobile webpages, most frequently in JavaScript. because the two primary touch actions (tap and swipe) may be used to ingest raw data. Furthermore, it just needs information from the application, unlike other significant algorithms. This quickens the learning process and makes it simple to update the student model as needed. This technique is better suitable for our system's specific needs because to its speedy registration (usually, 11 gestures are sufficient for teaching these classifier) and great accuracy. The learnt filters serve as a representation of the

touching data that our gadget maintains for each learner. Several successive user gestures are shown to classifiers that have already been trained for the targeted student during the process of verification. The average probability derived by the two classifiers serves as a representation for the T3 score. The value is first normalised to the range [0, 1], after which it is subtracted from 1 to get a distance in the same range.

4.2. Subsystem response reliability

In the authorization response, each subsystem provides (i) an appropriate number and (ii) a related trust level. A dependability metric that considers the environment in which match scores are calculated rather than the quality of the input data leads to better performance. The authors developed a biometric-free trustability function for a photos-dependent recognition system. They see the arranged collection of identities generated by the verification process like a cloud; the more similar the rating is to the initial identification provided, the less credible the response. The density ratio can be used to model this concept. To handle the calculation of score dependability, each subsystem in our presentation implements a distinct variation of this idea. The system uses the candidate pattern, or the first identification returned in every identification scenario, as the initial collection that is distinct while all other patterns are employed as fake patterns since each subsystem has a gallery of every pupil's patterns. That's how the idea is presented. The density ratios I of p_i at A_i is defined as follows if a pupil s_k requests a sensor p_i with a registered design g_{ik} and an authenticity of its parts A_i with the cheating G_i :

$$\varphi_I(p_i, s_k) = 1 - |N_b|/|G_i| \quad (1)$$

Where:

$$N_b = \{g_{ij} \in G_i | d(p_i, g_{ij}) < r * d(p_i, g_{ik}) \wedge j \neq k\} \quad (2)$$

where the radius r is. The SRR value, also known as the SRR, is obtained by further procedures once the value i has been calculated. employing the reliable benchmark of the density ratio i . The QLS function brings the result into the [0, 1] range. Through doing that, we may clarify the substantial difference in answers that the setting where the data was collected caused.

4.3. Fusion schema

Five biometric characteristics are merged at the point level in the method suggested in this study in order to increase authentication performance. This is generally regarded as the optimum balance between the intricacy of the fusion process and the quantity of information available. Each subsystem in our system gives back a value pair. The first is the distance in the range [0, 1], which comes from comparing the sensor model with the necessary doll model. The second shows the degree of confidence a specific subsystem score has in the range [0, 1]. while no information is received for the relevant biometric, the confidence level is taken to be 0, allowing the associated

match point to be ignored while figuring out the overall answer. It has been shown that in order to have a better recognition result, the confidence level connected with the response should be measured against a larger distance, which often indicates that the user is not who he claims to be. Even if the distance is minimal, the same idea still holds true. The SRR measurements generated by the subsystems are employed in our system's composition strategy to weight the match points. Five distinct trust standards, notably SRR1 as face, SRR2 as voice, as well as SRR3 as touch, may be explicitly identified. They are used as weights to obtain a weighted total equal to the global length the system generated. For the result to be constant, the weights must total up to 1. To arrive at their overall value, the SRR scores are averaged.

$$SRR\sigma = \sum_{i=1}^5 SRR_i \quad (3)$$

Three reaction points are also present: T1 as face, T2 as voice, T3 as touch and T as the mouse, The findings for all of network core T are the following when the equation from [1] is extended:

$$T = \sum_{i=1}^5 SRR_i / SRR\sigma * T_i \quad (4)$$

If the student's global authentication response is below a predefined acceptance threshold, the platform allows them to keep up their studies; if not, it imposes limits on access.

4.4. Integration in e-learning platforms

This section explains how the multi-biometric system presented in this paper may be integrated into an e-learning platform. Additionally, we show how the parts are distributed across the client's and client sides. defines their connection; Since the integration strategy raises the issue of how much data needs to be gathered before detection begins, we introduce and outline the concept of a time identification window. We offer global reliability measurements that are related to the system's ability to identify a particular student during a certain type of contact with a particular piece of equipment.

