FACIAL AND KEYSTROKE BIOMETRIC RECOGNITION FOR COMPUTER BASED ASSESSMENTS

by

TEMITOPE OLUWAFUNMILAYO ADETUNJI

Student number: 216165431

Submitted in fulfilment of the requirements for the degree

MAGISTER TECHNOLOGIAE: INFORMATION TECHNOLOGY

Department of Information and Communications Technology,

FACULTY OF APPLIED AND COMPUTER SCIENCES

VAAL UNIVERSITY OF TECHNOLOGY

Supervisor: Prof. Tranos Zuva

Co-Supervisor: Dr. Martin Appiah

December 2019

DECLARATION AND COPYRIGHT

“I hereby declare that the dissertation submitted for the degree MTech: Information Technology, at Vaal University of Technology, is my original work and has not previously been submitted to any other institution of higher education. I further declare that all sources cited or quoted are indicated and acknowledge by means of a comprehensive list of references”.

Temitope Oluwafunmilayo Adetunji

DEDICATION

This study is dedicated to the Sovereign God, the Maker of heaven and the earth, the Almighty Father, a very present help in times of trouble.

ACKNOWLEDGEMENTS

To God be the glory for His mercies endures forever and for keeping me alive until this day. He alone is worthy to receive all glory, honour and adoration.

First and foremost, I would like to thank my supervisor, Professor Tranos Zuva for his constructive ideas for the successful completion of this Masters' programme. I also appreciate the support of my co-supervisor Dr. Martin Appiah for his insightful encouragement and constructive criticism.

I am grateful to Dr. Olusanya Yinka Agunbiade, who I owe a lot of gratitude for his financial and academic support.

Among those worthy to be mentioned are Dr TK Bello and family, Dr Isaac Adebiyi and family, Dr Richard Ikuesan and family, Dr Ilesanmi Daniyan and family and Dr Nnamdi Nwulu and family, may God bless you all.

I would also like to thank my immediate family: my lovely husband: Pastor Adetona Festus Adetunji and my wonderful children (Deborah, Dominion, Delight and Divine) for their support. I wish they would be rewarded for joys they have sacrificed during the period of my study. Not forgetting my mother, brothers, sisters, my in-laws, friends and their families for their indefatigable efforts and contributions, may God reward you mightily.

Last but not least a big thank you to Vaal University of Technology, the staff members of the Information and Communication Technology Department and the authorities at the Vaal University of Technology for the opportunities and financial support given to me and for giving me the opportunity to further my studies.

ABSTRACT

Computer based assessments have become one of the largest growing sectors in both non-academic and academic establishments. Successful computer based assessments require security against impersonation and fraud and many researchers have proposed the use of Biometric technologies to overcome this issue. Biometric technologies are defined as a computerised method of authenticating an individual (character) based on behavioural and physiological characteristic features. Basic biometric based computer based assessment systems are prone to security threats in the form of fraud and impersonations. In a bid to combat these security problems, keystroke dynamic technique and facial biometric recognition was introduced into the computer based assessment biometric system so as to enhance the authentication ability of the computer based assessment system. The keystroke dynamic technique was measured using latency and pressure while the facial biometrics was measured using principal component analysis (PCA). Experimental performance was carried out quantitatively using MATLAB for simulation and Excel application package for data analysis. System performance was measured using the following evaluation schemes: False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) and Accuracy (AC), for a comparison between the biometric computer based assessment system with and without the keystroke and face recognition alongside other biometric computer based assessment techniques proposed in the literature. Successful implementation of the proposed technique would improve computer based assessment's reliability, efficiency and effectiveness and if deployed into the society would improve authentication and security whilst reducing fraud and impersonation in our society.

TABLE OF CONTENTS

DECLARATION AND COPYRIGHT i

DEDICATION ii

ACKNOWLEDGEMENTS iii

ABSTRACT iv

LIST OF TABLES viii

LIST OF FIGURES ix

LIST OF ALGORITHMS x

LIST OF ABBREVATIONS xi

CHAPTER ONE 1

1 INTRODUCTION 1

1.1 Face Biometric 3

1.2 Keystroke Dynamics 5

1.3 Statement of Problem 6

1.4 Research Questions 6

1.5 Goal and Objectives 7

1.6 Expected Research Contribution 7

1.7 Thesis Structure 8

1.8 Chapter Summary 9

CHAPTER TWO: LITERATURE REVIEW 10

2 INTRODUCTION 10

2.1 Computer Based Assessment: Theoretical Background 11

2.2 Authentication in Computer Based Assessment 14

2.2.1 Knowledge based authentication 15

2.2.2 Possession based authentication 15

2.2.3 Biometrics based authentication 16

2.2.4 Other mechanisms 38

2.3 Bimodal Biometric 38

2.4 User Authentication using Face Biometric Authentication 41

2.4.1 Angle and pose 42

2.4.2 3D Facial Recognition 43

2.4.3 Attendance monitoring system 46

2.4.4. Face detection 48

2.4.5 Face tracking 49
2.5 User Authentication using Keystroke Biometric Recognition 50
2.6 Computer Based Assessment using Multimodal Biometrics 51
2.7 Chapter Summary 53
CHAPTER THREE: METHODOLOGY 54
3 INTRODUCTION 54
3.1 Proposed Bimodal Biometrics Model 55
3.2 Keystroke Authentication 56
3.2.1 Enrolment phase 57
3.2.2 Authentication/verification phase 60
3.2.3 Analysis of the proposed latency and pressure using moving average 60
3.2.4 Distance metrics used in the keystroke authentication experiment 60
3.3 Face Recognition 63
3.3.1 Image acquisition phase 64
3.3.2 Image pre-processing phase 66
3.3.3 Feature extraction using fast Principal Component Analysis 66
3.4 Matching Phase 69
3.5 Bimodal Authentication Decision 69
3.6 Data Collection (Biometrics Database Sources) 70
3.7 Chapter Summary 72
CHAPTER FOUR: EXPERIMENTATION AND RESULTS 73
4 INTRODUCTION 73
4.1 Experiment1: Performance of Fast PCA on face Image 75
4.2 Experiment 2: Performance of Moving Averages on Keystrokes Biometrics 76
4.3 Experiment 3: Performance of Bimodal Biometrics System 80
4.3.1 Authorized user attempt 80
4.3.2 Impostor attempt 81
4.4 Performance Evaluation 82
4.5 Experiment Discussion 84
4.6 Chapter Summary 85
CHAPTER FIVE: CONCLUSION, CONTRIBUTION AND FUTURE WORK 86
5 INTRODUCTION 86
5.1 Objectives Revisited 86
5.3 Contribution to Knowledge 89

5.4 Future Work 89

5.4 Chapter Summary 90

References 91

LIST OF TABLES

1.1 Features extracted in keystroke pressure……………………………………………….5

3.1 Features and users of the Faces96 database…………………………………………….72

4.1 Results of face biometric model………………………………………………….......76

4.2 Results of keystroke biometric model……………………………………………….79

4.3 Results showing the FAR, FRR and Accuracy of keystroke and face biometrics………………………………………………………………………….83

4.4 Results showing the average mean and standard deviation of the moving averages for both latency and pressure……………………………………………………………84

LIST OF FIGURES

1.1 Some of the features employed in face recognition ………………………………........4

1.2 Human face with distortion...4

2.1 Improved from Pellegrino……………………………………………………………...12

2.2 Invigilators observing online exam text takers………………………………………13

2.3 Online user authentication………………………………………………………....38

2.4 Biometric based methods of authentication……………………………………......41

2.5 Angle and pose showing various degrees……………………………………………43

2.6 Steps involved in authenticating a user……………………………………………...46

2.7 Feature point tracking..48

2.8 Images of an individual in two position……………………………………………..49

2.9 Real-time visual output……………………………………………………………...49

3.1 System model for face and keystroke authentication..56

3.2 Keystroke dynamic model…..57

3.3 Face recognition model...64

3.4 Logitech Camcorder……...65

4.1 Facial image with query and trained...75

4.2 ROC curve of face biometrics…………………………………………………….76

4.3 Interpolation of training and testing data on keystroke latency..................................77

4.4 Interpolation of training and testing data on keystroke pressure................................78

4.5 ROC curve of keystroke biometrics……………………………………………….....79

4.6a Combined face with keystroke image for authorized user...80

4.6b Combined face with keystroke image for unauthorized user.....................................81

4.7 ROC curves for face and keystroke biometrics………………………………………..82

LIST OF ALGORITHMS

1 Feature extraction algorithm in keystroke authentication……………………………61

2 Authentication algorithm in keystroke authentication . . . . …………....62

3 Training phase in face recognition ………………………………………………….67

4 Testing phase in face recognition ………………………………………………....68

LIST OF ABBREVATIONS

EFF	Effectiveness
FAR	False Acceptance Rate
FRR	False Rejection Rate
EER	Equal Error Rate
CON	Convenience
ACC	Accuracy
KBA	Knowledge Based Authentication
PBAF	Profile Based Authentication Framework
MATLAB	Matrix Laboratory
PIN	Personal Identification Number
ICT	Information and Communication Technology
IP address	Internet Protocol address
DNA	Deoxyribonucleic acid
ID	Identity

List of Publications

For the duration of the research, the following research papers were published or submitted that are related to the research work

Refereed Conference Papers

Temitope Oluwafunmilayo Adetunji, Tranos Zuva, and Martin Appiah (2018), A Framework of Bimodal Biometrics for Computer Based Assessment Authentication Systems**,** International Conference on Intelligent and Innovative Computing Applications (ICONIC), 6-7 August 2018, Durban, South Africa. 978-1-5386-6477-3/18/$31.00 ©2018 IEEE.

CHAPTER ONE

1 INTRODUCTION

Computer based assessment, according to the Joint Information Systems Committee (2006) involves the use of a computer for assessment-related actions. Computer based assessment can either be summative or formative (Jortberg, 2009). Formative Computer based assessments are used for gap identification between goals and current understanding by providing feedbacks, non-assessed activities and dialogue while summative computer based assessment are activities used for accountability, promotion, placement and certification (Peres, Lima & Lima, 2014). Computer based assessment has various advantages, which are:

- Speed: The results of the assessments would be pronounced speedily.
- Fairness: The fairness in the assessment will positively rise (Karami, Eussen, Schmitz-Rode & Baumann, 2009).
- Connectivity: Ability to connect with other virtual or computer based resources.
- Ease of Assess: Ability to assess the strengths and weaknesses of courses.

As a result of the advantages stated above, many organisations in the institution of learning, commercial, trade and industry sectors have been able to incorporate computer based assessments into their business operations (Alwi and Fan, 2010). On the other hand, the verification and security of a user appear to be a critical problem and a number of scholars have recommended the practice of biometrics to increase safety in computer based assessment systems. Biometric systems are systems, which make use of computer systems to detect a computer user based on physiological and behavioural uniqueness. The biological characteristics are: keystroke, speech, signature, gait, speech and over time, these traits usually change. The physiological traits include iris, face, palm print, and fingerprint, which are not subject to changes throughout a person’s lifetime (Aboalsamh, 2009).

Depending on the application context, a biometric system can operate in the authentication mode or in the identification mode. Authentication mode involves individual physically present biometric data, which was then compared against the stored database template. Data authentication has been a method of confirming the genuine rights of a computer user prior to the time secured resources were released. This method was accomplished by cross-checking unique data that was supplied by the user, which was centred on the face biometric and keystroke dynamic. On the user's uniqueness, the authenticity of the clone was required to be verified by the system based on the user's biometric features and keystroke dynamics.

