REPUBLIC OF TURKEY

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Information Technologies

DESIGN A SYSTEM FOR CHEATING DETECTION IN ELECTRONIC EXAMINATION

Alaa Jabbar HAFI

Master's Thesis

Supervisor

Asst. Prof. Dr. Sefer KURNAZ

Istanbul, 2022

DESIGN A SYSTEM FOR CHEATING DETECTION IN ELECTRONIC EXAMINATION

Alaa Jabbar HAFI

Information Technologies

Master's Thesis

ALTINBAŞ UNIVERSITY

2022

The thesis titled DESIGN A SYSTEM FOR CHEATING DETECTION IN ELECTRONIC EXAMINATION prepared by ALAA JABBAR HAFI and submitted on 18/05/2022 has been **accepted unanimously** for the degree of Master of Science in Information technologies.

Asst. Prof. Dr. Sefer KURNAZ

the Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Sefer KURNAZ	Faculty of Engineering and Architecture, Altinbas University	_____
Asst. Prof. ABDULLAHI ABDU IBRAHIM	Faculty of Engineering and Architecture, Altinbas University	_____
Asst. Prof. Dr. serdr KARGIN	Faculty of Engineering and Architecture Electronics and Communication Engineering, Beykent University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.
Submission date of the thesis to Institute of Graduate Studies: ___/___/___

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Alaa Jabbar HAFI

Signature

ACKNOWLEDGEMENTS

I might want to thank my administrators: Asst. Prof. Dr. Sefer KURNAZ Please let me express my profound feeling of appreciation and gratefulness to both of you for the information: direction and unrestricted help you have given me. I want you to enjoy all that life has to offer and further achievement and accomplishments throughout your life.

ABSTRACT

DESIGN A SYSTEM FOR CHEATING DETECTION IN ELECTRONIC EXAMINATION

Hafi, Alaa Jabbar

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Asst. Prof. Dr. Sefer KURNAZ

Date: May/2022

Pages: 49

An advanced and the good education system is the backbone of any country's progress. Only by having very valuable students in your country and gaining notoriety for their talents and efforts will you be able to establish a high international reputation. In order to achieve this, an education system must be fraudulent, so that unworthy students do not get the places they do not deserve. The objective of this study is to design a system to avoid fraud on the basis of eye movement in examination rooms. The system finds people from the scene and then identifies and recognizes them. The following step consists of eye detection and eye movement monitoring to examine the student or not in the fraud. The technique is widely used in educational and business establishments, wherever examinations have been carried out.

Keywords: Online Exam, Eye’s Detection, Cheating, Eye Movement, Eye Tracking.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

ANN	:	Artificial Neural Networks
DARPA	:	Defense Advanced Research Projects Agency
DoS	:	Denial of Service
IDS	:	Intrusion Detection System
KDD	:	Knowledge discoveries in Databases
k-NN	:	k-Nearest Neighbor
NSL	:	Network Security Laboratory

1. INTRODUCTION

1.1 INTRODUCTION

The ICT has been witnessing rapid transformations in recent years and has had a direct influence on human life, especially in education. ICT has a multiplier impact in the education sector by improving the education of students and offering them different talents, targeting underprivileged students, and those in rural and remote communities, in particular. In combination with cheaper and more responsive technologies, Interactive instructional software is used to improve the connection between students and educators and to improve the level of information by making it more available. E-learning has since been highly common and broadly accepted by colleges and educational organizations in the last few years. This allows you to have knowledge whenever and whenever students require it online. That's why web-based learning or online learning is sometimes named. Learning assessment is the mechanism by which learners and their instructors look for and evaluate evidence to make it possible to determine when students understand, where they ought to be taught and how best to get there [1]. The evaluation is one of the most important aspects of schooling. During the course of any e-Learning course it is relevant. Assessment is characterized as a group of activities like research, problem solving, collective and individual project creation, conversation involvement and so on. This could be combined into an evaluation device. Assessment work is used to measure the data gathered on learning performance and assessment of students to simultaneously validate information gained through the learning phase and represent the teaching effectiveness of teachers [2, 3]. The most often used distance test or e-exam is to evaluate student learning. It is also an effective way to carry out an exam. E-examinations are a means to ask students who are not physically there, for example, in a school. They are based on random questions per student with a fixed time period to be answered [4]. In addition, the time for manual paper correction is saved or reduced and paper processing is saving, thereby preserving the environment. E-exam provides teachers with new challenges; in particular, how to avoid students cheating. Cheating on examinations at both classes was a common practice in the country. There are different patterns of hacking, including copying a reply from a textbook, finding responses on the Internet, talking about e-mail, or

chatting messages and illegal examination instead of authentication [5]. In consequence, electronic learning institutions rely on the test phase during which students under controlled condition take a face-to-face assessment at a physical site assigned to the student's name on the university campus [6]. This, however, contradicts the idea of e-learning, which reduces time and space between students and the medium of learning. To be able to take the examination each student must be present physically [7]. This study examined any kind of system used to identify or deter cheats in an E-exam and resolves this issue [8]. Cheating detection and prevention needs human involvement (i.e. the presence of a proctor). Until beginning the examination, the protocol should authenticate student IDs [9]. This control is not sufficient, though. Continuous authentication is quite important in the examination session [10]. We will need an ongoing supervision and management mechanism for all students during the examination [11]. Then we will also study how the E-exam issue can be resolved through avoidance and identification [12]. One of the mechanisms intended to secure personal identification is continuous authentication [15]. It tries to see whether the users are the same and to check if the new user is the same. In contrast to face-to-face tests, E-exam doesn't have proctors or screens. They are kept in a separate remote area that is unregulated. In order to monitor the identity of online students, authentication goals in E-exam are therefore essential because they play a key role in protection [13, 14] In order to continuously authenticate the examiner, fingerprints and eye monitoring can be used. The authentication of fingerprints relates to the automatic way to check the match of two human fingerprints. Identification of fingerprints is one of the most popular and reported biometrics, since it is unique and consistent over time. Fingerprint recognition has 2 stages: registration in which the user characteristics of a fingerprint are calculated and processed in the database; and checks in which user characteristics of fingerprint are measured and contrasted with the database prototype. Face trace is the method from which either the point of view of the eye or the movement of the eye with respect to the head is measured. The coordinates of your eye gaze are calculated for a screen and represented by a pair of (x, Y) co-ordinates in the screen coordinate system [45]. Another technique that is intended to be investigated in order to track a pupil when conducting an E-exam is online proctor (E-proctor). The task of the e-projector is to detect fraud during the E-exam. The e-exam administration framework is an application included in this study to identify and deter fraud in E-exam by utilizing the visual C# and SQL

servers databases. A fingerprint reader and Eye Tribe Tracker are used to authenticate the examiners, to consistently ensure that the examiners appear to be the person who is examined. E-exam management system Therefore, the examiners' position may be classified as cheating or not cheating by two parameters: the average time the examiner is off-screen and the amount of times the examiner gets out of the screen.

1.2 PROBLEM STATEMENT

Cheating on examinations at both classes was a common practice in the country. In the last decade, several reports have been done on student misconduct and on how the University should try to tackle this issue [6]. E-exam also does not fix the dilemma of cheat. Cheating detection and prevention needs human involvement (i.e. the presence of a proctor). Before beginning the test, this proctor has to physically authenticate student ids. But that isn't enough; during the examination period, we need continuous authentication. We will need an ongoing supervision and management mechanism for all students during the examination. Then we will also study how the E-exam issue can be resolved through avoidance and identification.

1.3 OBJECTIVES

This research is primarily concerned with the implementation and architecture of a method that can either regulate the cheating in E-exam:

i. Continuous authentication, a way to ensure that the authenticated individual only takes the examination during the whole examination sessions.
ii. Use internet suppliers to identify and deter fraud in an e-test using appropriate methods.

1.4 PROJECT SCOPE

The scope of the study will focus on the following three major factors:

i. We examined both aspects of strategies for e-exam cheating with a view to achieving these objectives.

ii. Username/password and fingerprints are required to authenticate the examiner so they can participate in an e-examen session.

iii. During the e-exam session eye monitoring is included. The prover is a technique which the student will observe by camera while he/she takes an e-exam.

1.5 THESIS OUTLINE

Chapter 1 explains the motivation of science, the definition of issue and the method of this research to tackling the problem.

Chapter 2, This section presents current study studies to resolve the problems approaches utilized by students for E-exam cheating and to continually authenticate the pupil during the examination.

Chapter3, Online exam Application for the identification of the face to detect deception by fake name or party attendance and even for the eye monitoring of anyone who looks at the far right or at the left not to read something on their screen.
Chapter 4, Simulations Results

Chapter 5, Conclusions and Future Work

2. LITERATURE REVIEW

2.1 INTRODUCTION

This section presents current study studies to resolve the problems approaches utilized by students for E-exam cheating and to continually authenticate the pupil during the examination.

2.2 CHEATING

Students take tests using a lot of cheating tactics. Faucher and Caves[4] have proven the occurrence of fraud via the provision, receipt, receipt and examination. In addition, they have presented mechanisms for detecting and preventing fraud, and the intellectual credibility of the education curriculum must be upheld with all appropriate means to develop appropriate policies and procedures.