4.4.1. Integration methodology

The process of integration The web/mobile client of the online education platform's administrative modules must be incorporated with the user side of the system. On the server side, there is a multi-biometric system and a backend for an e-learning platform. Through the administration module, the multibiometric system running on the e-learning platform's server and client may connect with one another. Every biometric feature's raw data must be collected by it, and it is responsible for sending the data to different biometric systems for processing. Additionally, it controls the global authentication response of the multi-biometric system. Our software and the server-side backbone of the e-learning platform don't need to be dependent on one another. The proposed an improved-biometric system receives the initial input, performs identification, and then delivers a global authentication response to the management module. As an observer points out, we made the decision not to use the

entire multi biometric systems on the consumer side to acquire the data.

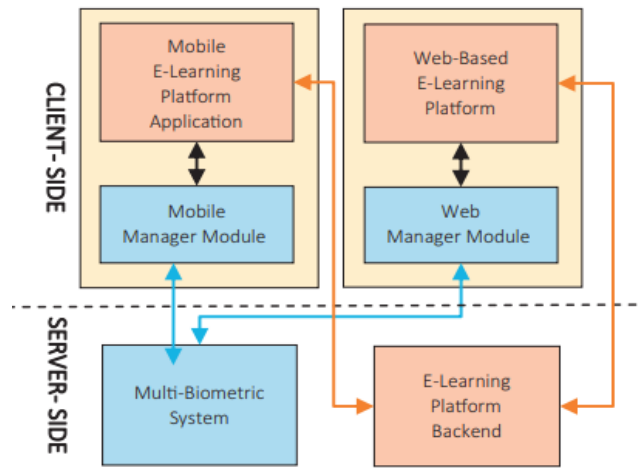


Fig. 1. Plans for integrating our system with a platform for e-learning.

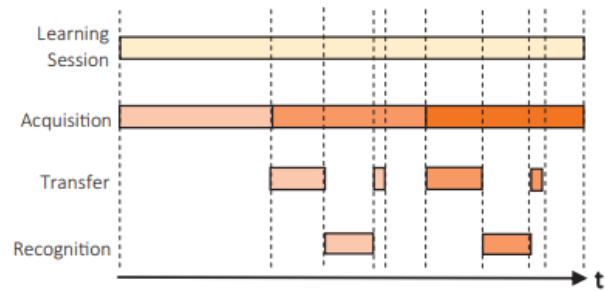


Fig. 2. An illustration of using temporal windows for biometric identification.

flexibility in system administration and light client device workload.

4.4.2. Temporal windowing of the authentication process

Current realistic authentication often accomplish continuous authentication by quickly acquiring and instantaneously identifying a new sensor (such a touch gesture or face picture). Because (i) doing the extraction of features, matching, and merging phases each time the data is obtained requires a lot of computing work, and (ii) the reduction in the quantity of information available for biometric identification, this is rather challenging for our system. cycle, particularly for behavioural biometrics, which need information gathered over time for better matching, and (iii) instability and limited effect of the fusion phase as a result of issues at the second point. Our multi-biometric system employs timed authentication windows in an effort to reduce them. In the management module, the initial data is collected throughout a series of fixed-duration time frames. The raw data gathered during this time frame is transferred to numerous biometric systems for identification once the

time window has passed. The management module begins gathering data for the next time range at the same time. The management module replies appropriately after receiving an authentication response from the multi-realistic authentication system, enabling the student to resume their studies or remove access restrictions. If the sum of the times in both of the initial points is smaller or equal to the size of the time window, the multi realistic authentication system can utilise the data collected for that window before delivering the data collected for the subsequent window. The major disadvantage of this tactic is that the cheater is able to interact with the online educational system from when the browser tab closes until the worldwide authentication response is obtained.

5.1 Convolutional Neural Network (CNN)

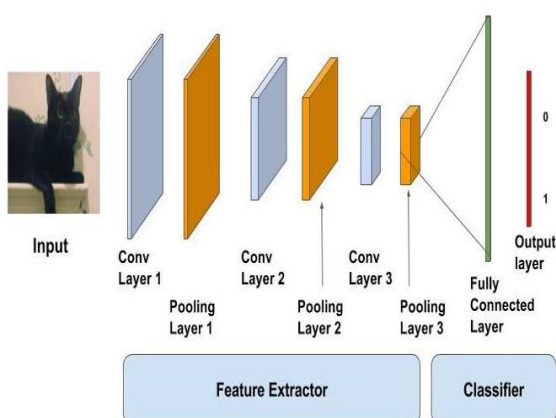
A. Introduction to CNN

A deep learning system specifically created to work with pictures and videos is termed as convolutional neural network. It uses photos as inputs to extract and learn image features, then uses those learnt features to categorise the images.