In the identification mode, the biometric system recognizes the individual's identity by matching against multiple characteristics templates. It involves one-to-many comparisons for establishing individual identity (Hong & Jain, 1998; Ravi, Raja & Venugopal, 2011).

Thus, in the research of Salil and Sharath (2003), emphasis were made that problems and issues with the conventional physiological biometric systems arise with the tendency to lead to imitation or impersonation. Other issues such as malformed fingers as a result of genetic disorder, identical biometric features (identical twins), all pose risk to computer based assessment system. However, biometric system can be used as system authentication mode provided it satisfies the following requirements highlighted by Aboalsamh (2009) as well as Hong and Jain (1999).

- Uniqueness: This means no two individuals must have the same trait.
- Universality: It indicates that every individual must have the characteristics features.
- Collectability: The trait must be measured quantitatively.
- Circumvention: The rate at which the trait can easily be fooled.
- Acceptability: This implies the level of people agreeing to the biometric system.

- Performance: It shows that the robustness of the biometric system was measured by the accuracy and the speed.

In an attempt to overcome these threats, this research proposes the use of keystroke biometric (behavioural biometric technique) and facial biometric (physiological biometric technique) to improve the security concerns of computer based assessment system. The keystroke biometric recognition approach introduced to the biometric computer based assessment system talks about the habitual measures a user exhibits despite the fact that the user employs the keyboard as an input device. The smart phone as well as the touch screen devices are good examples of this (Zhong, Deng & Jain, 2012)**.** The keystroke biometric technique was used due to the fact that it does not require any hardware. Darwish, Abdelghafar and Ali (2010) as well as Wang, Mu and Zheng (2008) defined face recognition system as a technique of identifying human faces in an image by comparing the computed face image from the database. The face biometric technique was used due to the fact that image data can be acquired in non-intrusive conditions and its relatively low costs (Darwish *et al.*, 2010; Wang *et al.* 2008).

However, successful implementation of both techniques can improve security and privacy concerns in computer based assessment that focuses on biometric features only and if adopted into the society. It would reduce impersonation and theft for organisations using computer based assessment for their business operation (Zhong *et al.*, 2012).

1.1 Face Biometric

There are some significant features necessary for system recognition in face recognition. Some of these features are: eyes, mouth, nose, nostril and eyebrows (Mittal & Walia, 2008). In order to recognise an individual’s face, some weights are assigned to each of these highlighted features. Some of the features usually employed in face recognition are shown in

Figure 1-1. The task of extracting human face features with significant degree of accuracy and precision is a challenging task.

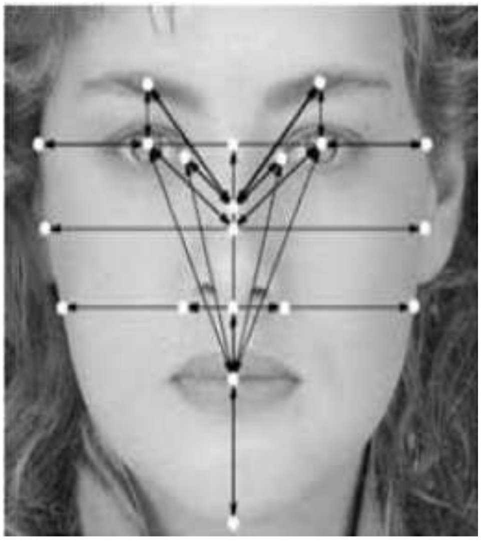


Figure 1-1: Some features employed in face recognition (Esan, Ngwira & Zuva, 2014)

The process of human eye extraction at a grey level can be obtained from the valley features. There exist a relationship between the human face and other facial characteristics such that the distance between the eyes, which contains the region of the eyes, eyebrows, nose and mouth, is equal to the size of the human face (Mittal & Walia 2008; Wong, Lam & Siu, 2001). Thus, several factors can affect the extraction of these features. Some of these factors are: face impressions, facial hair, glasses, amongst others. These factors can affect the accuracy of the process of features extraction and positioning (Mittal & Walia 2008; Wong *et al.*, 2001). Moreover, human face is known to be a 3-D object that remains susceptible to distortion and irregular illumination which can make the detection of the true face to be challenging. This is illustrated in Figure 1-2.

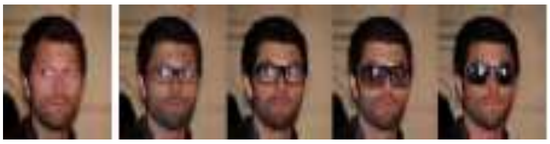


Figure 1-2: Human faces with distortion and intricate background (Zhenliang, Jie, Meina, Shiguang & Xilin, 2018)

1.2 Keystroke Dynamics

Flior and Kowalski (2010) defined keystroke dynamics as a strong behavioural biometric that deals with the unique characteristics present in an individual‘s typing rhythm. It means the biometric activities when each key was pressed and when it was released as a person types at computer keyboard. How we type on a keyboard defines what we call keystroke dynamics, which most often use timing information to decide the typing characteristics of a user. By measuring the time, a key was pressed and the time a key was released, possibility may arise to detect pattern that can be used to authenticate the user. In keystroke biometric, there are some characteristics, which are necessary for system recognition. Some of these features include: arithmetic mean, root mean square, energy, etc. Table 1-1 presents some of the features used in keystroke biometric recognition.

Table 1-1: Features extracted in keystroke pressure

Name of feature	
1. Root mean square	6. Energy
2. Peak	7. Skewness
3. Arithmetic mean	8. Signal in noise & distortion
4. Kurtosis	9. Fundamental frequency
5. Total harmonic distortion	

In view of the aforementioned, the aim of this research is to explore the concept of bimodal biometric authentication to design a system which will address the issue of authentication using the keystroke biometrics system and also provide a fast and accurate face extraction technique. This is to address the issue of impersonation and illumination to enhance user convenience and bolster computer based assessments.

Hence, one major contribution of this research to the body of knowledge is the provision of a new bimodal biometric authentication system, which has the potential of combating the challenges of an imposter being able to replicate or imitate exactly the authorized user's typing patterns and face feature extraction and illumination for user's authentication.

1.3 Statement of Problem

Over the years, the deployment of computer based assessment systems has been on the increase because of its advantages for businesses and organisations.

In computer based assessment, security and fraud are major concerns but Shende, Arode and Ghonge (2014) have recommended the application of biometrics to develop security with outstanding results. However, some limitations need to be addressed to improve the security concern of impersonation and fraud. One of the major problems of biometric security is that biometric features can be stolen without the awareness of the user (Flior & Kowalski, 2010). It can also be possessed by other people, for example, in the case of identical twins, and all these pose security threats for computer based assessment systems. These problems can be minimised by introducing the combination of both keystroke and face technique which is a unique way of identification for every individual into biometric computer based assessment systems to improve their security issues and concerns (Salil & Sharath, 2003).

Thus, the successful implementation of the proposed technique would make it better than other computer based assessment systems that rely on biometrics technique alone to address the issue of security (El-Abed, Giot, Hemery & Roenberger, 2012).

1.4 Research Questions

Computer based assessment systems have become an important tool employed in businesses and organisations but biometrics could help reduce impersonation and fraud, although there are still security issues and concerns that need to be addressed to improve its performance. Therefore, in this study the key research question is:

- How can you use facial and keystrokes techniques for bimodal computer based assessment authentication to minimize threats?

In addressing this question the following sub-questions need to be answered:

- How can we improve the computer based assessment biometric technique proposed to minimise security threats?
- How can the keystroke techniques and facial biometrics recognition be introduced into the computer based assessment systems?
- What evaluation methods can be used to measure keystroke and facial biometric computer based assessment systems?

1.5 Goal and Objectives

Based on the main question stated above, the goal of the research was to have a system that continuously authenticate a user and this would be attained by implementing the following research objectives:

- To conduct studies on various computer based assessment systems proposed in the literature.
- To propose the use of facial and keystrokes techniques for bimodal computer based assessment authentication.
- To measure the effectiveness of a bimodal authentication computer based assessment systems.

1.6 Expected Research Contribution

The major contributions of this research are as follows:

- Improvement on a multimodal biometrics of facial biometric and keystroke dynamics, which would be used to authenticate and validate newly computer, based assessment system.
- A combination of facial biometric technique and keystroke dynamics would be employed to verify and validate the physiological and behavioural characteristics of an individual in order to prevent impersonation and fraud in computer based assessment systems.
- Improvement in the system security, which would be a major contribution to the computer based assessment field and if deployed in industries, would minimize fraud, impersonation and theft whilst increasing effectiveness and efficiency of the system.

1.7 Thesis Structure

This thesis is structured as follows:

Chapter 2: Reviews of related works on biometrics and computer based assessments as well as discussion based on theoretical framework for this research work.

Chapter 3: Presents proposed system design model, methods and pseudo-codes used in the experiments.

Chapter 4: Discusses and presents the results of the experiments performed to obtain the research objectives for this research work.

Chapter 5: Presents summary of the entire study, recommendations, conclusion, contribution and future work, of the research work. The achievements, shortfalls and future endeavours are discussed in the chapter.

1.8 Chapter Summary

This chapter focused on the introduction of this research. The techniques to be used as it would be shown in subsequent chapters are briefly discussed. The problem facing biometric security was outlined. The introduction of the combination of both keystroke and face technique which remains a unique way of identification for every individual into biometric computer based assessment systems are presented as a possible solution to this challenge. Furthermore, the research questions and the contribution to knowledge of this research were outlined.

CHAPTER TWO: LITERATURE REVIEW

2 INTRODUCTION

The fast growth in technology has added value to the tendencies of insecurity in the academic environment where the use of computer based assessment is of paramount use. In a bid to overcome this uncertainty, certain techniques have been proposed by researchers such as the use of password, token, signatures ID, etc. (Das and Debbarama, 2010). However, these traditional authentication techniques exhibit some disadvantages as they can easily be lost, stolen and forgotten (Zhang, 2008). Thus, in the research of Salil and Sharath (2003), they recognized that there are problems and issues with the old techniques of authentication as it can be imitated by non-genuine users which may increase hazard rate to computer based system.

Nevertheless, in order to improve security in computer based assessment, several scholars have recommended the use of biometrics (Darwish *et al.*, 2010; Wang *et al.*, 2008).

The structure of biometric are measures that practice workstations to recognize a user centred on behavioural and physiological features e.g. face, fingerprint, signature voice etc. (Shende *et al.*, 2014). Models of behavioural traits are: speech, gait, keystroke and signature, whereas the physiological traits include fingerprint, face, iris and palm print (Aboalsamh, 2009).

Despite the fact that biometrics systems was used as alternatives for determining the verification of a user during computer based assessment, a number of individuals are still confronted by several issues which are still directed towards the dreadful conditions of the system performance as regards interval, identification and precision (Awad, 2012).

Nonetheless, these issues have been looked into by many scholars via dissimilar procedures so as to improve the overall identification system performance; the perfect ways out for various problems are still inaccessible. On the other hand, this chapter presents an in-depth review of computer based assessment, biometrics, multimodal biometric authentication in computer based assessments, brief overview of keystrokes dynamics, face biometric and their theoretical background.

2.1 Computer Based Assessment: Theoretical Background

Computer based assessment systems refer to the method of evaluating human footprint produced on computerised systems such as phone and touch screen panels (Ullah, Xiao, Lilley & Barker, 2012). These footprint holds footprints which possess cognitive characteristics and is also unique in a way to each individual and holds huge characteristics for personal identification (Ullah *et al.,* 2012). Successful implementation of this technique would improve security and privacy concerns in computer based assessments that focus on biometric technique only and if adopted into the society, it would reduce impersonation and theft for organisations that uses computer based assessment for their business operations. Assessment systems offer the ways to measure single and organisational achievements, and so can have a deep driving effect on structures they were intended to serve. There exists to be an intimate association between teaching, knowledge and assessment as illustrated in Fig. 2-1. Robitaille Schmidt, Raizen, Mcknight, Britton and Nicol (1993) differentiated three modules of the curriculum: the proposed curriculum (set out in policy statements), the applied curriculum (which can only be known by studying the classroom practices) and the accomplished curriculum (which relates to what students can do at the end of a course of study).