In classic tests which they categorized into three different categories: exchange of knowledge among students, use forbidden objects, and circumvention of the evaluation mechanism, Keresztury and Cser[5] evaluated cheating methods. Nevertheless, there have been new types of cheating, such as utilizing storage records.

Cheating methods are increasingly evolved and difficult to spot. The typical cheating tactics Curran, Middleton and Doherty[6] illustrate such as: covering notes, pencil case, writing on weapons and leaving the rooms. But vast volumes of knowledge can be substituted by emerging technology, e.g. mobile phones, calculators, MP3 players, radio recipients and digital staff (PDAs). They also provide theoretically viable solutions that stop the fraud utilizing signal-jamming devices to detect active cell phones and interrupt contact between them.

Gao [7] has outlined the methods often used to prevent students taking e-cheating exams as follows: establishing a time limit; set up questionnaires and examinations that consist of randomly chosen questions from a huge pool of questions, such that . student has a different test/test; Biometrics usually involve keystroke, signature, speech, face, iris and fingerprint. It also revealed two items which are widely accessible and can be used for safe testing: Web assessor and Proctor U; which were also validated by several universities and can be used for e-testing processes.

Tampering with this is a constant problem in advanced education; for educationists, scholars and the general public, it is both significant. In a research conducted by Federal University of Nigeria, Williams, Abdullah and Owolabi[8] investigated gender differences, course of learning, academic success and trend-specific location. They also looked at the 76.5% of the pupils as cheating; fewer than 66% of the pupils were cheating; a greater percentage of males than females contributed to cheating and less people were cheating than high performers.

For online student tests, the chance of screen-capture and writing, searching and web browsing, HTML-Source Search, Sending Messagerie and screen-sharing is expanded to include material cutting, copying and pasting from/to the test setting. Frankl, Schartner and Zebedi [8] provided a Secure Exam Environment (SEE) to be kept in students' mobile PCs without local files and resources such as the internet, at the Alpen-Adria-Universität Klagenfurt (AAUK).

The Web and the "any time, wherever" are provided by PDAs and provide us almost infinite detail. Many students have found smart ways to use creativity to cheat during examinations. Kelley and Dooley [10] emphasize some of the more often used tactics for high tech cheating such as smartphones. Text messages from other beta users answer back and forth. Take a phone and submit the test pictures to the second group, either to copy or to assist the first pupil. Data can also safely be stored on graphic calculators and retrieved after examinations without the teacher cheating. Small microcameras and very small hearing aids allow a second individual to view the examination, look up at the answer in the guidebook, and then pass the response to the person taking the examination.

As of late, students cheat because of the spread of university cheating. This problem was further discussed by Simkin and mcleod [11]. You used the theory of reasoned action (TRA) hypothesis to expose deceitfulness and identify which reasons motivate students to deceive. Three motivational reasons: Internet access; ability to excel and penalties do not occur where a few trainers enforce offenses. Any diagrams were seen which are used in cheating processes. Text messages for testing responses, using PDAs to take photographs and e-mail testing content for other people. They found that cheating among undergraduates is much more regular than non-company undergraduates.

In the online learning world Rains, Ricci, Brown, Eggenberger, Hindle and Mara Schiff [12] focussed on the concept of cheating by students. Nevertheless, they gathered and studied

everyday terms that offer the concept of cheating a sense. First, 60% of students have identified trickery through breaking beliefs, dishonesty and not with their own brain. Breaking (expressed or implied) the concept of an examination, to receive answers by misleading your instructor to save answers in the memory of a computer and for example to apply answers which are not yourself. Secondly, 39 percent of students mentioned fraud with an emphasis on the concrete results of fraud, such that knowledge can be collected by means of non-ethical means to pass a test, and information or tools known to the cheater may be used to boost their ratings. Finally, 3% of students do not or would not identify fraud.

Cheating is simply false; it offers unfair advantages and hinders learning claims against it. Clearly, misguiding should not be a procedural problem but should be legal. Bouville [13] explored how to cope with deceit: cheaters are undeservedly big, and therefore have a disproportionate edge over other student. This may imply that the degree is unfailingly good, because if the degree is bad, it may be because the subject does not function enough. It's a positive thing.

Grades are also a reference for what students know and will do, and they are used as a proxy for what students can accomplish in the future.

2.2.1 Rates of Student Cheating

There are troubling patterns of cheating in academic institutions. There must be a caution when reading the recorded cheating rates. There are no descriptions of what is and isn't cheating as explained in chapter 1. Researchers thus use different meanings for various communities of various variables that produce a number of outcomes. Certain rates are listed below, but this is only a sample of how the incidence is, not a definite cheating figure. In one survey, teachers and students agree that fraud is a big issue in their own classroom, and 90 percent of students admit that fraud faces a mistake. (Evans & Craig, 1990). (Davis, Grover, Becker, & McGregor, 1992). Whitley's (1998) metadics examined 107 mostly college study trials between the 1970s and late 1990s and noticed an average of 70.4 percent of students who were accepted to university cheat, with such figures seeming to be on the increase (Jenson, Arnett, Feldman & Cauffman, 2002). Middle school numbers are also strong, though smaller than university. Anderman et al. (1998) estimated 39% fraud in middle schools.

The problem in high school is greater, as shocking as it may seem. Davis et al. (1992) and Cizek (1999) found that all high-school cheating rates were smaller than high-school ones. When questioned whether they were fraudulent at high school, 51 percent (woman at a tiny college of liberal art) and 83 percent (male at a major state university) suggested that Davis et al. were surveying 6000 undergraduate students. Davis et al. found an average of 76 percent of high-school students who were allowed to cheat. The Josephson Ethics Institute periodically carries out extensive nationwide polls, which question high school students regarding different ethical problems. In 2002, 74% of students who participated in this research admitted that at least once at high school they had taken tests; in 2004, 62% indicated that they had taken tests positively; and in 2006, 60% of surveyed students admitted cheating on an exam. In 2005, the Ethics Institute Josephson said that 62% of students reacted positively to the same issue. Maybe a quotation from Cizek (1999) will best sum up the extent of high school cheating: "A number of major trials have been carried out... nearly all of them are doing so. A high proportion of admitted fraud is a common result from high school fraud study." " (p. 16). These high levels of suspected cheating are the subject of several study studies and educators.

These experiments also helped to clarify the types of student features of cheating.

2.2.2 Student Characteristics Associated with Cheating

A large number of academic dishonesty study studies focused on student connection to deceitful actions and attitudes. The majority of features taken into account in these surveys can be split down into two broad categories: socioeconomic and scholarly.

2.2.3 Demographic Characteristics: Gender, Ethnicity, and Age

The following three demographics include: sex, ethnicity and age. The following One of the demographic factors most often observed is sex. In various college and high school tests, a gender gap was constant in that men reported to cheat more than women (Antion & Michael, 1983; Davis et al., 1992; Genereux & McLeod, 1995; Roig & De Tommaso, 1995). However, Whitley (1998) found out that gaps in self-reported survey research were consistently substantial (as opposed to classroom observations of cheating and cheating on laboratory tasks). Perhaps

men trick more and get captured fewer, or there are no differences in gender in trickery behaviour, but men are more prone to record certain incidents than women.

Another feature that researchers have been paying attention to is race. Sutton and Hubba (1995) noticed in their college degrees no distinction between African American (n=161) and Caucasian (n=161) self-reported deceitfulness. Latest findings at middle school level have been similar. Anderman et al. (1998) noticed little distinction between Caucasian (n=123), African American (n=116), and other ethnic groups (n=46) in self-reported cheating behaviors and attitudes.

Age is known to be the third and final demographic function. Just a few reports deal with high school theft, and far fewer with younger children. When fraud starts or the rates in primary schools are not evident, but Anderman et al. (1998), as discussed above, discovered that around 39% of middle school students they surveyed were allowed to betroth. These rates rise sharply to about 76% in high school years, or to about 70% in college (Davis et al., 1992, respectively) (Whitley, 1998) [36].

Analysis has shown that the markers of sex (Whitley, 1998) and race (Sutton & Hubba, 1995) are bad. However, it was discovered that secondary school children steal more than university students, who cheat more than secondary school students (Cizek, 1999). The following student attributes are academic features.

2.2.4 Academic Characteristics: Ability and Behavior

There can be two types of academic traits examined, academic capabilities and academic behaviour. Academic skill is also calculated by the average point of a student (GPA). A variety of experiments have attempted to detect the link between GPA and cheating. The GPA has a somewhat to mild inverse link between Diekhoff et al. (1996) and the Genereaux and McLeod (1995). The lower the GPA of the participant, the more probable the participant is to cheat. The better the participant. However, it cannot be said that high-level students are not cheating. The Who's Who Of the American High School Students (1999) study of the young people who had high-realization admits that 78% of students were admitted to different levels of fraud indicated a high admission rate based on their interviews with high-school advanced students.

A variety of studies have also examined the link between student conduct and cheating. The students who recorded cheating were found to be even more prone to delay their schoolwork, by Roig and De Tommaso (1995). The Evans and Craig survey (1990) have observed a correlation between student time management and student fraud in a favorable way. Finally, the self-ratified laziness of Evans and Craig and Schab (1991) was favorably associated with stealing.