The visual cortex, one component of the human brain, served as the model for this programme. The area of the human brain in charge of analysing visual data from the environment is known as the visual cortex. It includes a number of levels, and each layer serves a different purpose, such as extracting different information from images or other visuals. Once all the information from the various layers has been merged, the picture or visual may then be analysed or classed.

A typical CNN model appears like follows:

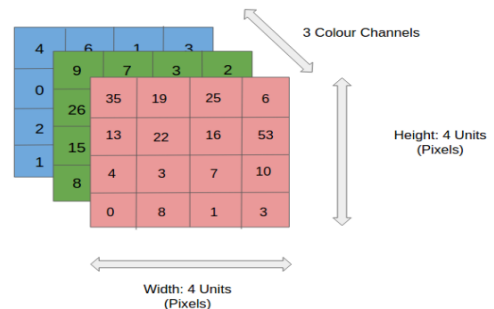
- Input layers
- Convolution layers + Activation function
- Pooling layers
- Fully Connected Layers



1) INPUT LAYER

This is our input image, as the name implies, and it might be either RGB or grayscale. Pixels in each picture range from 0 to 255. Prior to submitting them to the model, we must normalise them, or transform the range from 0 to 1.

An example of an input picture containing three channels, or RGB and pixel values, is shown below.



2) CONVOLUTION LAYER

To be able to gather or identify the properties of the input picture, a layer of convolution provides an enhancement to it. Multiple applications of the technique result in the creation of a feature map that aids in the classification of the input picture. Let's use an example to better grasp this. We create a 2D input picture with regularised pixels for simplicity's sake.

$$\begin{array}{|c|c|c|c|c|c|} \hline 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 \\ \hline \end{array} \quad 6 \times 6$$

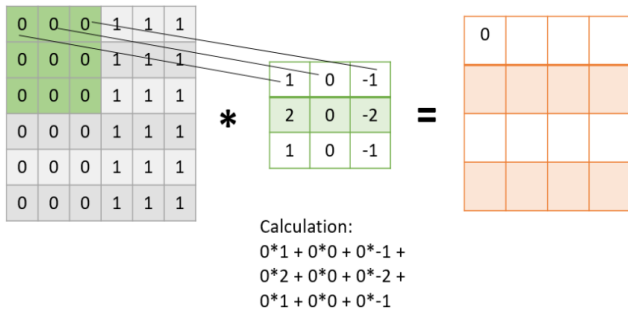
$$* \quad \begin{array}{|c|c|c|} \hline 1 & 0 & -1 \\ \hline 2 & 0 & -2 \\ \hline 1 & 0 & -1 \\ \hline \end{array} \quad 3 \times 3$$

$$= \quad \begin{array}{|c|c|c|c|} \hline 0 & -4 & -4 & 0 \\ \hline 0 & -4 & -4 & 0 \\ \hline 0 & -4 & -4 & 0 \\ \hline 0 & -4 & -4 & 0 \\ \hline \end{array} \quad 4 \times 4$$

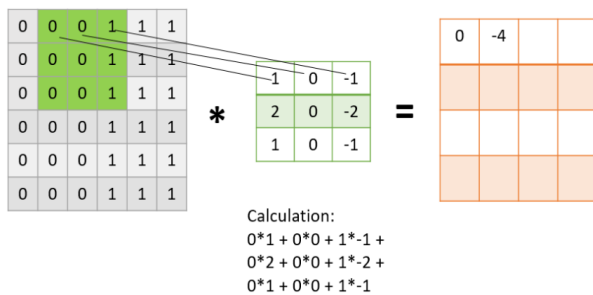
In the image above, we used a 3x3 filter to highlight specific elements on an input image that was 6x6 in size. In this example, we've just used one filter, but in reality, many of these kinds of filters are used to extract information from images.

We obtain a 4x4 point chart with some information on the input picture as a result of applying the algorithm to the image. Such point charts are frequently produced in operational settings.

Let's look at some of the calculations used to create the point chart in the image above.



As seen in the figure above, the first phase involves adding sludge to green stressed area of picture, multiplying the image's pixel scores by the filter values (represented by the lines in the image), and adding the results to obtain the final value. The sludge is modified by one column in the following phase, as seen in the image below. A step is a leap to the following column or row. In this example, we take step 1, which implies we move one column.



This is how a sludge with a stride of one moves through the entire picture.