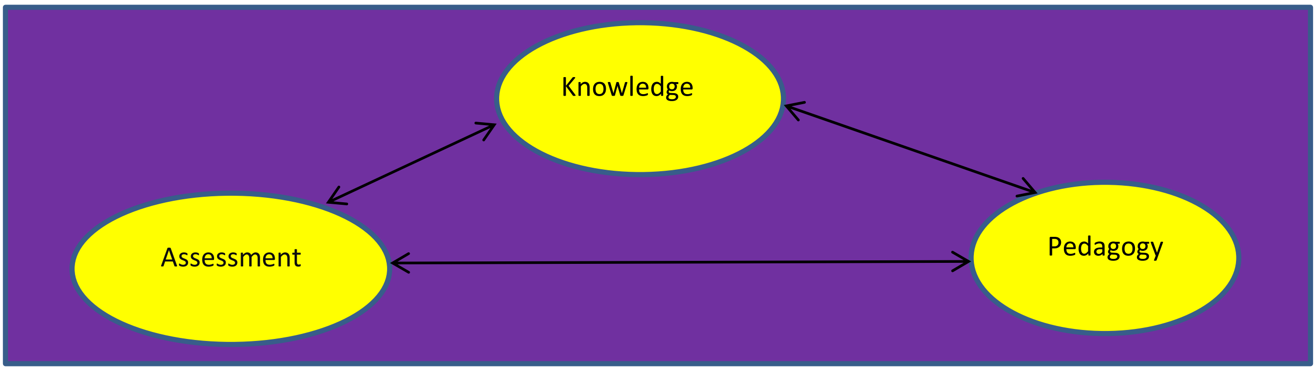


Figure 2-1: Relationship between teaching, knowledge and assessment (Improved from Pellegrino, Chudowski & Glaser, 2001)

Over the past few decades, the use of the internet has been growing extensively due to the establishment of innovative applications such as distributed data processing, multimedia, teleconferencing, particularly distance learning and e-learning (Hillier & Fluck, 2013). Therefore, educational establishments have sustained the operation of e-learning in taking electronic exam (e-exam), teaching courses and taking electronic assessment (computer based assessment). One of the major concerns in education is the successful evaluation of a student especially during the computer based assessment. The introduction and application of the computer based assessment was gradually taking the place of the traditional evaluation. Furthermore, computer based assessments techniques are created for successful learning environment and also to provide the appropriate information linked to the improvement of the educational development (Hillier & Fluck, 2013).

In the past, research done in the area of assessments, which are computer based, has generally concentrated on the desire to intensify supervision and proper scrutiny in a classroom or organized location in the course of assessments that use computers. Figure 2-2 shows invigilators standing in order to observe online exam test takers.

Figure 2-2: Invigilators observing online exam test takers (Jean, 2017)

Countless number of these structures combines a number of checking which are network-based, which in itself necessitates suitable monitoring software and system arrangement. The more important concern however was regarding the uniqueness of the verification during assessment. Commonly, user authentication was performed interferingly and hence the computer user is mindful as soon as authorizations remain necessary. In an environment where examination malpractice is rampat on the part of the computer user, this offers information to the computer user as to when to make available the illustration. Also, away from the original authentication at the start of the assessment, no additional authentication is completed – even though stages of checking over video and microphones can be delivered.

A structure that would authenticate a computer user either non- interferingly or visibly, would make accessible a tool intended for uninterruptedly authenticating the legitimacy of the computer user nonetheless, devoid of them having to clearly offer a record or model of biometric.

In spite of the predicted aids of Computer based assessments, one of the major issues and threat is basically security (Zviran and Erlich, 2006).

Limitations and challenges recognized by scholars and practitioners associated to Computer based assessment are:

- Impartiality to the student
- Objective testing of knowledge the capacity of students to respond in electronic mode
- Plagiarism
- Impersonation threats on user's security

2.2 Authentication in Computer Based Assessment

Karim, Shukur & Ghazal (2016) defined authentication as a method of verifying a person's legitimate right prior to the period when safe resources are released. Generally, this happens to be attained via counterchecking unique information provided by an individual.

The area of dynamic verification was quite original in association towards out-dated verification tools. Its motivation is based on the capacity to conspicuous and uninterruptedly verify a computer user using credentials gotten from the computer user despite the fact that they habitually intermingle by means of the automated device or computer system.

Several computer systems are secured through a method of user authentication (Zviran and Erlich, 2006). Apampa Woulds and Argels (2010) claim that computer based assessment systems are observed as safe and applicable when the instruments effectively identify (Who are you?) and confirm (Is it really you?) the examinee. Karim *et al.* (2016) in their work introduced different groups of instruments for online authentication, which they term, knowledge, biometric, possession and others. The groups and methods of authentication are:

- Knowledge based authentication
- Possession based authentication

- Biometric based authentication
- Other mechanism based

2.2.1 Knowledge based authentication

Knowledge Based Authentication usually stated as KBA is the most widely used authentication technique which seek to prove the identity of an individual accessing a service such as a website (Ullah *et al.*, 2012; Zviran & Erlich, 2006). This kind of authentication requires the knowledge of an individual's private information in order to gain access to a secured information or data. Examples of commonly used KBA are embedded in textual or graphical password, personal identification number (PIN) and pattern code. The major advantages of this technique is the fact that the implementation of passwords are less costly, it stands to be less difficult to use and user friendly (Ullah *et al.*, 2012, Zviran & Erlich, 2006). Nevertheless, due to the fact that students may share their user ID or passwords to friends in order to increase their result grades, this technique stands to be liable to malicious attacks and impersonation (Ullah *et al.*, 2012).

Some limitations associated with KBA are:

- Password could be revealed from time to time therefore it happens to be insecure.
- Not ever trusted for authentication throughout computer based assessment.

2.2.2 Possession based authentication

Zviran and Erlich (2006) defines Possession Based Authentication (PBA) as a token-based authentication, which is an authentication centred on secretive entity that the user has. A token is usually a hardware device that can be kept in a pocket and can be carried with the user. It stands to be an entity that involves user to physically own as a method of authentication. Token however, are vulnerable to loss or theft as it can be stolen or reproduced by fraudulent means (Flior & Kowalski, 2010). This however implies that there is no assurance on uniquely identifying a legitimate user even with the ownership of token because, it remains susceptible to loss, theft or replicated through fraudulent means. The most common examples of PBA ae smart cards tokens, memory cards, keys, smart cards, etc. (Zviran & Erlich, 2006).

Some limitations associated with PBA are:

- Device may possibly be transferred to others.
- It would not be entirely efficient if lost by the student.
- Deliberate disclosure of the password to be used by another unauthorised student.

2.2.3 Biometrics based authentication

Vaclav and Riha (2003) defines biometrics as the physiological and behavioural characteristics, which is uniquely linked to an individual and can be classified as soft biometrics and hard biometrics. Hard biometrics include fingerprints, retinas, facial features and vein pattern while soft biometrics include signature, voice, tattoo, skin, height, etc. Physiological biometrics are the characteristics features of an individual that can be seen such as: face, palm prints, hand, eye, dental and DNA. Behavioural biometrics are the characteristic features of an individual, which is based on the individual's behavioural qualities that are measured as learned actions. As an illustration, using the framework of an electronic mobile device, certain quantity of biometric-based techniques could be used towards capturing and authenticating the genuineness of the computer user as shown in Fig 2-2.

The benefit of biometrics remains that, most times, it happens to be mobile, so, it must in the possession of the owner frequently and they cannot be disremembered. Drawbacks are numerous, comprising of the inability to modify them if desirable, or inability to utilize them for all purposes as they are easily disclosed and are not influenced by non-human individuals that require authentication (Vaclav & Riha, 2003).

Depending upon the application framework, the identity of a person can be determined in two ways:

- Verification
- Identification

2.2.3.1 Verification

An individual to be identified submits a claim; which can be either accepted or rejected. Authentication is carried out on the user in conjunction with a username or ID number and smart card. Thereafter, the biometric template captured will be compared with the one stored against the registered user either on a smart card or on database for verification.

2.2.3.2 Identification

An individual is identified without a person claiming to be identified. Authentication is carried out on the user from the biometric characteristic only without the use of username or ID number and smart card. The biometric template is matched to all records within the database and a closest match score is returned. The closest match within the allowed threshold is considered as the individual and authenticated (Awad, 2012).

In literature, however, verification and identification are interchangeably used for biometrics recognition (Jain & Kumar, 2010).

Various diverse phases of social composition, behaviour or chemistry could be designed for verification of biometric. The variety of a specific biometric for use in a precise presentation consists of a weighting of quite a lot of aspects. Hong and Jain (1999) recognized seven of such aspects to be used when evaluating the appropriateness of any feature for use in the verification of biometric. The seven factors are enumerated and well-defined below:

- Universality implies that every individual using a system should possess the trait.
- Uniqueness implies the trait should be adequately different from one individual to another in the relevant population such that they can be easily identified from one another.
- Permanence deals with the variation of the trait over time. More specifically, a trait with 'good' permanence would be reasonably invariant over time with respect to the specific matching algorithm.
- Measurability otherwise known as collectability deals with the ease of acquiring or measuring the trait. In essence, such data acquired should be in a form, which allows subsequent extraction and processing of the sets of important feature.
- Performance deals with the precision, accuracy, speed, and robustness of technology employed.
- Acceptability relates to the acceptability of the employed technology by individuals within the relevant population as evidenced by the willingness of the individuals to have their biometric trait captured and evaluated.
- Circumvention deals with the ease of imitation of a trait using an object or substitute.

Proper biometric use is application dependent. Certain biometrics would be better than others based on the required levels of convenience and security. No single biometric would meet all the requirements of every possible application.

Listed below are the performance indicators applied for the biometric systems, which are:

- False Match Rate (FMR): This otherwise referred to as the False Accept Rate (FAR). It is the possibility that the structure wrongly equals the form of input to a non-matching model in the database. It measures the percentage of unacceptable inputs that are wrongly accepted. In a situation of match scale, if the individual happens to be an imitator in the actual sense, but the corresponding score was greater than the starting point, then the individual would be treated as real. As a result, this would bring an increase in the FAR, which therefore also be subjected to the rate of threshold

- False Non-Match Rate (FNMR): This is otherwise referred to as the False Reject Rate (FRR). It is the possibility that the system refuse to identify equality among the input design and a corresponding pattern in the database. It measures the percentage of usable inputs that are wrongly disallowed.
- Receiver Operating Characteristic or Relative Operating Characteristic (ROC): The ROC diagram is a graphical representation of the exchange between the FAR and the FRR. Broadly, the corresponding algorithm carry out a conclusion established on a starting point that defines how close to a pattern the input requires to be in order for it to be well thought-out to be a match. If the starting point is decreased, there would be smaller quantity of non-matches that are false but more false accepts. On the other hand, a higher starting point would decrease the FAR but would make the FRR to increase. A joint disparity is the Detection Error Trade-off (DET), which remained obtained by means of usual aberration scales on the two axes. This additional linear graph light up the variation for greater routines (fewer mistakes).
- Equal Error Rate or Crossover Error Rate (EER or CER): This is the percentage at which the acceptance error equals the rejection error. The ROC curve can be used to obtain the rate of the EER. The EER remains a rapid method to equate the precision of devices with diverse ROC curves. Broadly, the degree of precision of a device is a measure of its EER. The higher the EER, the less precise the device and vice versa.