The conduct of students outside the classroom was also given some focus in fraud analysis. Nowell and Laufer (1997) observed that complete or part-time students are more prone to lie than students without a job in their sample of high school graduates. The students who did the work were often more prone to lie than students who did not do the work, as Hains, Diekhoff, LaBeff and Clark, (1986) and Diekhoff, etc. (1966) observed. The studies Haines et al. and Diekhoff et al. both identified a connection between student and school sports. Both of the experiments also shown that both intramural and inter-collegial athletes are more susceptible to cheating than non-sporting students.

The above data show that cheating students are usually older (Cizek, 199), have a lower GPA (Diekhoff et al., 1996), seem to be lazy and self-disabled (Schab, 1991), employee (Nowell & Laufer, 1997) and play sports (Roig and De Tommaso, 1995). (Diekhoff et al., 1996). This knowledge does not therefore illuminate the motives for the behavior; the people who want to learn why students steal for that kind of information.

2.3 WHY DO STUDENTS CHEAT

Raisons for historically exploring students cheating using two common categories: expectations and factors of personality. Perceptions are the first group considered.

2.3.1 Perceptions: Self-Perceptions and Perceived Peer Norms

In two trials, low self-perception and cheating actions and attitudes were associated. A strong link between cheat and the poor academic self-concept of students was noticed by Evans and Craig (1990). These results were verified by a more modern Finn and Frone analysis (2004). Finn and Frone find that students who mentioned misleading, rather than students who didn't, had low levels of self-efficacy.

Students have often been positive towards stealing in the expectations of peer standards. Students who think that fraud is common and believe that their peers are not guilty of conduct have a greater risk of cheating themselves (Eisenberg, 2004; Jordan, 2001; Whitley, 1998). Additional solutions are likely to the issue of 'why are they cheating?'.

2.3.2 Personality Variables: Morality, Deviance, and Anxiety

Three factors common to scholarly dishonesty and fraud are morals, deviance and fear. Cheating is clearly an ethical problem, and scholars have focused on examining it in this way. Studies also noticed no connection only between Kohlberg's spiritual thinking (1983) and self-reported cheating rates (Lanza-Kaduce & Klug, 1986; Leming 1978). Cheaters excuse their cheating actions better than non-cheaters (Jordan, 2001) and have more external rationale for cheating (McCabe, 1999). (Taylor et al., 2002). Jenson et al. (2002) observed, when assessing the admissibility of academically unethical conduct, that secondary and college students took the reason into account. Students saw academically unfair practices as justified when they were inspired by prosocial motives (e.g., to support their relatives) and when the reason was to see if they were willing to do so.

Diversity and paranoia are also associated with fraud. Blankenship, Muncie and Whitley (2000) observed that students who were cheating were often more prone to partake in different behaviour, such as reckless driving. Whitley (1998) has indicated that cheating is positive for behaviours, such as petty crime, friendship deception and substance addiction.

Their paranoia was all shown to be associated with deception. Anderman et al. (1998), Evans and Craig (90) and Schab (1991). Anderman et al. observed that cheating students became more concerned too. Evans and Craig and Schab all indicated that they were afraid that the students might not be among the main causes for cheating. Because anxiety is linked to trickery, considering certain possible triggers of anxiety would be beneficial. Research indicates that students are under tremendous strain to meet their parents, their teachers and their potential ambitions from at least 3 places. Parental stresses were all shown to be one of the most important causes for deception by students: Evans and Craig (1990), Schab (1991) and Taylor et al. (2002). Teacher and college pressure were also found positively linked with theft, Taylor et al.

Possible replies: 'Why are the students cheating? "Perceptions and attitude variables are used in the literature. It could be that students cheat on their low academic concepts because of their behaviors and feel little culpable afterwards (Jenson et al, 2002; McCabe, 1999; Taylor et al., 2002) because students are divergent in other fields in their lives (Blankenship et al., 2000; Whitley, 1998) because of their lack of knowledge about themselves (Evans & Craig, 1990; Finn & Frone, 2004), because students are divisive in their life (Evans & Craig, 1990; Schab, 1991; Taylor et al., 2002). Although teachers may have a profound effect on instructional characteristics such as a low self-concept and low self-efficiency ratings, educating people find it impossible to change other characteristics such as demographic and personality variables. While fascinating the association between these demographic and academic factors and student misconduct, offers the instructor no support in trying to curb academic dishonesty (Whitley, 1999). The next segment reflects on the avoidance of fraud in the literature.

2.4 ENVIRONMENTAL FACTORS

For certain cases, academic discretion focuses on the demographic and behavioral traits of individual students. It is assumed that students are mostly responsible for cheating. Factors including paranoia (Anderman et al., 1998), cognitive capabilities (Diekhoff et al., 1996) and moral character (Eisenberg, 2004) are linked to student cheating in this study. Factories including interpret societal standards (Jordan 2001) and social pressures may be explained from other studies (Taylor et al., 2002). While it is necessary to consider and to research the effect of these personal and social influences on fraud, an education provider is highly restricted in controlling or modifying those factors.

Study on fraud has recently indicated that considerations such as the conduct of teachers and the history of schools and schools may also be used to justify fraud. These environmental ideas will easily address educators. Educators will both actively impact and change factors including climate, organization, leadership and the atmosphere of the school and the classroom. This study re-focused emphasis on educators and suggested that educators build school and classroom environments that promote and not prevent dishonesties (unknowing and unintentional).

2.4.1 Classroom Environment

Study on the classroom is a different kind of literature than fraud. The dissertation of Herbert Walberg (Walberg & Anderson, 1968) and Rudolf Moos (Moos, 1979) has been the analysis of the classroom environments and has been a significant subject for the past 35 years. The world of the classroom includes several aspects such as class culture, environment, sound or temperature (Dorman, 2002). Also known as community, atmosphere or climate, evidence shows the important, positive impact the classroom environment has on student education (Fraser 1994, 1998). When students are optimistic about the learning setting, they perform more. The value of the classroom setting is largely attributed to Rudolf Moos' early theory. The human world, according to Moos, has three aspects, including partnership, the creation of individuals and the preservation and modification of the systems. The connection component relating to educational environments comprises topics like student attention, interest and engagement, student concern and friendship, and the amount of confidence that teachers display towards their students and support them (Moos, 1979). The component of personal growth involves scheduled events, topics, competitiveness and difficulties (Moos, 1979).

Maintenance and improvement require the organization and order of the classroom, consistency of rules, supervision of teachers, opportunity to relate to program work and jobs for students and creativity for teachers (Moos, 1979).

Research has demonstrated consistently that in supportive school settings students perform well (Dorman, 2002). Positive and healthy school environments characterize supportive relations with and between students and teachers; those in which students are able to make choices and to co-create standards and goals; those that are well-ordained and well organized; those with clear assignment expectations and rules, with sufficient time available for students to complete work; and those where assignment expectations and standards are clear (Dorman, Fraser, & McRobbie, 1997; Fraser, 1989; Huffman, Lawrenz, & Minger, 1997; Wang, Haertel, & Walberg, 1993; Waxman & Huang, 1997). A supportive atmosphere in schools is related to low levels of distress in students (Taylor and Fraser, 2003), elevated levels of self-conception in students (Byer, 1999), better cognitive and affective effects for students (Goh & Fraser, 1998) and lower levels of student self-disability (Dorman, McRobbie, & Foster, 2002). The study often

connected the classroom with intellectual dishonesty (Anderman et al., 1998; Pulvers & Deikhoff, 1999).

2.4.2 Classroom Environment and Cheating

Anderman et al. (1998) is interested in the impact of fraud in the classroom and pointed out that students stressing extrinsic targets in a classroom (i.e. that students would get out of other academic duties and be praised for academic performance) had higher rates of fraud and conviction that cheating was permissible. The findings also found that high grades report higher levels of cheating activity among students who experience school achievement. Jordan (2001) observed that students who are inspired to learn or to study are less prone to steal than university students. The low level of teaching is linked favorably to student cheating. Blackburn and Miller (1996), Steininger (1968) and Steininger, Johnson and Kirts (1964). Students have often shown that when they feel that course material is irrelevant and uninteresting, they are also more inclined to deceive [27].

Any of the findings from the Evans and Craig students (1990) concern the school [28]. Their research suggests that students conclude that instructor features (e.g. appearance and behaviour) are more likely than teaching staff to encourage students to cheat. Students often found that the features of the school, such as the volume and complexity of the materials studied, whether a course was compulsory or not and that the usage of the grade curve influenced fraudulent behaviour. Finn and Frone (2004) noticed that low student performers are more likely to cheat when they have bad school identity (as compared to strong) – such as a sense of school membership, and value school and school outcomes. In addition to discovering an association between auto efficacy and cheating behaviour.

A self-report cheating study and a college and university-level climate scale analyzed the association between academic dishonesty and the college-level environment (Fraser & Treagust, 1986). Pulvers and Diekhoff (1999) findings show that students cheat lessons are less rewarding, customized and goal driven than non-cheaters. They are less satisfying. In Pulvers and Diekhoff's student study Pulvers and Diekhoff argue that the school atmosphere is a significant predictor.