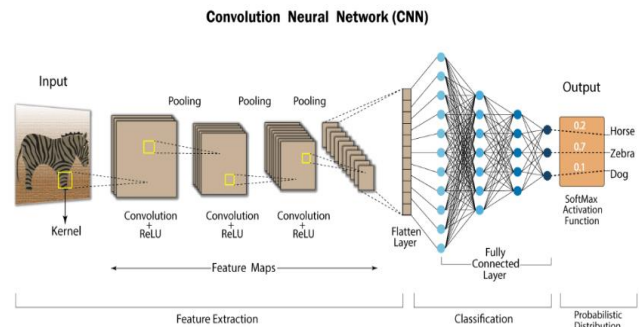
3) Pooling Layer

The pooling layer, which is designed to decrease the dimensionality of the feature map and preserve crucial details or characteristics of the input picture, is applied after the complexity layer. This speeds up calculation time. By using a fleck, one may produce a reduced resolution interpretation of the input that yet preserves significant or substantial portions of the original image. Maximum Pooling and Average Pooling are the two most popular forms of pooling. How Max Pooling functions is seen in the graphic below. Applying the join using the function chart from the previous example. Here, step 2 and a merging layer of size 2*2 are applied.

4) Fully Connected Layer

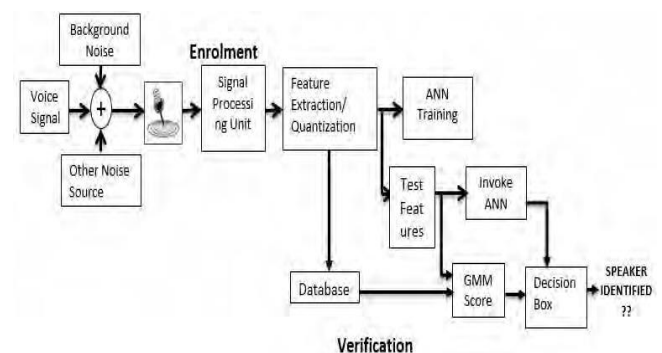
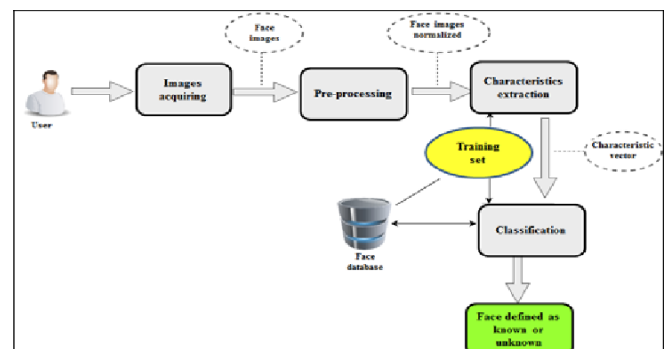
We've used the point birth method up until this point; the bracket component is next. The input picture is classified into a marker using the Fully connected subcaste (as in ANN). This subcaste links the data that was removed from the last method (ex. the complication subcaste & Pooling layers) to the affair subcaste, which in turn categorises the input into the requested marker.

In the figure below, which is being presented, you can see the entire CNN model process.



IV. SYSTEM DESIGN

6.1 Architecture Diagram



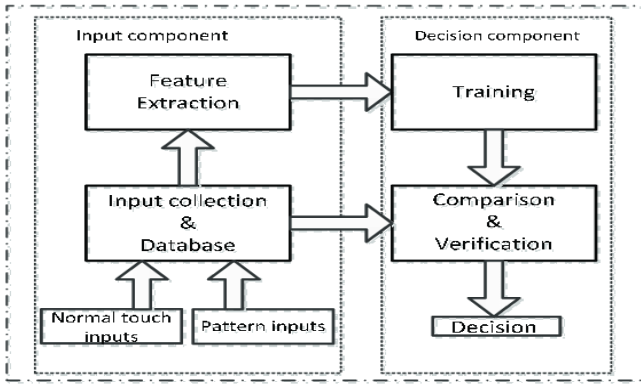
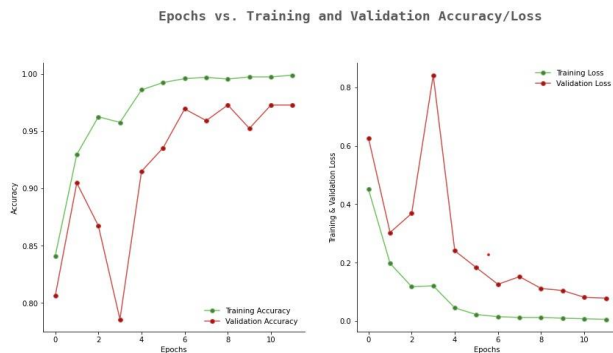


Fig. 6.1.1, 6.1.2 & 6.1.3 The tasking-biometric system that is being postulated's reference layout.