- Failure to Enrol Rate (FTE or FER): This is the percentage at which the efforts to generate a pattern from an input remains failed. This is usually triggered by near to the ground superiority inputs.
- Failure to Capture Rate (FTC): Surrounded by automatic systems, this is the possibility that the system will fail to identify a biometric input when accessed properly.
- Template Capacity: This represents the full number of groups of data that could be stored in the system.

There are two major categories of biometrics, they are:

- Physiological biometrics
- Behavioural biometrics

2.2.3.3 Physiological biometrics

Physical biometrics relies on creating a profile of an individual based on a particular physical characteristic. The most commonly used are fingerprint, iris, facial, hand geometry, vein pattern, voice and retina.

This type of mechanism according to researchers is found out to be more dependable, more precise, and more safe, as it happens to be hard to make a replica of it compared to the behavioural biometric mechanism which are noticeable. Examples of commonly used physiological mechanisms are listed as follow:

- Fingerprint
- Iris
- Facial
- Voice

2.2.3.3.1 Fingerprint

The use of fingerprint in an authentication process is very important. Fingerprints are the most common form and are now found in many laptops and mobile devices. The fingerprint of the user was scanned for the purpose of authentication. A fingerprint scanner requires an image of a user's finger and it needs to ascertain if the pattern of ridges and valleys in the image matches the pattern of ridges and valleys already in the database. Following the scanning of the fingerprint, some distinct points are established in order to know the performance of the features of fingerprint (Stén, Kaseva & Virtanen, 2003). These features are thereafter matched with the ones that have earlier been stored. Fingerprint systems are measured to be the earliest means of identification. It is desirable due to the fact that the consolidated fingerprint readers used in measuring the performance accuracy of the characteristic feature of the fingerprint was of low cost and readily available for use (Jain & Kumar, 2010).

2.2.3.3.2 Iris

The iris is one of the utmost reliable and precise physical biometric features in the human's eye (Jain & Kumar, 2010). This organ (iris) which is positioned in the middle of the cornea and lens of the human is a thin circular diaphragm. One of the major reasons why this particular biometric feature was sometimes preferred was due to the fact that it was relatively insensitive to modifications in observing angle and deviations (Lumini & Nanni, 2007).

2.2.3.3.3 Face

Face recognition, which is the outcome of the two main methods, was also used in authentication. The methods are: geometric method and photometric method. Geometric method, which became the first method used in authentication under face recognition was centred on computing the geometric distribution amid face features (eyes, nose, mouth, etc.).

This type of recognition can take charge of both the non-frontal and frontal face outlook. The other method, which happens to be photometric in feature, was based on the overall view of the face and it covers only frontal face. These two methods i.e. geometric and photometric require prior data of the features extracted and the pre-processed image, which have been stored in the databases. Nevertheless, a method that eradicates the necessity of such data was proposed by Śluzek and Paradowski (2012); the concept of near-duplicate detection and key-point matching was used for the image match.

The use of facial biometrics for the authentication of a person is a non-intrusive process, thus, can be done clearly without bias. The authentication process can be done without the knowledge of the person being authenticated. Over the years, some specific algorithms have been developed with the ability for face detection and features tracking of the face primarily to identify and authenticate individuals. One of such algorithm is the Kanade-Lucas-Tomasi (KLT) algorithm. With the aid of the camera, the face images can be obtained and represented as vectors. The facial biometric can be computed by finding the mean Eigenvector. The Kanade Lucas-Tomasi (KLT) algorithm is one such algorithm. Images of the face can be obtained by a camera and are represented as vectors. The conclusion of the result shows a face recognition rate of 93.5%. Equation 2-1 expresses the mean vector of the images being assessed.

$$\mu = \sum_{i=1}^{\mathrm{N}} \chi_i \qquad (2\text{-}1)$$

Where: $\mathrm{X} = (x_1, x_2, \ldots\ldots x_i, \ldots\ldots x_N)$ represents a $n \times N$ data matrix

N is the number of facial images being examined

x_i is the vector with dimension n having a $p \times q$ image

Therefore;

$$n = p \times q \qquad (2\text{-}2)$$

Some of the works done on face recognition by researchers indicating results and limitations are reviewed below:

In the work of Chin and Suter (2006), an explicit report of universal technique for face recognition system using Eigen approach was used. In this approach, the problem of variations in identifying faces from images was addressed. The research was conducted to authenticate the method on YALE face database and the result achieved indicate that the approach was vigorous in addressing the problem of variations in facial appearance and likewise able to categorize the identified faces from unidentified faces. The outcome of this method appears unfavourable for the real-world resolutions.

While using neural network and Eigen face, Agarwal, Jain, Kumar and Agrawal (2010) in their research introduced face recognition. The principal component analysis was employed for the extraction of the face features and a feed forward back propagation neural network was also used to identify the input face from the database. Face database of Olivetti as well as Oracle Research Laboratory (ORL) were both used to experiment the algorithm with 40 classes and 10 images collected from each class, which resulted, to 400 images.

In the result, a recognition rate of 97.018% was obtained. Hence, the researchers concluded that the method was good though it was not carried out on a distorted face.

In the research of Sahoolizadeh Heidari and Dehghani (2008), they presented a different face recognition method, which was centred on Principal Component Analysis, LDA (Linear Discriminating Analysis), and Neural Network. The technique encompasses pre-processing phase which was aimed at improving the clarity of facial image, alongside with the Principal Component Analysis (PCA), which was used to decrease the dimensionality of the image and linear discriminating analysis was also employed for features extraction from the image. The classification of the images was used using the artificial neural network. Publicly available Yale facial database was used to carry out the experiment and the outcome of the result shows the efficiency when related with further approach which led to a recognition percentage of 89.5% being obtained. Furthermore, they found out that the method they used can improve the clarity of 28 facial image though the pragmatism of the method was not stated and the experiment was also not carried out on distorted face.

Nandini, Bhargavi and Sekhar (2013) in their work on face recognition carried out an experiment using Neural Network. In identifying the images, the features of the new faces were compared with the image that was already in the database. Furthermore, the feature extraction was carried out from face localization parts such as eyeballs, mouth endpoints and the distance between the eyeballs and the mouth endpoints were calculated. The face recognition experiment was carried out through the neural network using Back Propagation Networks (BPN) and Radial Basis Function (RBF) Networks and there was comparison with the results obtained with that of other previous techniques. The conclusion of the result shows a face recognition rate of 90.5%.

In a quest to resolve the problems of existing line-based face recognition method Ming & Ma, (2006) in their research proposed an upgraded line based face recognition method which is a well-known by its features. This method used a feature known as Line-based Singular Value (LSV) feature to reduce the effect of face recognition under variable illumination intensity. The LSV feature was used to compute the distance between two lines instead of image grey-level rate. The result of the approach was proved to be invariant to illumination intensity. However, the disadvantage of this approach is its high cost of computation.

Another group of researcher that worked on face recognition were Lin, Kung and Lin (1997). In their work, a triangular-based approach was used to carry out a well-organized human face recognition system. The approach comprises of two main parts: the first part searched for the potential face region while the second part was used for the purpose of identification.

Lin *et al.* (1997) proceeded further to prove that there are certain problems which the recognition can address, which are: occlusion of mouth and sunglasses, different lightning conditions, different face sizes and varying pose and expression.

The outcomes of the results indicate that the approach produced an effective precision of 92%, which makes it an improvement over the conventional methods.

Using Artificial Neural Network (ANN), Ouerhani, Jridi and Alfalou (2010) in their work proposed face recognition and authentication to answer the problem of the method of learning which originates from enormous database necessary for face or no face images detection. In this method, a neural network which has a database tested on window 18 × 27 pixels was utilized in order to ascertain whether the image is a face or non-face. In the approach, the pre-processing phase was used for image precision, gradient vector was used to extract while artificial neural network was used for the face recognition.

Performance evaluation was done on the experiment using holomorphic filtering and histogram equalization and a better performance was indicated in the result.

A new optimized method for face recognition using Eigen faces was established by Gupta Markey & Bovik (2010). The Eigen face method applied a threshold rate to reduce the measurement of the face space which was determined by the quantity of Eigen faces selected and also, to increase the routine of face space.

Nevertheless, an optimized value for the threshold was selected which is 0.8 times of the extreme value of the least Euclidean distances of each images from other images and this was joined with the designated 15% Eigen face values for human face recognition. The evaluation of the experiment indicates an improvement in the performance of recognition system, which resulted to a precision rate of 87%.

Nagi, Ahmed and Nagi (2008) proposed another technique for face recognition by means of image-based approach towards artificial intelligence. In this approach, the redundant data from face image was removed by the technique by compressing the image using 2-Dimensional Discrete Cosine Transform (2D-DCT). In order to construct feature vector, features were extracted by the DCT from compressed face image, which was based on the skin colour, and the DCT co-efficient were also computed. An unconfirmed learning procedure which uses a Self-Organizing Map (SOM) was put in place in order to classify DCT-based feature vectors into groups to categorize if the subject in the input image is present or not.

In the work of Neagoe, Mitrache and Preotesoiu (2006), a face recognition model that utilizes Gabor wavelet cascade with simultaneous neural modules was projected. The face database that was used to carry out the experiment was ORL face database. In the process, the feature localization conforming to face boundary, nose, mouth and eyes were extracted. The image dimensionality was reduced by the Principal Component Analysis (PCA) while, concurrent self-maps was used for the classification of the image. The outcome of the results produced a recognition rate of 86%.

In order to detect a hierarchical image, Wang *et al.* (2008) in their research used a pattern equivalent and 2DPCA algorithm with a multifaceted background applying a coarse image classifier to group image as both face or non-face by means of face prototype and two-eye template. Face from the outstanding images in the database was identified through the use of the 2DPCA algorithm. The outcome of the result indicates that the method decreases the time in which the image would be detected and also develops the accuracy rate of face detection.

In recognizing face image, Latha, Ganesan and Annadurai (2002) in their work used a neural based algorithm to identify the frontal view of face. The dimensionality of the face was reduced via the Principal Component Analysis (PCA) while the recognition was done through the use of Back Propagation Neural Network (BPNN). The total number of face images that tested were 200 and this was gotten from a YALE face database. The outcome of the result indicates an improved performance with an acceptance ratio that happens to be above 90%.

In the work of Thakur, Sing, Basu and Nasipuri (2007), they proposed a well-organized face recognition method using principal component analysis (PCA) and Radia Basis Function (RBF) neural network. The research was analysed on AT & T by means of 120 hidden layers, in order to decrease the dimensionality and the variation of face image data, the Principal Component Analysis (PCA) was used while intra31 class selective features of the trained images was used to model the hidden layer neurons of the neural network. This helps the Radia Basis Function (RBF) neural network to acquire enormous differences in lower-dimensional input space and upgraded the generalization properties. The conclusion of the end result shows an average sensitivity percentage of 87.75% and an exact rate of 89.94%.

Rani and Devoraj (2012) proposed another face recognition system, which was based on hybrid feature extraction method. In a bid to carry out this experiment, 2D Principal Component Analysis (2DPCA) and discrete orthogonal Krawtchouk Moment (KM) were both used to acquire universal and local features from the face. In order to generate accurate classification, a fuzzy integral was used, also, in classifying the image, the RBF classifiers were used. The conclusion of the experimental end result shows an improved routine of fusing several RBF's with the use of fussy fundamental.