2.5 LIMITATIONS

The aforementioned analysis of applicable scholarly dishonesty literature has to be taken into account with the following restrictions. While betrothal is a focused field of academic research for decades, the literature as it stands today is still limited by at least three. The first drawback is that most scholarly dishonesty experiments are quantitative in nature.

Academic dishonesty is studied, demonstrated and avoided by theoretical consequences. The above was mostly researched through positive epistemology through university dishonesty. Academic dishonesty methods aim to generalize results in all pupils, instructors and classrooms, making students more responsible for deceiving and not investigating and changing failings in the educational processes that cause or contribute to the issue. The dynamics around cheating students are very likely to differ significantly from one classroom to another, one academic level to another, one school to the next, and one district to the next. It is also possible that educators bear the duty to trick students by building environments that promote and facilitate intellectual dishonesty and cultures that do not emphasize mastery and learning [31].

Usually in cheating studies the second restriction of the literature concerns the community. This thesis looks at secondary fraud, although much of the commonly available analysis has been conducted on university students. There is a need for further studies on high schools and also on young people; very little knowledge exists as to where, when or how these unethical attitudes and habits are developed in pupils. In addition, all of these experiments are suspect of their reliability. Most frequently, only a few reports have included variables mentioned above (sometimes only one). While these could be significant results, it also needs to be seen if the results can repeat. This presents an up-to-date challenge, since some of these experiments were performed in the early 1990s (some were earlier), with possibly interesting yet nonreplicated results, and it is uncertain if the findings will reproduce today.

In studies of intellectual dishonesty, the third and final constraint is relevant to the essence of the issues. The lack of speech is a frequent challenge with the traditional problems of intellectual dishonesty. The demographics and behaviour, however, are scarcely sought by the students. There is a great deal of attention paid to finding students who lie and investigate habits and personalities, but broader structural issues are sometimes overlooked. While relationships are fascinating and useful between demographics, perceptions and behaviours, they are not

particularly beneficial for educators and school children. Characteristics and behaviors are not quick to change or change (Whitley, 1999). The most helpful (once again, few) research are focused around what kinds of environmental and systemic improvements educators and schools need to make such that classrooms are not just less mocking, but also that honest attitudes can be developed.

2.6 AUTHENTICATION

Authentication is one of the ways in which personal identification is protected;[18] it also aims to check if users are the ones whom they appear to be. D-exam does not include protors or watchdogs as opposed to face-to-face exams. They are kept in a separate remote area that is unregulated. The authentication objectives in the D-exam therefore are essential for the identification of online students since they play a major role in the safety process[16, 17].

There are two types of authentication [18]: static and ongoing authentication. Static authentication applies to authentication which is made at the beginning of the exam access and is then valid during the test before the student logs out. The continuous authentication applies to an authentication, which is continued after the test is started and checks if the actual user is the same as the user carrying out the original examination.

The modern system of e-examining authentication is presented by Sabbah, Saroit and Kotb [14]. This approach enables schools to conduct scam-free e-examinations, a key concern for e-learning in the past decade. They provide e-examination sessions that are virtual, interactive and stable. The framework needs user authentication to verify the identities of the user when attempting to enter system services and to track the examiners interactively and remotely utilizing a camera and video call during their test.

On the basis of community cryptography with an e-monitoring program, Jung and Yeom [15] proposed a security control mechanism during the online examination (SECONE). The encryption supports improved safety control, verification and honesty for the online examination method. However, two groups in the online examination framework supported safe contact among dispersed organizations. Communication between intergroups is secured by public key infrastructure (PKI) while communication intragroups requires multiple Diffie-Hellman keys.

Just the first login session authenticates a person for most current computing and network networks. The safety deficiency may be crucial. A modern users authentication system, which is mostly based on soft biometrial traits (e.g. apparel colors and facial skin), has been proposed by Niinuma, Park and Jain [19]. Soft biometric characteristics are described as "characteristics which provide some data on the entity, but lack the distinctness and permanence to distinguish between two persons sufficiently." The following benefits can be derived from the usage of soft biometrics in a continued authentication scheme. 1) the user can be authenticated continuously even though no hard biometric details or insufficient hard biometric data are present, and 2) no prelude of biometric soft features are necessary; soft biometric features are immediately registered each time the user logs in. They also shown that the machine will consistently authenticate the user with a strong tolerance of the device [46].

Right now, e-learning facilities are facing two main identity management challenges. There is no customary static clarification at the login period whether a simple hidden key plan or a sound watchword would be taken into consideration. An understudy will without a doubt convey the hidden word to a specialist and enable the master, who is a real risk to the respectability of degree programs provided by e-learning foundations, to undergo an online exam for his sake. To avoid continuous authentication by e-cheating students are using. Continuous verification is a guard that keeps an eye on who uses a device, uses facial and biometrical identification features.

The authentication of an unauthorized person could prevent it from slipping into the computer system and using it until the approved user has been authenticated first. The modern e-learning models for identifying, authenticating, and monitoring students were presented by Bhandwalkar and Hanwate[20]. In terms of consumer posture in front of the workstation, the device is stable. Soft biometrics for continuous verification provides a high level of flexibility and contributes to greater protection with the use of both hard and soft biometrics such as facial recognition. In addition, no additional soft biometric hardware is needed.

Fingerprint and eye monitor are mainstream authentication strategies.

2.6.1 Fingerprint

In online exams, continuous authentication is the main thing as the user is verified during the whole session on an on-line basis. Sudarvizhi and Sumathi[21] have attempted to conduct a systematic research study of biometric continuous authentication systems. The strengths and disadvantages of each biometric rely on the application. Sclera and Fingerprint were the main features for their many biometric characteristics for continuous device authentication.

Online reviews are known as e-views. A remote consumer takes them over the Internet. Most applications have, though, used username/password approach for user recognition. Instead of standard approaches Wei, Cong and Zhiwei [22] suggested a fingerprint-based identification technique. On the examination server cooperating with an online examination scheme for authentication a fingerprint identification / classification program and load balancing facility was introduced. Code incorporation or SDC invoking approaches should be used for the interfaces between the examining device and the identity verification program to adapt various sensors. The verification of the identification functions quite well in internet/intranet schemes.

Biometric technology involves the diagnosis and authentication by observing the features of the human body. It was commonly used for different purposes in various aspects of life, especially the topic of staff attendance in the context of this research. The Oloyede, Adedoyin and Adewole [23] studied the same biometric identifier used to improve standard workers attendance systems utilizing a telecommunication business in the south-west area of Nigeria. They show that fingerprint is the right biometric method to address the lingering staffing challenge in the proposed organisation in the long term.

Authentication of fingerprints is one of the most accurate and used techniques. Designed and implemented an Embedded Fingerprint authentication device, Shinde and Bendre[24] operate in two phases: minute extraction and meticulously matched. They also clarified the co-design of hardware-software that covers the matching of two fingerprint-sets and recommends that automatic fingerprint authentication system reconfigurable architectures be used. They also introduced an A Spartan-6 fingerprint algorithm (FPGA). The experimental findings show that the device complies with the Automatic Fingerprint Authentication System's high-speed hardware co-design reaction time.

Verification of fingerprint is an effective biometric authentication technique. In order to authenticate an individual's identity, Jain, Lin Hong, Pankanti and Bolle [25] have introduced the automated identification authentication method prototype. They improved the thorough extraction algorithm, which can locate correspondences between input minutiae and the stored prototype without using a thorough check and can adapt for non-linear deformations and inaccurate transformations between the input and the template. The experimental findings indicate that the device on these databases will achieve decent performance; it also takes around 1.4 seconds on average for a full Sun ULTRA 1 authentication process.

2.6.2 Eye Tracker

Eye Monitoring is an assistant to the interaction between human and computer (HCI). Applications of eye movements on real-time interfaces can be divided into two classifications: (1) eye movement as simple control device (i.e., a non-touchable mouse pointer for people with disabilities and (2) eye movement analysis to achieve the user's intention and, for example, interactive graphical displays and interface usab, to facilitate the interaction environment. Using authentication with eye tracking technologies provides the compromise between the simplicity of usage and reliability of an authentication device a hopeful and practicable alternative. The Eye Movement Authentication Technique (EMBA) has decomposed Zhang, Zheru and Dagan[26], into three fundamental aspects: (1) the input mode of the eye, (2) a system for contact with eye movement and (3) the identification of moving pattern in the eye. They have been researching the EMBA method. A considerable number of reports are experiments only without a substantial machine error review and rigorous usability testing.

Eye Monitoring is an assistant to the interaction between human and computer (HCI). Applications of eye movements on real-time interfaces can be divided into two classifications: (1) eye movement as simple control device (i.e., a non-touchable mouse pointer for people with disabilities and (2) eye movement analysis to achieve the user's intention and, for example, interactive graphical displays and interface usab, to facilitate the interaction environment. Using authentication with eye tracking technologies provides the compromise between the simplicity of usage and reliability of an authentication device a hopeful and practicable alternative. The Eye Movement Authentication Technique (EMBA) has decomposed Zhang, Zheru and

Dagan[26], into three fundamental aspects: (1) the input mode of the eye, (2) a system for contact with eye movement and (3) the identification of moving pattern in the eye. They have been researching the EMBA method. A considerable number of reports are experiments only without a substantial machine error review and rigorous usability testing.