V. RESULT AND ANALYSIS

In this research, we introduced and a tasking-biometric system was suggested for the open and ongoing verification of those enrolled on platforms for e-learning. Making the system compatible with the broadest range of potential biases and learning conditioning was one of the key goals. The technology recognises scholars based on the commodities they are (presence) and do (commerce) by combining the five biometric qualities. Additionally, as our method doesn't exhibit new bias or unambiguous behaviour, it is transparent from the standpoint of the student. This has a strong chance of putting our method forward as a workable outcome to certify that the certified student is the one who actually conducts the literacy conditioning.



VI. CONCLUSION

We chose a parallel architecture and score level fusion for our system since they offer both speed and accuracy. Unlike many cutting-edge systems, this dynamic structure may change depending on the device being used and the sort of contact being made with it. To identify the student, at least one behavioural biometric and one physiological biometric are integrated. We employ the idea of a temporal authentication window to control such a combination; the system collects input during the window before beginning the recognition. Every time a new sample is collected, it does not go through a recognition cycle. Since the output is very standardised, each subsystem may also be represented using other commercially available techniques. Every one of them also generates an equivalent score and an accuracy measurement, which are used to evaluate how much every

component contributed to the final result. By doing this, we can also determine which student's equipment is the most accurate in recognising him or her.

The first comparison with the various solutions in use motivates us to conduct more investigation. We intend to test our innovation in actual situations in addition to looking at its integration into proctoring platforms with cheating detectors. We could certify that these learners are who they claim to be and that they are taking the examinations honestly by doing this. We utilise the setting of e-learning as a case study, but our authentication mechanism may also be used on various other websites.

VII. FUTURE SCOPE

In this study, online assessment systems are looked at as a tool, and the findings (characteristics of online assessment systems) can help interpreters, decision-makers, experimenters, and system developers choose and/or build online assessment systems in the future. Online assessment systems are used by learners, thus it's important to understand scholars' viewpoints on how these instruments reflect students and improve their literacy. Future studies might therefore examine how online grading systems affect other academic variables.

VIII. REFERENCE

- [1] K.M. Apampa, G. Wills, D. Argles, Towards security goals in summative e-assessment security, in: the Proceedings of the International Conference for Internet Technology and Secured Transactions, IEEE, 2009, pp. 1–5.
- [2] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, Security in an online website learning assessments and protocols, *World Wide Web(www)* 18 (6) (2015) 1655 to 1676 Springer.
- [3] X. Li, K.M. Chang, Y. Yuan, A. Hauptmann, Massive open online proctor: protecting the credibility of MOOCs certificates, in: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, ACM, 2015, pp. 1129–1137.
- [4] Y. Atoum, L. Chen, A.X. Liu, S.D. Hsu, X. Liu, Automated online exam proctoring, *IEEE Trans. Multimedia* 99 (2016).
- [5] A. Moini, A.M. Madni, Leveraging biometric for online users authentications in online user learning systems: a systems perspective, *IEEE System. J.* 3 (4) (2009) 469–476 IEEE.
- [6] S. Asha, C. Chellappan, Authentication of e-learners using multi-modal bio metrics technologies, in the Proceedings of the International Symposium on Bio metrics and Security Technologies, IEEE, 2008, pp. 1–6.
- [7] E.G. Agulla, E.A. Rúa, J.L.A. Castro, D.G. Jiménez, L.A. Rifón, Multimodal biometrics-based student attendance measurement in learning management systems, in: the Proceedings of the 11th IEEE International Symposium on Multimedia (ISM), IEEE, 2009, pp. 699–704.
- [8] E. Flior, K. Kowalski, Continuous bio metrics of user authentication in an online exams systems, describing that in the Proceedings with 7th International Conference on Information Technologies, 2010, pp. 488–492.

[9] A. Morales, J. Fierrez, Keystroke Biometrics for Student Authentication systems: A Case Study is describing that in the Proceedings of the ACM Conferences on Innovations and Technologies in the Computer Science Education system, 2015, p. 337.

[10] L.D. Spano, G. Fenu, IceTT: a responsive visualization for task models, in: Proceedings of the 2014 ACM SIGCHI Symposium on Engineering Interactive computing systems, ACM, 2014, pp. 197–200.