In the work of Gowda, Kumar and Imran (2018), a face recognition structure using hybrid approach was proposed. In their experiment, the database that was used as a benchmark was the YALE face database and this was utilised by partitioning the face image into matrices of rows and columns and in order to generate a global vector, Eigen vectors were estimated on each matrix. In their results, they discovered that hybrid-based approach has an improved recovery time rate and average recognition rate in comparison with other approaches. Their limitation was in the aspect of recognising face from image which they termed it as a problematic task as a result of disparity in the difficulty of image background and face appearance.

Nandini *et al.* (2013), did another research on face recognition. In their work, they experimented face recognition via Neural Network, and implemented their recognition by relating the features of the new face images to that in the database. The features of the new face images were extracted from face localization parts, for example: eyeballs and mouth end points. The distance between the mouth endpoints and eyeballs were also calculated. The face recognition was done with the use of the Radial Basis Function (RBF) Networks and Neural Network using Back Propagation Networks (BPN) and 32 results were obtained related with other aforementioned methods. The outcome of the result indicates an improved performance with a system accuracy of 89.5%.

Yang, Wang, Zeng, Shen (2017), introduced a novel Gabor feature-based face recognition method. In carrying out their experiment, they made use of the Supervised Local Preserving Projection (SLPP) in continuing the local arrangement in the facial image through the use of class labels of data point in order to improve its discriminant power into a low-dimensional space. Furthermore, Yang *et al.* (2017) found out that SLPP are vigorous to facial expressions and lights. However, SLPP was also joined with Gabor feature vector, which was gotten from Gabor wavelet face image representation. CMU PIE database and AR database were both used to carry out test on numerous face images. The outcome of the result indicates that SLPP method has a higher performance when matched with combination of Gabor and PCA technique, LPP technique, PCA method and LDA technique.

In addressing the problem of skin colour like backgrounds with series of illuminations, Hu, Yang, Huang and Huang (2011), presented a feature-based face recognition that was centred on skin colour and facial feature. The method was divided into three phases: In the first phase, the skin region was extracted through the use of YcbCr skin-colour model. In the second phase, in a bid to acquire corresponding candidate face, the template of the face was estimated. In the third and the final phase, the feature of the faces was extracted in order to discover candidate's faces.

The outcome research shows that the method used yielded a very positive and good result in identifying face images with lights as their background.

Using a holistic representation, which is a known as spectra face, Lai, Yuen, and Feng (2001), in their work, presented a new technique for face recognition. The Fourier transform and the wavelet transform were combined together by the spectra face. Lai *et al*. (2001), improved on the already existing spectra face in order to handle problems associated with the translation and rotation of face images. In order to calculate the recognition rate of the technique, YALE and Olivetti face databases were used. In the course of carrying out the experiment, 565 face images with 55 persons who has diverse illumination and impressions environments were used. The outcome of the results indicate that the first three face images gives a system accuracy that is above 98% while a recognition time of less than 3 seconds was obtained.

A technique that uses Linear Discriminant Analysis (LDA) and Principal Component Analysis (PCA) in detecting face regardless of face recognition problems such as occlusions, pose, lightning, ageing, illumination and expressions, was the research carried out by Suhas, Khurle and Khanale (2012). Pose variation database, standard face data base and local face databases were the basis on which the experiment was carried out. The outcome of the result in their first experiment using PCA shows a performance accuracy of 100% while the other experiment using grimace face database also indicate a performance accuracy of 100% as well.

Another research worthy of note on face recognition was the work of Sharif, Ayub, Sattar and Raza (2012). In their research, a face recognition system which increases the accuracy of face recognition via Sub-Holistic PCA (SH-PCA) method was proposed. In carrying out their experiment, ORL face database was used in testing the method on 400 face images. The outcome of the result indicates performance accuracy rate of 90%. Conversely, when Sharif *et al.* (2012) compared the method they used which was Sub-Holistic PCA (SH-PCA) method to that of Principal Component Analysis (PCA), they found out that extra computational power and memory is needed in SH-PCA method compared to PCA method.

2.2.3.4 Behavioural biometrics

Al-khazzar (2010) defines behavioural biometrics as a measurable behaviour, which could be used to identify or confirm the uniqueness of a person. It focuses on behavioural patterns rather than physical attributes. Behavioural mechanism are the features of an individual's feedback concerning a positive incidence; the performance accuracy of these features are calculated through broad interpretations and clarifications. In order to foretell an individual's future behaviour, the distinctive features are analysed through specialised software (Al-khazzar, 2010). Examples of commonly used behavioural mechanisms are listed as follow:

- Voice
- Mouse dynamics
- Keystrokes dynamics
- Signature authentication

2.2.3.4.1 Voice

Eveno and Besacier (2005) defines voice biometric as a biometric that can be used for both speaker identification and speech recognition. In this type of biometric feature, the human voice can be identified via computerized system based on speech wave data acquired. Some intra-individual variations such as accent, voice pitch, and human voice features, can be used a unique identifier for biometric feature (Eveno & Besacier, 2005). As a behavioural method of authentication, it may be a safe option for securing online examinations (Shaver & Acken, 2009). A foremost practical problem in voice recognition can be the intra-individual variation. In the course of recording the samples of the voice during the enrolment and authentication period, user training can be an overhead in the context of virtual learning (Eveno & Besacier, 2005).

2.2.3.4.2 Mouse dynamics

Asha and Chellappan (2008) defines mouse dynamics (like keystroke dynamics) as a behavioural biometric that also captures non-intrusively as a learner interact with the computer (uses the mouse). Any mouse action can be classified into one of four categories (Asha & Chellappan, 2008):

- Mouse-Move – Any all-purpose movement of the mouse.
- Drag-and-Drop – This depicts the downward action of a mouse down which is followed by the upward mouse action.
- Point-and-Click –This illustrates the motion of the mouse, which is followed by a single or double click.
- Silence –This is a situation where there is no motion. The actions of the mouse are measured within an angle of 45° of a circle. This shows that a maximum of 8 directions in which the movement of the mouse movement can take place. With the use of the keystroke and mouse dynamics, the complexities associated with the use of non-standard computer equipment for authentication are eliminated.

2.2.3.4.3 Keystroke dynamics

Keystroke dynamics biometrics is a data processing method which analyses the manner in which a user types via proper monitoring of inputs of the keyboard in order to identify them by their characteristic typing trends (Araujo, Sucupira, Lizarraga, Ling, & Yabuuti, 2004).

Also known as typing biometrics, this authentication mechanism uses typing patterns (elapsed time between pairs of keystrokes) in order to authenticate a user. A technique was presented by Flior and Kowalski (2010) for offering uninterrupted biometric user verification in computer based assessments by means of keystroke dynamics. As related to other physical and behavioural biometrics, keystroke dynamics biometrics falls short to be a sole biometrics authenticator. Conversely, by integrating keystroke dynamics, biometrics into the existing password authentication system, even if the imitator is able to present the correct login information, either by hacking or key logger, without the right typing pattern, access would be denied. In contrast, the use of a singular password authentication would guarantee access to any user in as much as the login credential received is correct not considering if the user is authentic.

The aim of the keystroke dynamics is to obtain the biometric data when a learner types on the computer keyboard. The following metrics are considered in the process of authenticating a learner using the keystroke biometrics: characteristic errors, flight time, typing speed, characteristic sequences and keystroke seek time. The diagraph is the time between keystrokes and forms an important part of the keystroke biometric data. In order to match the keystroke data obtained with the templates in a database, the correlation approach is usually employed. The correlation coefficient r can be determined using equation 2-3.

$$r = \frac{\sum_{i=1}^{n}(k_i * t_i)}{\sqrt{(\sum_{i=1}^{n}(k_t^2) * \sum_{i=1}^{n}(t_t^2)}} \qquad (2\text{-}3)$$

Where:

K is the vector length n in storing the flight of the stored template

T is the vector of length in storing flight between keystrokes of a biometric sample

Over the years, lot of research has been done by several authors in addressing the problem of fraud and impersonation during computer based assessment. Numerous algorithms have been structured by many researchers to address some issues that affect keystrokes biometrics authentication system.

In the works of Forsen, Nelson and Staron (1977), they investigated the possibility of using keystrokes dynamics to differentiate between typist. In their research, diverse means of authentication were considered which include; keystrokes dynamics. A small group of subjects were made to type their own and each other's names. The summary statistics indicated that the subject typing his/her own name can be differentiated from another subject typing the same name. This work done by Forsen *et al.* (1977), provided typical illustration of two extensive broad classes of keystrokes dynamics research namely the: log-on type and in-session classes of authentication. The merit of this approach is that, with log-in type application, there is presentation of classifiers with short typing samples which are similar to what could be seen at log-ins, names, user IDs, and passwords. Also with the in-session application, classifiers are presented with longer and more free-style typing of samples that a classifier, which could be encountered when monitoring the typing activities of a particular user, e.g., word processing and composing mails.

In order to produce a concise report in their findings in keystrokes dynamics, Gaines, Lisowski, Press and Shapiro (1980) in their work recorded 7 typists over two sessions separated by months. The subjects transcribed Three (3) pages of words and sentences in each session. A down-down time (the time between the key-down-event of the first key in a diagraph and the key-down event of the second key) was indicated by the researchers, which are log-normally distributed. Their findings indicated that there are no significant changes in a subject's down-down times from the first session to the second. A statistical test capable of ascertaining whether a transcription record was typed by a certain subject or not was produced. The results obtained from their experiments indicate the seven (7) subjects were perfectly distinguished but the authors further explained the need for follow-up work as a result of the small number of subjects on which require large amount of transcriptions.

Stewart, Monaco, Cha and Tappert (2011) proposed a new technique for keystrokes dynamics using stylometry. In their work, they collected textual input data from 40 students in a spreadsheet modelling class. The students took a series of three exams each with ten questions; the questions were structured so as to consider textual input in the answer. Keystrokes Entry System (KES) online test taker system was used to capture the textual and keystrokes timings (The KES is a web-based application that provides an interface for instructions as well as an interface for students to answer test questions). In their study, the researchers investigated keystrokes and stylometry biometric systems with the aim of developing a system that verifies test-takers' identities in an online environment and in their results, they observed that although some biometric authentication can provide continuous and random authentication, nevertheless, keystrokes biometric is superior to the stylometry biometric as it shows limited and inadequate applicability to test takers.

In the development of a keystroke dynamics-based user authentication system using the ARTMAP-FD neural network, Loy, Lai and Lim (2007) in their work, made use of both latency and pressure in improving the error rate. To achieve this, the effectiveness of ARTMAPFD in classifying keystroke patterns, which was analysed and compared against a number of widely used machine learning systems, was indicated. The results show that ARTMAP-FD performs efficiently compared to many of its counterparts in keystroke patterns classification. Apart from that, in order to investigate the identity of a user, typing pressure was applied. The results from the experimentations show that the combination of both the latency and pressure patterns can significantly improve the Equal Error Rate (ERR) of the system. Some of the features used in keystroke biometric recognition are represented in table 1-1.

While using a single biometric system during computer based assessments, Flior and Kowalski (2010) in their research tried to present a method for providing continuous biometric user authentication in an online examination via keystrokes dynamics. They found out that keystrokes dynamics can be used for continuous authentication of online users during computer based assessments as there is no need for additional hardware. The demerits of their work is that a unimodal biometric is liable to impersonation threats (Apampa *et al.*, 2010).