Eye monitoring in relation to usability testing is now a well-known technique. Users watch the pupils of the person and their location on a computer with the aid of an eye tracker and thus have accurate details on user experience elements regarding their visual focus. It can be seen as a valuable source of user knowledge. The eye monitoring investigations conducted by Manhartsberger and Zellhofer[29] are a valued tool to enhance the results of quality testing. Often, in the user interface sense, eye tracking information is essential for interpretation.

However, certain eye monitoring devices include the consumer or have cameras or other equipment installed on the operator's head. These limitations render the devices unacceptable in immersive software for extended usage. In order to enhance visual contact, Meyer, Böhme, Martinetz, & Barth[30] use eye trackers to direct the gaze. The eye-tracking devices using a remote eye-tracking device with a single-camera achieve precision between 0.5 and 1.0 grades. There are no precise measurements on the whole method, however, experiments on simulated data reveal that the algorithm for the gaze calculation will reach a certain degree or better.

Eye tracking systems have various possible uses, such as emotion management systems for studying, fatigue monitoring systems for drivers and others. The eye monitoring device is used by Su, Wang and Chen to install the 'eye mouse' to enable people with serious disabilities computer access. The eye mouse allows individuals with serious disabilities to control machines by using their eye motions. Only one web and a personal computer are required. This is cheap. They created a five-phase algorithm to assess the directions of eye motions and then control the machine by using direction knowledge. Experiments showed that the machine can be used by people with serious disabilities.

2.7 PROCTORS

E-learning, with many vendors that employ networks to use materials and train students, is a widely recognized type of learning. While much has been done to create and install Virtual Learning Environments, the associated issue of electronic surveillance is less focused. The

method to e-invigilation remotely dependent evaluations using straightforward Biometrics has been proposed by Clarke, Dowland and Furnell [32]. In this way, physical surveillance devices, assigned classes or evaluation centers are avoided and both the assessor and applicant are free to use, thus ensuring a certain degree of protection from the formal evaluation process.

In advanced education, online education is already a big strength. There are double-digit growth in both the amount of online students and the number of courses available. Without a guarantee of fairness from the course applicants, the faculty was hesitant to follow online classes. In reaction to this issue, the identity of the learners online and the possibilities for academic discretion are being verified by new technology. The Secure Remote E-proctoring Software was developed by Cluskey, Ehlen and Raiborn [40]. The camera needed this device to capture the test by 360°. The framework may be an advantage for organisations who aim to extend or upgrade their online courses.

2.7.1 Proctor U

ProctorU is a part of the online cottage industry of suppliers that have recently expanded as universities and colleges focus on non-traditional students, who have to graduate without leaving their homes[33]. ProctorU is a procurement service that enables students to take tests on their webcam. Using ProctorU is mainly because it allows students to undergo supervision exams without having to move to various test centers [34]. The student is associated with real individuals who guide the process. You see the evaluation screen in real time to see what the pupil does on site and on display [35].

2.7.2 Tegrity

Tegrity's remote protection feature ensures the completeness of examinations taken off campus. Tegrity records the pupil's video of the test and its screen activity, while students can take their exam at home [36]. During the exam the student cannot pause the recording, and after completing it the instructors can immediately upload the recording. [37].

2.7.3 B Virtual

B Virtual collaborates on the development, live, online examination of customary resources with higher education institutions [37]. B Virtual encourages students to take tests in a living, safe and secure world from the safety of their homes. In addition, B Virtual will collect all examination data including visual, audio and keystroke data for student monitoring [38].

2.7.4 Proctor Cam

Proctor Cam is a protocol solution for testing professionals and managers. Study participants plan their test with a proctor from the internet. Proctor Cam tracks research users worldwide with the use of tracking tools for laptop, audio and webcam [39].

2.7.5 Kryterion

A proctor that supervises the administration of a test and the student using a webcam and a microphone is needed for the Kryterion on-line proctoring scheme. Online certification allows research participants to prepare and take an online examination every day and everywhere, while our accredited providers maintain compliance with the training requirements. The protocol electronically checks the session for suspicious conduct or infringements of norms [41].

2.7.6 Proctor Cam Remote Proctor Now

Remote Proctor Now (Rpnow) is an online safe test distribution and identity verifying self-service model. Using a normal machine webcam with an internet link, it allows students to take a test online easily and affordably by capturing all the sounds and images, a 360-grade vision of the exam area. RPNOW is flexible for students who have the right to take examinations at times and dates that are suitable for them; [42].

2.7.7 Proctor Free

Proctor Free is an integrated, protocol approach that does not need human inclusion. Proctor Free authenticates the pupil with face recognition and keeps the identification check during the examination with the webcam. In order for students to have a freedom to navigate those web

sites or software, a safe browser may also be completely adapted to the requirements of this specific test. During the examination Proctor Free often monitors a number of usually fraudulent activities, habits and trends. In order to conveniently sort and display results the administrator can log in the dashboard of Proctor Free. It further emphasizes the specific time and the second time that cheating activities happened and enables the manager to decide whether or not the student was cheating [43].

2.7.8 Proctor Exam

Proctor Exam provides a Safe Online Exam web-based website. Identify the test driver behind the robot and build an extremely safe test area for high-level testing. The student shares the display with Proctor to guarantee that the programs and websites are only used whitelist. The machine uses a web camera with a complete 360-degree view of the examination environment. The proctor monitors and records the student's abnormal behaviour and may inform the institution promptly about any behaviour which falls below the proper criterion of testing. [44].

2.8 SUMMARY

Despite the above-mentioned restrictions, research seems to overwhelmingly suggest that student fraud at all academic levels is very high and high in secondary school students who typically cheat have bad academic conduct and students who cheat on their own behaviors, justify their behaviour, feel no guilt, fear failure and feel good at school. Prevention techniques such as honorary codes have been limited at kindergarten, but are not tested in high school.

Despite the above-mentioned restrictions, research seems to overwhelmingly suggest that student fraud at all academic levels is very high and high in secondary school students who typically cheat have bad academic conduct and students who cheat on their own behaviours, justify their behaviour, feel no guilt, fear failure and feel good at school. Prevention techniques such as honorary codes have been limited at kindergarten, but are not tested in high school.

3. METHODOLOGY

3.1 INTRODUCTION

Online exam Application for the identification of the face to detect deception by fake name or party attendance and even for the eye monitoring of anyone who looks at the far right or at the left not to read something on their screen.

Steps to solve the dilemma

3.1.1 For Face Recognition

We take a snapshot of the student and link him to our database so that we can identify him.

We took the student and encoded it in the live video.

His coding is compared to the remaining codes to see whether the match exists.

For consistency savvy, just 60 frames (~1 sec) are used for face recognition and encodes.

3.1.2 For Group Attendance

We recognize the number of faces in live feed

We screen a detected fraudulent picture if more than one exists.

The facial identification and encoding only operates in 30 frames (~500m) for output purposes.

3.1.3 For Eye Tracking (Not Very High Accuracy, because we are Using a Standard Laptop Camera)

We first recognize the eyes with a dlib model detector of 68 faces.

Use a trackbar to show the pupil's eye is the only white aspect of the picture.

Use dilatation, degradation and median blur to increase and clarify the contour.

The middle of the blob form of the eyes is detected using blob region measurement

We verify if the center is similar to the left or right frontiers of the 68-face points.

If it is near, the student cheats when he looks off the computer.

We also used python with open CV and dlib modules.

3.1.4 For Why We Choose Those Libraries

Open CV is fast, well recorded and has an enormous community dlib has pre-trained, quick and extremely precise models (our face recognition accuracy is 98 percent) Facial recognition is based on dlib and uses the same types, albeit with simpler functions and less code values.

3.2 EXAM

Exams are used most often to evaluate understanding in students. They often avoid material being made available to students during the course. Students choose to use one method or another to process knowledge to understand.
Examinations may also be graded in three types: standard, online and e-examinations.

3.2.1 Traditional Exam

Traditional examinations are known as a collection of class questionnaires. They are developed per student on static queries. Both students must begin and complete the exam simultaneously.

3.2.2 Online Exam

Internet-based examinations are also known as e-examinations. It is generated on the basis of random questions per student with some deadlines for completion. Students can also take a workshop for the examination.

3.2.3 Distance Exam

Distance examinations (D-examinations) are a way to ask students who are not present in a school, for example. They are generated on a random basis with specific time limits per student to be addressed. D-exams often allow students to conduct the examination in any place.

3.3 CHEATING

Cheating is the act of misconception, disappointment, swindle, quackery or imposition sometimes used to produce an unfair benefit at the cost of others. Cheating means the laws are violated. During tests, a general area for cheating must be included.

Cheating on examinations at both classes was a common practice in the country. In the last decade, several reports have been done on student misconduct and on how the University should try to tackle this issue [6]. In the U.S. 80 per cent of high school pupils have found cheating, 95 per cent of high school pupils admitted cheating, 51 per cent said cheating is wrong, 85 per cent said cheating is essential to get on, 75 per cent said cheating. It has been revealed that 80 per cent said cheating is not wrong.

The main factors for cheating are: expectation from parents to be good, fear of failure, uncertain educational goals, a desire for higher education, no penalty if detected, little chances of being caught, little time to learn and quick access to online knowledge.