In the work of Tenreiro de Magalhães and Santos (2005), a new keystroke dynamics algorithm was presented and the strategy was compared with some other solutions. In improving on the algorithm, they found out that for each keystroke, the algorithm would measure the time latency which is defined as TLP, and compare it with the one stored. The comparison result would be a hit if and only if equation 2-4 applies.

$$Lowest(Average\ median)*\left(0{,}95-\frac{SDeviation}{Average}\right)\leq TLP \leq Higher\ (Average, median)*\left(1{,}05+\frac{SDeviation}{Average}\right) \qquad (2\text{-}4)$$

This same calculation is repeated for all the password or passphrase keystrokes, resulting in a Boolean array. In their results, they concluded that this algorithm is a feasible solution for a flexible and easy to use identification and authentication process.

In a bid to address the practical importance of using keystrokes dynamics as a biometric for authenticating access to work stations, Monrose and Rubin (2000) in their work reviewed the current state of keystrokes dynamics and presented classification techniques based on template matching and Bayesian likelihood models. Their research gave rise to the limitation that unlike non-static biometrics (such as voice), there are no known features of feature transformations which are dedicated solely to carrying discriminating information. Hence, they therefore suggested the use of diagraph – specific measures of variability instead of single low – pass filters.

The use of a keystroke dynamics in addition to user name and password was the work proposed by Ramu, Suthendran and Arivoli (2020). In their work, the proposed system comprised of two layers of student's authentication using keystrokes biometric authentication in addition to user name and password. The result shows that the process of using keystrokes dynamics in addition to user name and password can be used as unending and transparent authentication of student during an on-line examination and that, there is no need for additional hardware thereby making the method cost effective. The only limitation is that, unimodal biometrics are susceptible to impersonation threats and fraud (Apampa *et al.,* 2010).

The possibility of imitating someone else's keystroke typing if appropriate feedback is provided is what gave rise to the research work of Teh, Teoh, Tee and Ong (2008). In their work, they proposed a novel feedback interface called mimesis with the aim of achieving the following:

- Ensuring that the information must be easy to understand with minimal cognitive load required.
- The interface should provide specific tips on particular aspects to improve on.
- Both positive and negative feedback should be provided to the attackers so that the individual can repeatedly make minor adjustments to the typing pattern in order to imitate better.

In achieving these objectives, a group of 84 participants were grouped together to play the roles of attackers against one of the best keystrokes biometric systems by Araujo *et al.* (2004), based on the analysis by Killourhy and Maxion (2009). They further evaluated in their research the effectiveness of mimesis and they demonstrated that there exists individuals who can adjust their typing pattern to imitate someone else. In their results, they found out that even the best detector can be defeated by imitation with mimesis. The authors concluded that keystroke biometrics alone is unsuitable as an authentication mechanism.

The findings of Tey, Gupta and Gao (2013) revealed that keystroke patterns can be imitated. The easier the password the greater the risk of imitation and vice versa. Conversely, factors such as the use of external keyboard, typing consistency, speed of typing, imitation strategy and similarities in typing patterns were reported to have less influence on the outcome of imitation.

2.2.3.4.4 Signature authentication

Signature authentication is a distinctive behavioural characteristic and a possible candidate for the authentication of users. It is a broad feature that has continued to gain increasing acceptability in every day's activities and life relations (Adamski, 2008). Nevertheless, as observed by Meshoul and Batouche (2010), technological advancement has facilitated the capture and authentication of human signature combining computer software and hardware. Some accessories such as the digital pens, tablets and digital signature pads are often used to capture data relating to digital signature (Asha & Chellappan, 2008). In contrast, signature may not be definitely repeated in some biometric features as only the signatory can imitate the original signatures. Conversely, there are some other issues that may mitigate the recognition of signature such as the influence of individual's physical and emotional conditions, signature disparities at different occasions, signature forgery and complexities of algorithms (Jazahanim, Ibrahim & Mohamed, *2*009).

2.2.4 Other mechanisms

In this method, authentication is based on a process, such as the user's location, a timestamp or their IP address. Before and during authentication, it answers the questions where are you? When did you login? How long does it take you to login>

The diagram in figure 2-3 shows the various techniques used in authenticating a user during computer assessment.

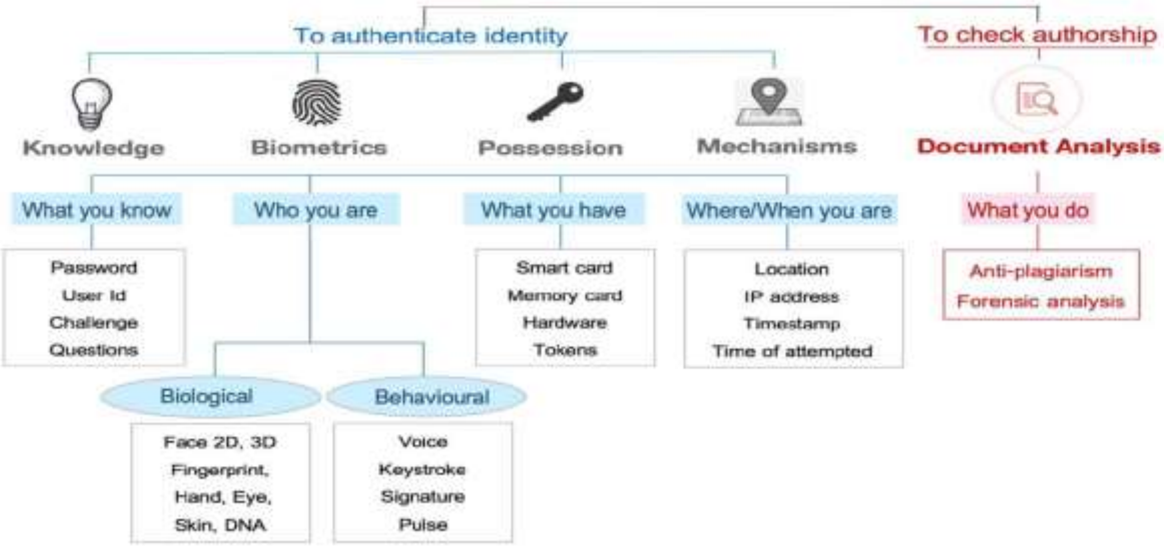


Figure 2-3: Online user authentication methods with its techniques (Nader & Zarina, 2016).

The limitations of biometric based authentication are as follow:

- Costly and hard to implement.
- It involves special-purpose hardware

2.3 Bimodal Biometric

Several years ago, in an attempt to examine and evaluate the issue of impersonation or imitation during computer based assessments; quite a lot of researchers had studied additional biometric techniques apart from a unimodal biometric system for the reason that a number of restrictions faced in the progress of their study they assumed more than one biometric system can evaluate (Jain & Kumar, 2010).

Considering the above, several methods of multimodal techniques by means of various manner of procedures have been recommended in the previous studies. Some of these include the use of palm patterns together with the name and password of the users was established by Al-saleem and Ullah (2014). In such practice, the outcome of their research show that both methods can be used for authentication and incessant confirmation and that the technique was good for authentication as soon as the student registers or input his records. They reached an assumption that using a unimodal type of biometric can be prone to fraud and impersonation (Apampa *et al.,* 2010).

In order to ascertain the genuineness of a computer user during computer assessment, Gao (2012) in their work, used IP address and timestamp in addition to a new method which was proposed to witness learners. In their study, the IP address and timestamps of the computer user were used to discover one or two false behaviour. In their outcome, they detected that the application of the method was not demanding because there was no necessity for further hardware but as stated in their outcomes, an inference was reached that this method is predisposed to risk if similar device is often used and besides, the address of the IP may perhaps be changed.

Ullah *et al.* (2012) in their study introduced the method of test questions by way of proposing an original technique known as Profile Based Authentication Framework (PBAF). In order to confirm the learners, which participated in the computer based assessment, the test queries were reset in. The findings of the study indicates that the use of the queries may remain structured without any difficulty and additional hardware was not required. Nevertheless, they came to a conclusion that the technique that was introduced is predisposed to fake risk since it is well thought-out to be easy to share.

Rudrapal, Das, Debbarma, Debbarma, and Kar (2012) in their study, proposed a new method for verifying a computer user during computer based which is voice recognition. As their study progress, a microphone was employed to improve the actual outcome of the voice recognition so as to permit the user of the computer enrol for the computer assessment. The findings of the study show that the concept of voice recognition can be employed for continuous authentication as well it can be beneficial for those with impaired vision or individuals who do not make use of a computer keyboard for interfacing with the computer system. Nonetheless, the conclusion of the findings was that the act of a single method of biometric for the authentication of a computer user during computer based assessment is prone to imitation and intimidations.

In order to detect the authentication of a computer user during computer assessment, Penteado and Marana (2006) in their work made use of another technique which is face recognition. In their study, an attempt was made in-order to evaluate the accuracy of face recognition, which was carried out, on-line via webcam. The outcome of the study revealed that face recognition is suitable for incessant authentication of computer users. On the other hand, they also added that a unimodal type of biometric for computer users during computer assessment is predisposed to fraud and risk (Apampa *et al.,* 2010).

In a quest to identify the validity of computer users during computer assessment, Chellappan Karim and Shukur (2015) in their work made use of finger print and mouse movement. They were able to achieve this by projecting an authentication system, which was then used to put up with numerous computer based assessment services. The outcomes of the study established the fact that the fingerprint method is suitable for the identification of individuals including their behaviour and can also be employed for continuous authentication of users. The result on the other hand indicates that there exists a diverse condition which is be required for effective incessant authentication. Also, an important necessity is a fingerprint which should be supported by a scanner device. The authors concluded that the device that was introduced can bring about issues to this verification technique due to the fact that it is expensive and more so, the fingerprint feature is also predisposed to theft. Figure 2-4: presents the biometric-based methods for authentication.

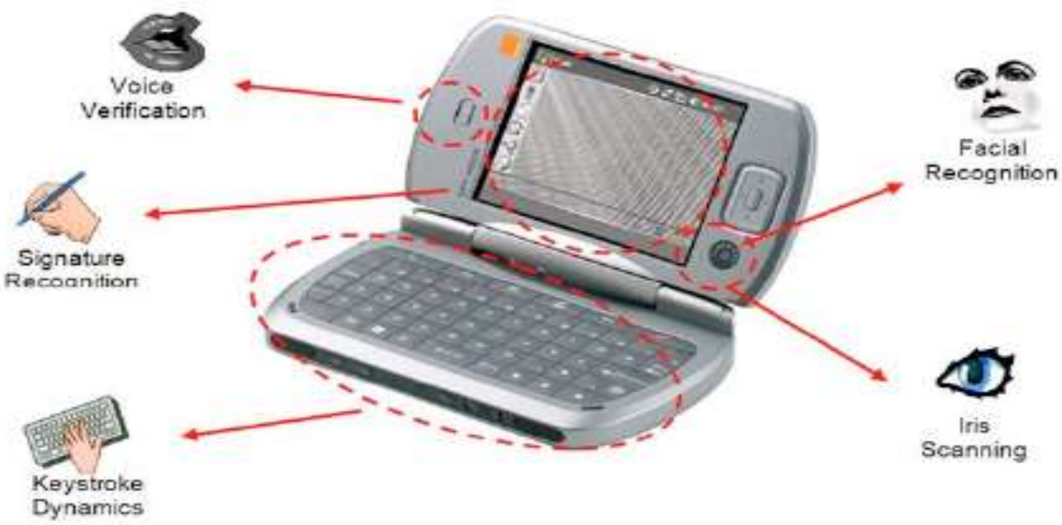


Figure 2-4: Biometric-based methods for authentication (Clarke, Dowland, and Furnell, 2013)

2.4 User Authentication using Face Biometric Authentication

The face biometric authentication system is incorporated in the computer based assessment device to recognize and authenticate the computer user permitted to gain entrance into the assessment and also to endlessly authenticate the individuality of the computer user pending the completion of the assessment.