Fighting cheaters is better once you grasp the technique. There have been reports on the tactics of cheaters and can be categorized in three levels: typical fraud, class online fraud and distance fraud.

3.3.1 Traditional Cheating

Many students choose to use conventional cheating tactics, since each student may deceive through one or another. This allows for two types: cheating individually and cheating in squad. Individual cheating applies to when a student cheats on his/her body parts or on a little notice and hides them in his/her clothing. group cheating refers to the situation where students exchange details with other students using hand signals, particularly fingers, to interact with others.

3.3.2 Online Cheating

Internet cheating is traditional cheating that occurs online. You should steal on the internet with your student. However, two forms of deception and electronic fraud may be classified. Personal cheating relates to whether students want to cheat on their own using a clock, iPod or cell phone, for example, to write tiny notes and put them in their dresses. Electronic cheating is about submitting a query to an expert via email or chatter while students exchange knowledge with others via the internet.

The various forms of fraud in conventional and online tests are described in Table 1. It also offers several proposed solutions for preventing and detecting cheating; proof is an individual who supervises or supervises tests.

Table 3.1: offers several proposed solutions for preventing and detecting cheating. **(**Table Continued)

	Type	**Traditional Cheating**		**Online Cheating**	
		Prevention	**Detection**	**Prevention**	**Detection**
1	Look at the paper/response sheet or job of another pupil. This is intended to be co-ordinated by the student's collusion	Leave the students empty space or make separate examination samples.	Seek assistance from physical suppliers		
2	Communicate using the sign language or with a code that may communicate replies such as pencil click, foot tap and headshape.	Create several test samples	Request assistance from physical suppliers		
3	Pencil for simple to wipe later: particularly when written in pencil.	Before the test is started, check all offices	Request assistance from physical suppliers		
4	Usage of cheat sheets: pre-written cheat sheets in tiny fonts, garments or wrist watches		Request assistance from physical suppliers		Request assistance from physical suppliers
5	Using scams on the floor: pre-written scams contained in books or folders beneath the desk	Ensure that books or notes are saved not beneath the desk, in the bag	Request assistance from physical suppliers	Ensure that books or notes are saved not beneath the desk, in the bag	Request assistance from physical suppliers

6	the faculty gives pupils a chance to go to the restroom to check notes in the garbage can.		Do not allow tests to go to the toilet Or pauses		Do not allow tests to go to the toilet Or pauses
7	To send question number or right answer through mobile phones, use numeric devices SMS messages	Do not allow mobile phones or use Microsoft Dongles to identify Bluetooth-based devices at "on"	Request assistance from physical suppliers	Do not allow mobile phones or use Microsoft Dongles to identify Bluetooth-based devices at "on"	Request assistance from physical suppliers
8	Copy exam questions and e-mail or talk them to someone			Software which cannot execute an application Examiner	Request assistance from physical suppliers
9	Use any kind of text-based memory calculator to capture all equations, notes, theorems, evidence, etc.	Use primitive computers	Request assistance from physical suppliers	Use primitive computers	Request assistance from physical suppliers
10	Hearing the iPod with recording capacity; earphone cables may be hidden beneath long hair	Don't let tests utilize iPod's	Request assistance from physical suppliers	Don't let tests utilize iPod's	Request assistance from physical suppliers

3.3.3 Distance Cheating

E-examination is an effective way to do an exam. Students may study at any convenient location. In addition, actual travel is not necessary. However, during tests the issue of cheating arises since physical proctors do not monitor and monitor the test. This is known as cheating distance. Distance fraud encompasses all preceding types of fraud.

Furthermore, there are additional sorts of fraud, including:

a. Taking another student's examination.
b. Use programs to tackle examination problems.
c. Copy the examination question and submit it back to an expert.
d. For example, by utilizing an e-book you download materials from the Internet.
e. Check the Internet for answers.
f. Use mobile phones and the internet to look for a reply.
g. To capture the test photos with a mobile phone camera.
h. Use discussion forums on the Internet to find an examination answer.

3.4 CONTINUOUS AUTHENTICATION

3.4.1 Fingerprint

Authentication by fingerprint is an automated way of checking the match between two human fingerprints. Because of its distinctive and consistent usage across time, fingerprint identification is one of the most famous and published biometrics. No fingerprints are identical for two persons. Even the same twins have distinct fingerprints, with the same DNA. This feature enables fingerprints, including background checks, to be utilized in any manner..[٤٥]

Fingerprint has several benefits:

a. Unique - the fingerprints are unique, differing between one finger and the fingerprints of each finger of our 10 fingers. Even the same twins have different fingerprints.
b. Practicability – Users must not remember more numerous, lengthy and difficult passwords, often changing or carrying several keys.
c. Non-repudiation - Ensures that the user has access to a system and that he or she is present at this moment.
d. Non-transferable - Unlike passwords, pins and smart cards, it is not shared, lost, stolen, duplicated, disseminated or forgotten.
e. Proven – Long history of effective identification – the USA and other nations have considerable fingerprint acknowledgement experience in the real world. For many more than a century fingerprint has been employed in forensics and a wide range of scientific research and real-world data demonstrate the distinction of fingerprints and their durability.

3.5 METHODOLOGY

The architecture of the project is simple we only have a single table database that holds the images encode and person name. We didn't use any dataset since we have a pretrained model The dlib face recognition model that we used has 98% accuracy.

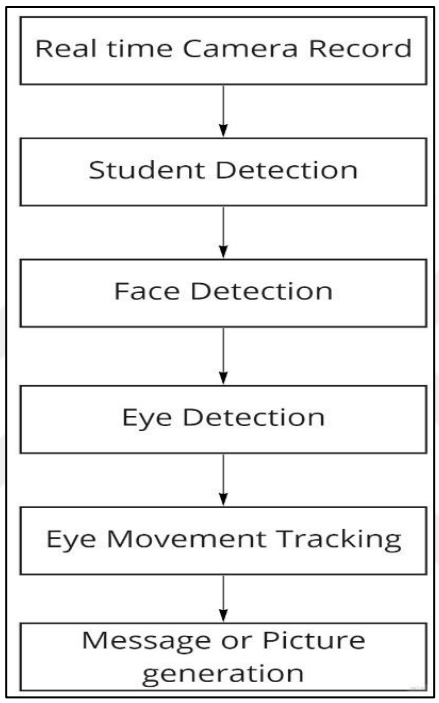

Figure 3.1: System Architecture

Input video acquisition is the first phase of the proposed method. The modes for input video gathering vary for various scenarios. The method used recordings taken during the semester test in the test hall of master's degree students. In the pre-processing phase right before processing, the collected footage was processed for improvement reasons**.**

4. SIMULATIONS RESULTS

4.1 STEPS TO RUN THE SOFTWARE

- ✓ We first need to install python, c++ compiler, cmake c++ tools
- ✓ Python Libs: opencv-python, cmake, dlib, face-recognition (the order is important), and pymysql for the database.
- ✓ You need to open your mysql server, change the database configs in DB.py and then run that file.
- ✓ If you want to add a person to the database, run NewPerson.py.
- ✓ For simplicity if you don't want to use the database, if you want you can just run the code but you have to put your student image in a direct.: Resources/Students images (or change that path in main_face_recognition.py load image's function), and also in the Video Cap.init change the lines as described in the comment.
- ✓ To run the face recognition run main.py, for eye tracking run eyeTracking.py.

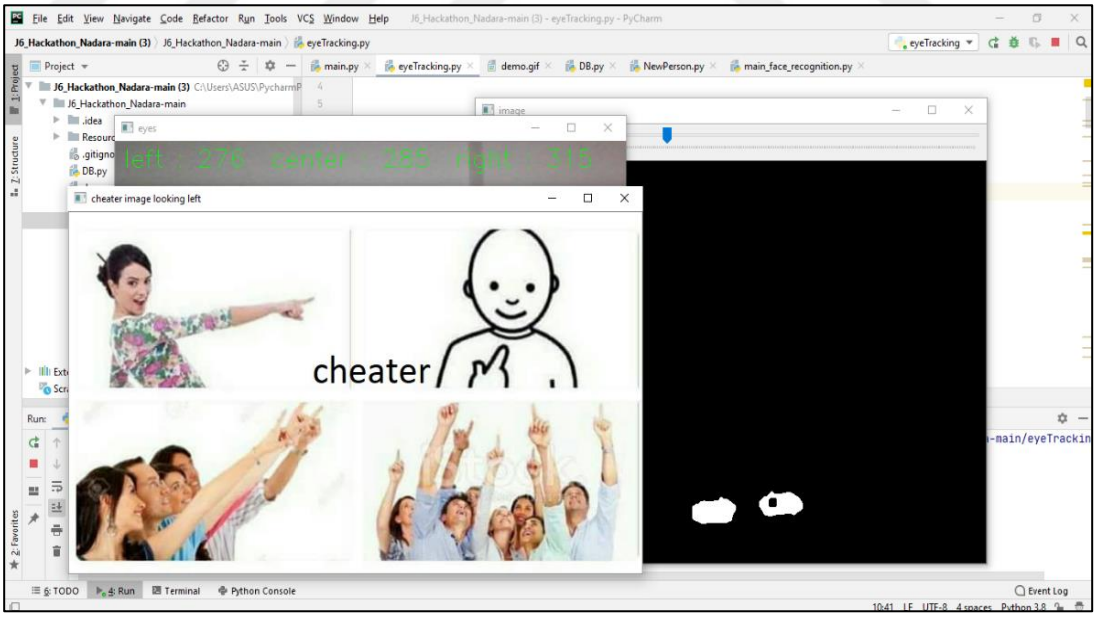

Figure 4.1: Screen shot of Python Result of Cheat Detection System**.**

4.2 RESULT

Video input from several sources was utilized. The camera may be utilized at various angles. Only the vides and pictures acquired from the front perspective are handled by the proposed method. The front view of the camera allowed to easily recognize people. The detection of human face and eyes could also be made from the side, but movement of the pupils and eyes cannot be studied and no conclusion could be given either on cheating or calm conditions As Fig. 4.2.

Figure 4.2: Input Video Frame.

Fig. 4.2 illustrates one of the students who was examined at the end of the MS semester. Only one pupil is shown in Fig. 4.2. The proposed algorithm for the treatment of video and pictures was developed and tested.

For human face detection, the frames of the input video have been analyzed. For the detection of the human face, several algorithms were created. Viola Jones face detection method[17] is employed in the suggested technique. The cause was that, with low resolutions and the use of affordable cameras, it delivered remarkably great results. Fig. 4.3 demonstrates the effective detection results.

Figure 4.3: Human Successful Detection

If the human face was not identified and the following picture was analyzed. The next phase, followed by the suggested technique, was eye detection after human face detection. Viola Jones [17] has been extended for the detection of the eye. Figure 4.4 displays the results of eye detection that marks the face with the red box of the eyes.

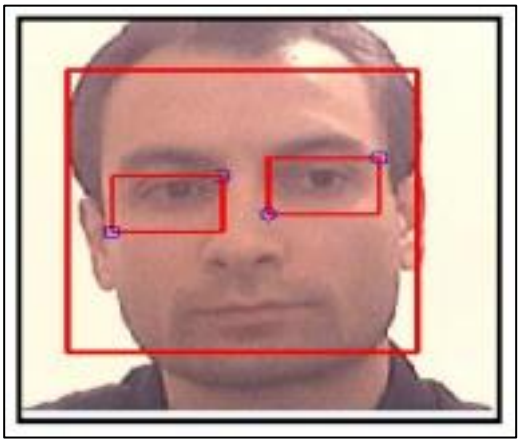

Figure 4.4: Eye's Detection

The frame would be removed if the outcome of the input processing frame did not lead to any eye detection. For monitoring and analysis of the movement of the eyes the results of effective eye detection have been processed. For mobility of the eye, first and foremost the segmentation of the eye by image [18]. Figure 4.5 shows the segmented region of the eye for subsequent treatment.

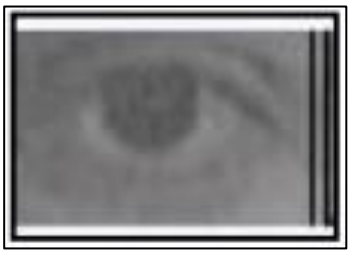

Figure 4.5: Eye Segmentation.

Separated eye part and tagged for further processing for the left and right eye. Segmentation was conducted to fulfill the goals of the suggested method and work on just the ocular component.

The pupil may be recognized using white part and black component distinction of the gray levels following eye segmentation. A template matching and pupil axis detection were obtained for pupil. The technique was done to the left and right eyes. Eyes were detected in Fig. 4.6 with little red boxes and pupils indicated by blue-colored margins.

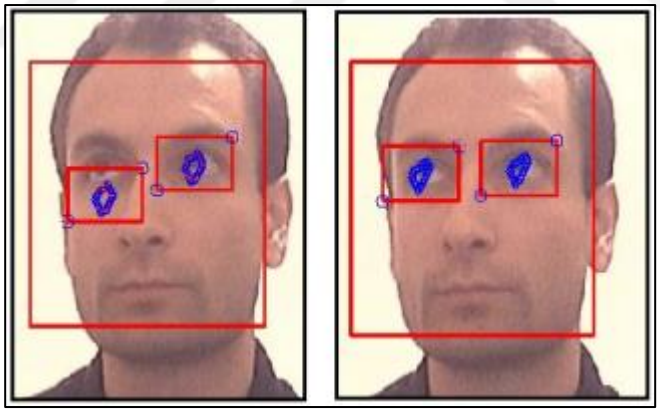

Figure 4.6: Pupil Detection.

Analysis was carried out of each frame processed and comparison of the preceding frame was carried out. In case of fraud involving students, the comparative analysis states the movement of the student's eye.

A noteworthy discrepancy between the prior and present axis values that meets the threshold value results in a statement of fraud and produced an alert. Figure 4.7 displays the view of both the left and the right side when the eye is shifted.

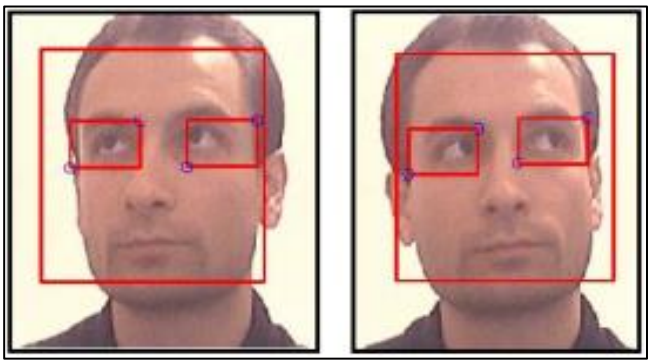

Figure 4.7: People view on both left side as well as on right side.

Table 4.1 illustrates the contrast between the proposed method and the existing technique with regard to fixed operating system time processing.

Table 4.1: Comparison of Time Processing with Windows 7 as OS

Ser	OS	Processing Time	Algorithm
1	Windows 7	5 Sec	Viola Jones
2	Windows 7	4 Sec	SVM
3	Windows 7	3.8 Sec	Tree Classifier
4	Windows 7	3.3 Sec	EOG
5	Windows 7	1.7 Sec	DWT-BD
6	Windows 7	0.9 Sec	Proposed Algorithm

5. CONCLUSIONS AND FUTURE WORK

5.1 CONCLUSIONS

This thesis deals with the problems of an online test for the student. It presents the fundamental ideas of cheating a method of online testing. It offers many techniques to identify and prevent online cheating by students. Continuous authentication is one of the approaches used to check that the users attend and check that the current user is the same. Algorithms have been developed for the implementation of a transparent and fair review system. For human face identification from low resolution photos, the technique has been presented. The suggested method for ocular motion detection continuously monitored pupil movement. The detection of the movement of the eyes is tracked to observe students engaging in cheating. It offered an effective method for monitoring and implementing the fair test system for entrance test students. It may also be utilized for study in academia and science.

5.2 FUTURE WORK

The technique presented included the identification of fraudulently pupils in groups of up to 3. To recognize 5 pupils from one frame, the system may be expanded.

The method presented may be enhanced to find students participating in cheating from the side perspective since the algorithm presented has not solved the issue from a side viewpoint. In the suggested approach, the processed video from the front perspective was acquired.

REFERENCES

[1] Bawarith, Razan, Abdullah Basuhail, Anas Fattouh, and Shehab Gamalel-Din. "E-exam cheating detection system." International Journal of Advanced Computer Science and Applications 8, no. 4 (2017): 176-181.

[2] Atoum, Yousef, Liping Chen, Alex X. Liu, Stephen DH Hsu, and Xiaoming Liu. "Automated online exam proctoring." IEEE Transactions on Multimedia 19, no. 7 (2017): 1609-1624.

[3] Rogerson, Ann M. "Detecting contract cheating in essay and report submissions: process, patterns, clues and conversations." International Journal for Educational Integrity 13, no. 1 (2017): 1-17.

[4] Meuschke, Norman, Moritz Schubotz, Felix Hamborg, Tomas Skopal, and Bela Gipp. "Analyzing mathematical content to detect academic plagiarism." In Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, pp. 2211-2214. 2017.

[5] Al-Bayed, Mohran HJ. "Intelligent Plagiarism Detection for Electronic Documents." PhD diss., 2017.

[6] He, Hui-Yu, Kan Kan, Chen-Yue Shao, Zhen-Yu Huang, and Xiang Zhang. "Method and realization of display information acquisition in black box cheating test of digital indicating weighing instruments." In Mechanical Engineering and Control Systems: Proceedings of the 2016 International Conference on Mechanical Engineering and Control System (MECS2016), pp. 282-288. 2017..

[7] Ruiperez-Valiente, Jose A., Pedro J. Muñoz-Merino, Giora Alexandron, and David E. Pritchard. "Using machine learning to detect ‘multiple-account’cheating and analyze the influence of student and problem features." IEEE transactions on learning technologies 12, no. 1 (2017): 112-122.

[8] Ferrara, Steve. "A framework for policies and practices to improve test security programs: Prevention, detection, investigation, and resolution (PDIR)." Educational Measurement: Issues and Practice 36, no. 3 (2017): 5-23.