In detail, all through the period of enrolling in the course (once used as a measure of a computer based system) or for an assessment, pictures of students, (in addition to further dynamic data), are taken and kept in the database. The images that have been captured are encoded to guard students' privacy. During the period of the assessment, the availability of the learner's identity is confirmed in the venue of examination and is supervised by matching the images that had been already captured with the one kept in the database.

A new method for continuous user authentication that continuously collects soft biometric traits is introduced. Soft biometrics traits are physical, behavioral or adhered human characteristics, which have been derived from the way human beings normally distinguish their peers (e.g. height, gender, hair color). Those attributes have a low discriminating power, thus not capable of identification performance. Additionally they are fully available to everyone, which makes them private and safe. The method used automatically registers the user every time the user logs in by combining conventional password with soft biometric traits or face recognition method (Clarke *et al.*, 2013).

The following features are the major ways a user can be authenticated using face biometric authentication**:**

- Angle and pose
- 3D facial recognition
- Attendance monitoring system
- Face detection
- Face tracking

2.4.1 Angle and pose

The angle at which the face to be recognised works correctly until 20°, and if this angle is overcome, problems begin to arise. It affects the expression, which, if different from the one stored in the database, can produce errors. There are methods where the database includes images of a person in different poses and are the most used. In the case of 3D recognition this inconvenience would disappear.

Figure 2-5 presents the angle and pose showing various degrees.

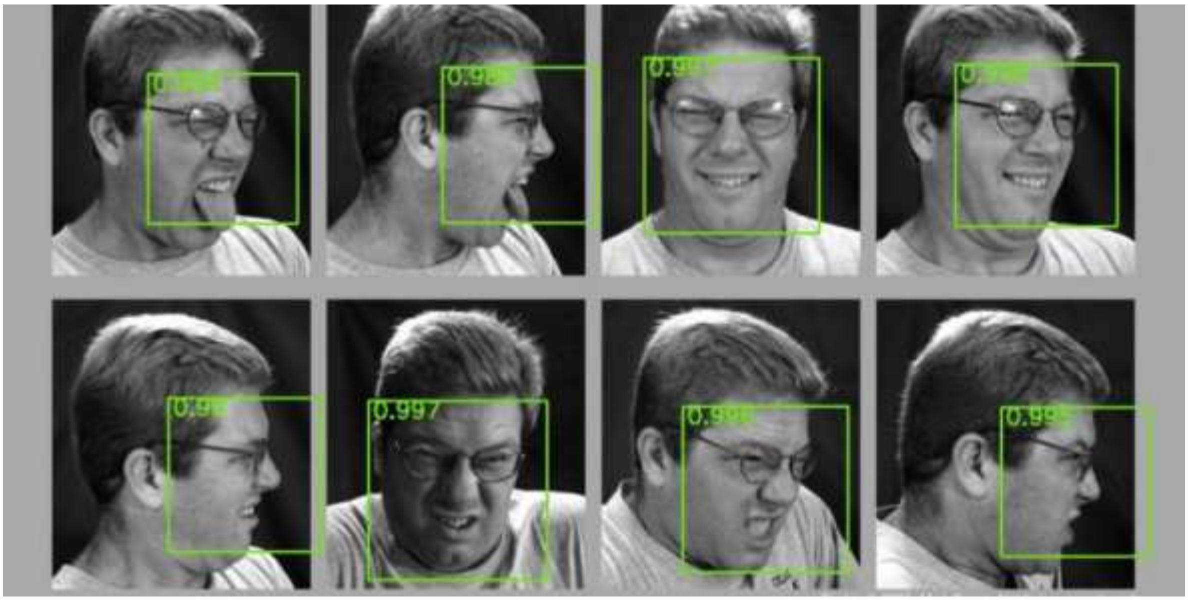


Figure 2-5: Angle and pose showing various degrees (Gourier, All & Crowley, 2004)

2.4.2 3D Facial Recognition

In facial recognition software, which uses a 3D model, there is a newly-emerging trend which claims to provide more accuracy. In order to capture the 3D image of an individual's facial surface in real time, the 3D facial recognition employs the unique characteristics of the face where the rigid tissue and bone is most obvious, like the nose, curves of the eye socket and chin in order to recognize the individual. These are specific examples of the areas that are matchless and not subject to change over time.

In the course of using depth and an axis of capacity which is not affected by light, 3D facial recognition can equally be carried out in the dark and possess the capacity to identify a user at diverse observe directions with the possibility to identify up to 90° (a face in sketch).

By using the 3D software, the system drives over a succession of stages to authenticate the individuality of a person. The following steps captured in figure 2-6 are involved in authenticating a user using 3D facial recognition, and they are:

- Detection
- Alignment
- Measurement
- Representation
- Representation
- Matching
- Verification and Identification

2.4.2.1 Detection

In order to acquire and detect an image, an existing photograph (2D) can be digitally scanned or by using a video image to acquire a live picture of a subject (3D).

2.4.2.2 Alignment

Once the system detects a face, it determines the position of the head, pose and size. As earlier stated, the individual has the possibility of being recognized up to 90^{o}, however with 2D, the head must be turned at least 35 ^{o} toward the camera.

2.4.2.3 Measurement

The curves of the face are measured by the system on a sub-millimetre (or microwave) scale and a format is then created.

2.4.2.4 Representation

The system decodes the template into a distinctive code. This coding gives each template a sequence of numbers to signify the features on a subject's face.

2.4.2.5 Matching

This would occur without any alterations being made to the image if it is a 3D image and the database also comprises 3D images.

However, there is an issue presently mitigating the effective use of databases, which are still in 2D images. The 3D images offer a quick subject whose variable move and can be compared to a flat and unchanging image. The introduction of innovative technology is resolving this problem. The minute a 3D image is captured, three diverse points are frequently identified which are: the outer eye, the inner eye and the nose’s tip. These would be drawn on view and weighed. As soon as those quantities are well positioned, an algorithm (which is a step-by-step process) would then be put on the image to transform it to a 2D image. Once transformation is done, the software would at that time associate the image with the 2D images in the database to obtain a likely equality.

2.4.2.6 Verification and identification

The process of verification involves the matching of an image to only one image in the database. For instance, an image taken of an individual may be matched to an existing image in another database with the aim of verifying the real identity of the person. However, in a situation where the identification is the main goal, then the captured image will be compared to all the images in the database. This is bring about the allocation of a score for each possible match. In this case, an image can be taken and compared to another database in order to identify the individual.

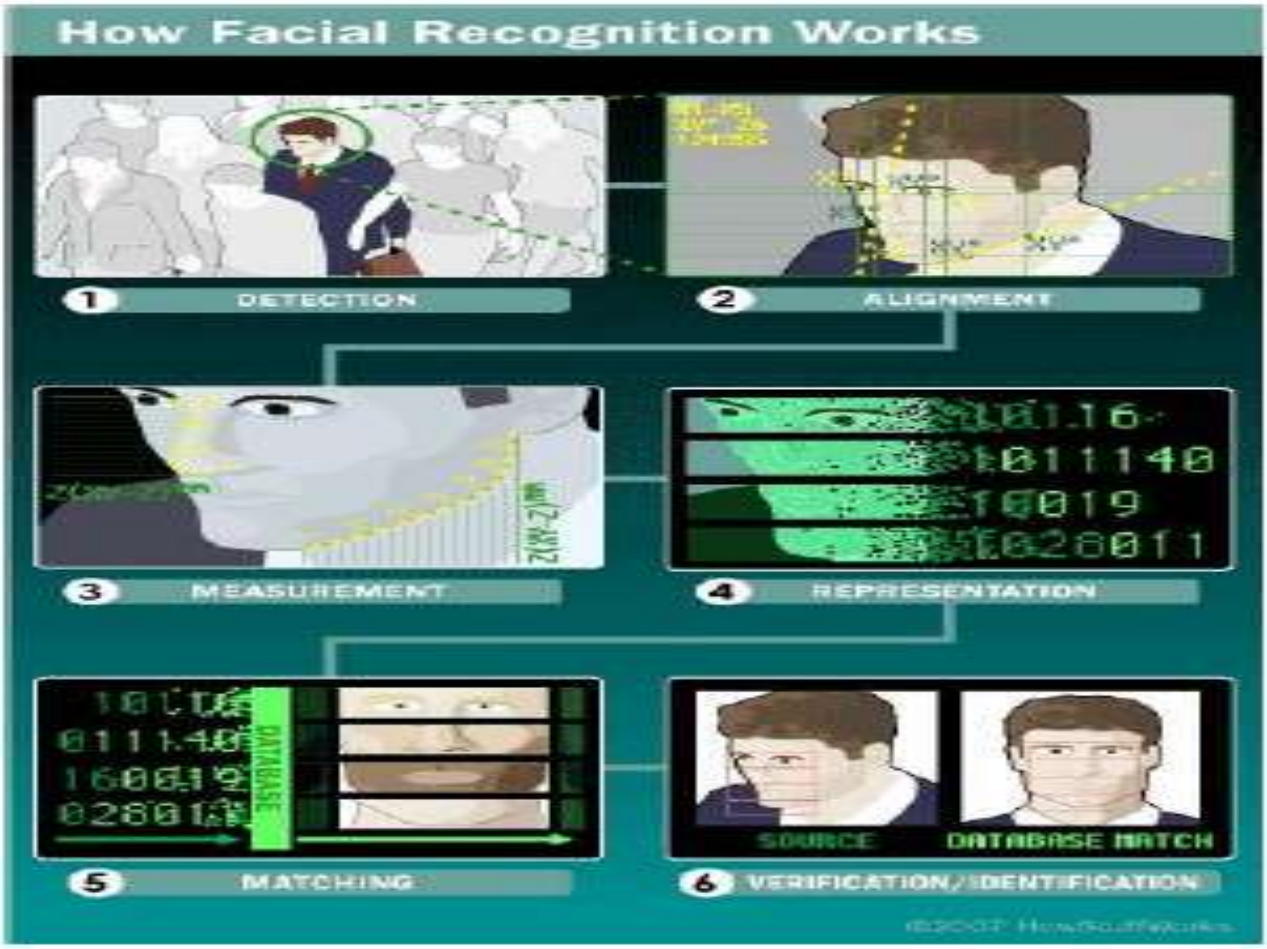


Figure 2-6 Steps involved in authenticating a user using 3D facial recognition (Gourier et al., 2004)

2.4.3 Attendance monitoring system

Facial recognition system is broadly employed for the identification and authentication of a person through the use of digital or a video camera from a video source (Bhattacharyya, Alisherov & Choi, 2009).

The main aim of applying face recognition biometrics in attendance monitoring system includes:

- The integration with the surveillance system.
- The capturing of images of people in a public area.
- Its use in legacy database.

While using an automated attendance monitoring system Bhattacharyya *et al.,* (2019) in their study presented a monitoring system with a real time face recognition background world having a database of student's information using the Personal Component Analysis (PCA) algorithm. The PCA is a method commonly used for identifying data patterns and transmitting such data as eigenvector in order to showcase the differences and similarities between the different data. The PCA process is summarized in the following steps according to equations 2-5 to 2.8 (Sayeed, Hossen, Kalaiarasi, Jayakumar, Yusof, & Samraj, 2017).