[9] Fluck, Andrew, Olawale S. Adebayo, and Shafi'I. Muhammad Abdulhamid. "Secure e-examination systems compared: Case studies from two countries." (2017).

[10] Grocevs, Aleksejs, and Natālija Prokofjeva. "Modern programming assignment verification, testing and plagiarism detection approaches." In Proceedings of the IVUS International Conference on Information Technology, pp. 61-64. 2017.

[11] Von Gruenigen, Dirk, Fernando Benites de Azevedo e Souza, Beatrice Pradarelli, Amani Magid, and Mark Cieliebak. "Best practices in e-assessments with a special focus on cheating prevention." In 2018 IEEE Global Engineering Education Conference (EDUCON), pp. 893-899. IEEE, 2018.

[12] Kocdar, Serpil, Abdulkadir Karadeniz, Roumiana Peytcheva-Forsyth, and Vessela Stoeva. "Cheating and plagiarism in e-assessment: Students' perspectives." Open Praxis 10, no. 3 (2018): 221-235.

[13] Küppers, Bastian, Marius Politze, Richard Zameitat, Florian Kerber, and Ulrik Schroeder. "Practical security for electronic examinations on students' devices." In Science and Information Conference, pp. 290-306. Springer, Cham, 2018.

[14] Al-Bayed, Mohran H., and Samy S. Abu-Naser. "Intelligent multi-language plagiarism detection system." (2018).

[15] Wan, Han, Kangxu Liu, and Xiaopeng Gao. "Token-based approach for real-time plagiarism detection in digital designs." In 2018 IEEE Frontiers in Education Conference (FIE), pp. 1-5. IEEE, 2018.

[16] Kuo, Jong-Yih, Hsuan-Kuei Cheng, and Ping-Feng Wang. "Program plagiarism detection with dynamic structure." In 2018 7th International Symposium on Next Generation Electronics (ISNE), pp. 1-3. IEEE, 2018.

[17] Migut, Gosia, Dennis Koelma, Cees GM Snoek, and Natasa Brouwer. "Cheat me not: Automated proctoring of digital exams on bring-your-own-device." In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, pp. 388-388. 2018.

[18] Ulinnuha, Nurissaidah, Muhammad Thohir, Dian Candra Rini Novitasari, Ahmad Hanif Asyhar, and Ahmad Zaenal Arifin. "Implementation of Winnowing Algorithm for Document Plagiarism Detection." Proceeding of the Electrical Engineering Computer Science and Informatics 5, no. 1 (2018): 631-636.

[19] Xylogiannopoulos, Konstantinos, Panagiotis Karampelas, and Reda Alhajj. "Text mining for plagiarism detection: multivariate pattern detection for recognition of text similarities." In 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 938-945. IEEE, 2018.

[20] Wang, Lisheng, Lingchao Jiang, and Guofeng Qin. "A search of Verilog code plagiarism detection method." In 2018 13th International Conference on Computer Science & Education (ICCSE), pp. 1-5. IEEE, 2018.

[21] Munoz, Albert, and Jonathon Mackay. "An online testing design choice typology towards cheating threat minimisation." Journal of University Teaching and Learning Practice 16, no. 3 (2019): 5.

[22] Halak, Basel, and Mohammed El-Hajjar. "Design and evaluation of plagiarism prevention and detection techniques in engineering education." Higher Education Pedagogies 4, no. 1 (2019): 197-208.

[23] Manoharan, Sathiamoorthy. "Cheat-resistant multiple-choice examinations using personalization." Computers & Education 130 (2019): 139-151.

[24] Li, Zhizhuang, Zhengzhou Zhu, and Teng Yang. "A multi-index examination cheating detection method based on neural network." In 2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI), pp. 575-581. IEEE, 2019.

[25] Farhan, Noor S., and Matheel E. Abdulmunem. "Image Plagiarism System for Forgery Detection in Maps Design." In 2019 2nd Scientific Conference of Computer Sciences (SCCS), pp. 51-56. IEEE, 2019.

[26] Küppers, Bastian, Julia Opgen-Rhein, Thomas Eifert, and Ulrik Schroeder. "Cheating Detection: Identifying Fraud in Digital Exams."

[27] Nordin, Ili Najaa Aimi Mohd, Najla Aiman Nazari, Muhammad Rusydi Muhammad Razif, Nurulaqilla Khamis, Noraishikin Zulkarnain, Farkhana Muchtar, and Nor Aira Zambri. "Optimization of RF signal detection and alert system for restricted area." Indonesian Journal of Electrical Engineering and Computer Science 16, no. 1 (2019): 325-332.

[28] Chua, Samuel S., Joshuel B. Bondad, Zechariah R. Lumapas, and Joven D. L. Garcia. "Online examination system with cheating prevention using question bank randomization and tab locking." In 2019 4th International Conference on Information Technology (InCIT), pp. 126-131. IEEE, 2019.

[29] Kleerekoper, Anthony, and Andrew Schofield. "The false-positive rate of automated plagiarism detection for SQL assessments." In Proceedings of the 1st UK & Ireland Computing Education Research Conference, pp. 1-6. 2019.

[30] Jiang, Jilu, Baoxian Wu, Liang Chang, Kui Liu, and Tianyong Hao. "The design and application of an Web-based online examination system." In International Symposium on Emerging Technologies for Education, pp. 246-256. Springer, Cham, 2019.

[31] Sharma, Nitesh Kumar, Deepesh Kumar Gautam, Shanti Rathore, and M. R. Khan. "CNN Implementation for Detect Cheating in Online Exams During COVID-19 Pandemic: A CVRU Perspective." Materials Today: Proceedings (2021).

[32] Tiong, Leslie Ching Ow, and HeeJeong Jasmine Lee. "E-cheating Prevention Measures: Detection of Cheating at Online Examinations Using Deep Learning Approach--A Case Study." arXiv preprint arXiv:2101.09841 (2021).

[33] Jadi, Amr. "New Detection Cheating Method of Online-Exams during COVID-19 Pandemic." International Journal of Computer Science & Network Security 21, no. 4 (2021): 123-130.

[34] Ozgen, Azmi Can, Mahiye Uluyağmur Öztürk, Orkun Torun, Jianguo Yang, and Mehmet Zahit Alparslan. "Cheating detection pipeline for online interviews." In 2021 29th Signal Processing and Communications Applications Conference (SIU), pp. 1-4. IEEE, 2021.

[35] Kamalov, Firuz, Hana Sulieman, and David Santandreu Calonge. "Machine learning based approach to exam cheating detection." Plos one 16, no. 8 (2021): e0254340.

[36] Soltane, Merzoug, and Mohamed Ridda Laouar. "A Smart System to Detect Cheating in the Online Exam." In 2021 International Conference on Information Systems and Advanced Technologies (ICISAT), pp. 1-5. IEEE, 2021.

[37] Brynildsrud, Hanne, Andreas N. Digernes, Thomas I. Ramm, and Alis W. Wilson. "Cheating detection and prevention of unproctored home exams at NTNU."

[38] Samir, Mohamed Amr, Youssef Maged, and Ayman Atia. "Exam Cheating Detection System with Multiple-Human Pose Estimation." In 2021 IEEE International Conference on Computing (ICOCO), pp. 236-240. IEEE, 2021.

[39] Chirumamilla, Aparna, and Guttorm Sindre. "E-exams in Norwegian higher education: Vendors and managers views on requirements in a digital ecosystem perspective." Computers & Education 172 (2021): 104263.

[40] Dilini, Nimesha, Asara Senaratne, Tharindu Yasarathna, Nalin Warnajith, and Leelanga Seneviratne. "Cheating Detection in Browser-based Online Exams through Eye Gaze Tracking." In 2021 6th International Conference on Information Technology Research (ICITR), pp. 1-8. IEEE, 2021.

[41] Brimzhanova, Saule, Sabyrzhan Atanov, Khuralay Moldamurat, Botagoz Baymuhambetova, Karlygash Brimzhanova, and Aitkul Seitmetova. "An intelligent testing system development based on the shingle algorithm for assessing humanities students' academic achievements." Education and Information Technologies (2022): 1-23.

[42] Eko, Ceasar E., Idongesit Eteng, and Eyo E. Essien. "Design and implementation of a fault tolerant web-based examination system for developing countries." Eastern-European Journal of Enterprise Technologies 1, no. 2 (2022): 115.

[43] Gamage, Kelum AA, Roshan GGR Pradeep, and Erandika K. de Silva. "Rethinking Assessment: The Future of Examinations in Higher Education." Sustainability 14, no. 6 (2022): 3552.

[44] Krambia Kapardis, Maria, and George Spanoudis. "Lessons learned during Covid-19 concerning cheating in e-examinations by university students." Journal of Financial Crime 29, no. 2 (2022): 506-518.

[45] Mansoor, Marwah Najm, and Mohammed SH Al-Tamimi. "Computer-based plagiarism detection techniques: A comparative study." International Journal of Nonlinear Analysis and Applications 13, no. 1 (2022): 3599-3611.

[46] Maertens, Rien, Charlotte Van Petegem, Niko Strijbol, Toon Baeyens, Arne Carla Jacobs, Peter Dawyndt, and Bart Mesuere. "Dolos: Language-agnostic plagiarism detection in source code." Journal of Computer Assisted Learning (2022).