Let $\{P1, P2,.....PN\}$ be the training dataset

The average Avr is defined as equation 2-5.

$$Avr = \frac{1}{N}\sum_{i=1}^{N} Pt \qquad (2\text{-}5)$$

All elements in the training dataset changes from Avr by the vector presented in equation 2-6.

$$V_i = P_i - Avr \qquad (2\text{-}6)$$

The covariance matrix Cox is obtained as equation 2-7.

$$Cox = \frac{1}{N}\sum_{i=1}^{N} V_{li} V_i^{\tau} \qquad (2\text{-}7)$$

Select N' significant eigenvectors of Cox as Y_k's and calculate the mass vectors M_{ik} for each element in the training dataset, where K differs from 1 to N'

$$M_{ik} = Y_k^T . (P_i - Avr), \forall, K \qquad (2\text{-}8)$$

As a result of using the attendance monitoring system, the attendance rate of the student is monitored and can be effectively analysed once the period of taking the attendance is over. If the attendance rate of the student falls below eighty percent, an automatic message of notification to that effect is generated by the system to warn such students.

2.4.4. Face detection

The accurate detection of human faces from arbitrary images is the first important step of facial recognition. Thus, the goal of face detection is to determine whether there are any faces in a given arbitrary image and, if present, to return the image location and extent of each face.

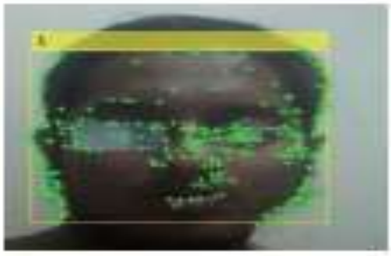


Figure 2-7: Feature point tracking (Viola & Jones 2001).

In the research work of Viola and Jones **(**2001), face detection was carried out using the "video-to-image" method. The registration phase of this method is characterized by the recording of two video samples of the user followed by the authentication process in future logins, which would, carried out via a comparison analysis between the image captured and the two videos recorded. The videos of the user are usually recorded during the registration phase in the following positions:

- Reading a 200-word text
- Typing a text

Each of the recoded video is usually within a period of three seconds with the number of frames depending on the frame rate of the webcam and the tow status as shown as in Figure 2-8.

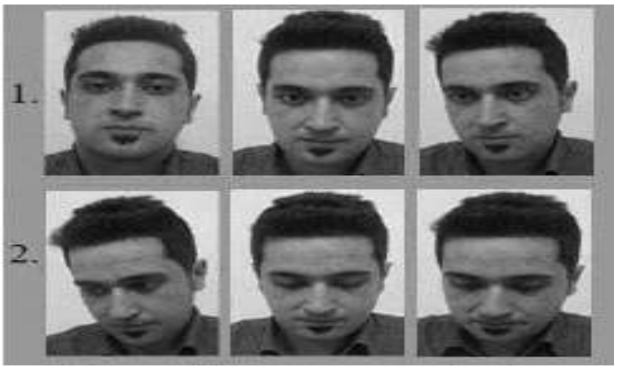


Figure 2-8: Images of an individual in two positions: 1) reading, 2) typing (Mohsen, Hadhoud & Amin, 2010).

2.4.5 Face tracking

The automatic detection and tracking of (typically corner-like) feature points throughout an image sequence is a necessary prerequisite for many algorithms in computer vision. One of the most popular methods for feature point tracking is the Kanade-Lucas-Tomasi (KLT) algorithm which was introduced by Lucas and Kanade (1981), later extended in the works of Tomasi and Kanade (1992). The process of face tracking continues as long as the user is in sight with the face uncovered.

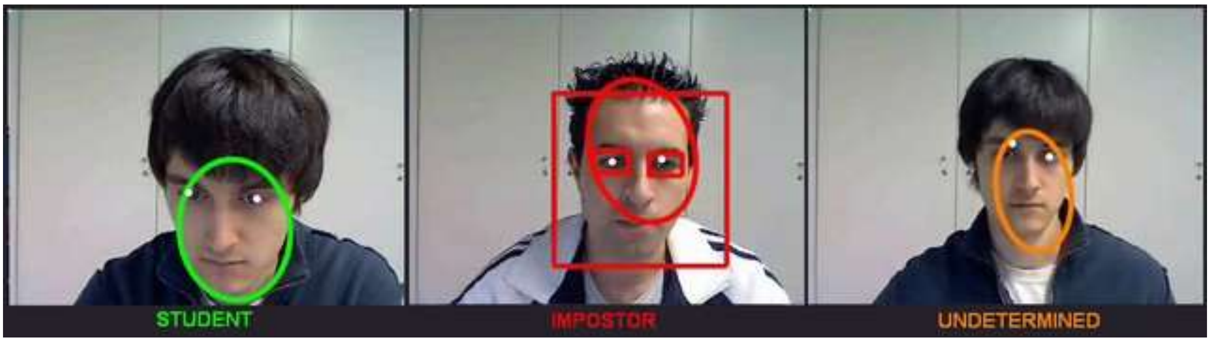


Figure 2-9. Real-time visual output provided by the face-tracking module (Tomasi & Kanade, 1992).

The colors of the squares and ellipses describe the authentication state of the detected face. Green stands for the logged student, red stands for an impostor and orange stands for undetermined (Agulla, Rúa, Alba-Castro & Jiménez, 2009).

By using the Kanade-Lucas-Tomasi (KLT) algorithm, some crucial tasks such as the control of the attendance of students, evaluation of students as well as other tracking activities can be performed more precisely and accurately.

2.5 User Authentication using Keystroke Biometric Recognition

Keystroke dynamics is a behavioral biometric technique, which does not require any additional hardware for the collection of the information similar to the mouse movement subsystem. To obtain the keystroke dynamics pattern, the person's signature is calculated and considered as the intervals between the pressing of the keys. This technique is based on the fact that each user has a personal and unique keystroke dynamics signature. The following factors are some of the keystroke dynamic characteristics: the total speed of typing, the time at which the key is held in the pressing mode as well as the intervals of pressing the key pressing etc. Sometimes, the recording of more than one pattern for each student is important. This is due to the fact that the patterns is a function of the students' emotional and physical characteristics, the keyboard's layouts as well as the work environments.

The analysis of the keystroke dynamics can be achieved using any of the following techniques:

- Neural networks.
- Fuzzy logic techniques
- Statistical methods and

The two main features that can be considered as the result of students' actions are:

- Key code: the ASCII code of each of the pressed key.
- The pause duration between actions: This gives an indication of the time interval between the pressings of two keys. This time interval is referred to as digraph. This factor is a function of the keyboard's layout and the hardware that is employed for the data collection (Sogukpinar & Yalçin 2004). Hence, the main goal of this strategy is

to select an architecture model, which contains both the software features and the environmental factors capable of influencing the mood of the user in order to analyze the keystroke dynamics. The results obtained will thereafter show an advantage of the model used as compared with other alternatives, which does not require high bandwidth.

Future works can consider the development of a new model for regulating the students' activities during an e-test in order to minimize mismanagement and to improve the performance of the systems. In order to reach this target, data relating to the physical and behavioural pattern as well as the mental state of the student's should be acquired, monitored and processed.

2.6 Computer Based Assessment using Multimodal Biometrics

The use of various biometric features for identifying a computer user is referred to multimodal biometrics. This biometric feature involves the essential procedure that is necessary to integrate various preferred biometric feature into the verification technique. The use of various biometric techniques has significantly improved the consistency of the process of verification of the computer user. One of the advantages of multimodal biometric technique is that; it assist in realizing a rise in routine that could not be likely with the use of a unimodal biometric indicator (Souheil, 2007). It may be very challenging for an imitator to simultaneously imitate the numerous character behaviours of a genuine user as a result of the appearance of various systems of biometric (Jain *et al.*, 2004).

During the course of the years, in order to bring solutions to the issues of theft and imitation during computer assessments, a number of scholars had carried out researches on various biometric recognition system as a result of several boundaries faced in their research process that they assumed more than a single biometric system can resolve (Ross, Prabhakar & Jain, 2004).

Considering the above, various approaches of multimodal techniques using diverse method of procedures have been recommended in the literature review, inclusive of the use of palm patterns together with user name in addition to password in the research of Al-Saleem & Ullah (2014). In their experimental results, it was indicated that their methods can be used for continuous authentication and that the technique could be used for authentication when the computer registers. It was inferred in the conclusion that using a unimodal biometric is liable to fraud and theft (Apampa *et al.*, 2010).

In the work of Ullah *et al.* (2012) they introduced the practice of test queries by recommending a innovative technique which is referred to as the Profile Based Authentication Framework (PBAF). The test queries were prepared to authenticate computer users that take part in computer assessment. In their outcomes, they detected that making use of the test queries can be controlled without difficulty and additional hardware is not required. Nevertheless, it was resolved that the technique employed is predisposed to imitation risk for the reason that it was well thought-out not to be difficult to share.

Using mouse movement and finger print in identifying the verification of computer users during computer assessment, Chellappan *et al.* (2015) in their study proposed an authentication method which was used to withstand quite a lot of computer assessment practices. The results obtained establishes that the use of fingerprint might be used to identify persons in addition to their distinctive behaviour and might also be used for continuous authentication of a computer user. The final outcome nevertheless indicates that separate condition was required for well-organized unceasing authentication. Also, a fingerprint supported scanner device would be a vital requirement. The authors posited that the devise could become an issue to this mode of verification due to the fact that it is expensive, more so, the fingerprint feature could also be predisposed to theft.

2.7 Chapter Summary

This chapter focuses on e-assessment, its background as well as the challenges facing e-assessments. Furthermore, it explains how knowledge based authentication, possession based authentication and biometric based authentication are methods of authentication in e-assessments. It also focuses on physiological mechanism and behavioural mechanism as the types of biometric technologies. It explains how the implementation of multimodal biometrics could be used to curb impersonation and fraud because a unimodal biometric when used for computer assessment might be predisposed to risk and imitation.

CHAPTER THREE: METHODOLOGY

3 INTRODUCTION

This section defines the bimodal authentication method for computer based assessments. The main objective of developing bimodal biometric technique is to provide user's authentication for computer based assessments. However, for this objective to be accomplished, an effective and efficient development of the bimodal biometric system must be successfully carried out.

The bimodal biometric technique for authentication of computer based assessment that would be developed is capable of authenticating an individual by matching the query image with the database and detects their similarities. The implementation of the system was carried out via MATLAB programming language. This programming language was selected owing to the fact that it is competent in preforming adequate analysis and simulation in image processing. The main reason why the bimodal biometric technique (face and keystroke biometric recognition) are used in the computer based assessment was because the use of a single biometric technique is liable to theft, impersonation and insecurity (Zviran & Erlich, 2006). By combining both biometrics with the aid of the proposed system, some important tasks such as the control of the attendance of student, evaluation of student and tracking activities can be performed more accurately and precisely.

In this chapter, the modules of bimodal biometric authentication techniques were considered so as to build an operational bimodal authentication system for computer based assessments.

In a bid to combat these security problems, keystroke dynamic technique and facial biometric recognition were introduced into the computer based assessment biometric system so as to enhance the authentication ability of the computer based assessment system. The keystroke dynamic technique was measured using latency and pressure while the facial biometrics was measured using principal component analysis (PCA). A secondary data source was employed for the collection of data relating to facial biometrics from a public database (Faces96, nd). The description of the database is explained further in section 3.7.

The system model was simulated on computer based assessments and also benchmarked with the public available datasets (keystroke100 benchmark dataset and Faces96 database, nd).

3.1 Proposed Bimodal Biometrics Model

The system technique indicated for a bimodal biometrics authentication system is divided into two phases: -

- Keystrokes authentication by latency and pressure using moving average.
- Face recognition using fast Principal Components Analysis (PCA).

Figure 3-1 presents the bimodal biometrics model for face and keystroke biometric authentication.

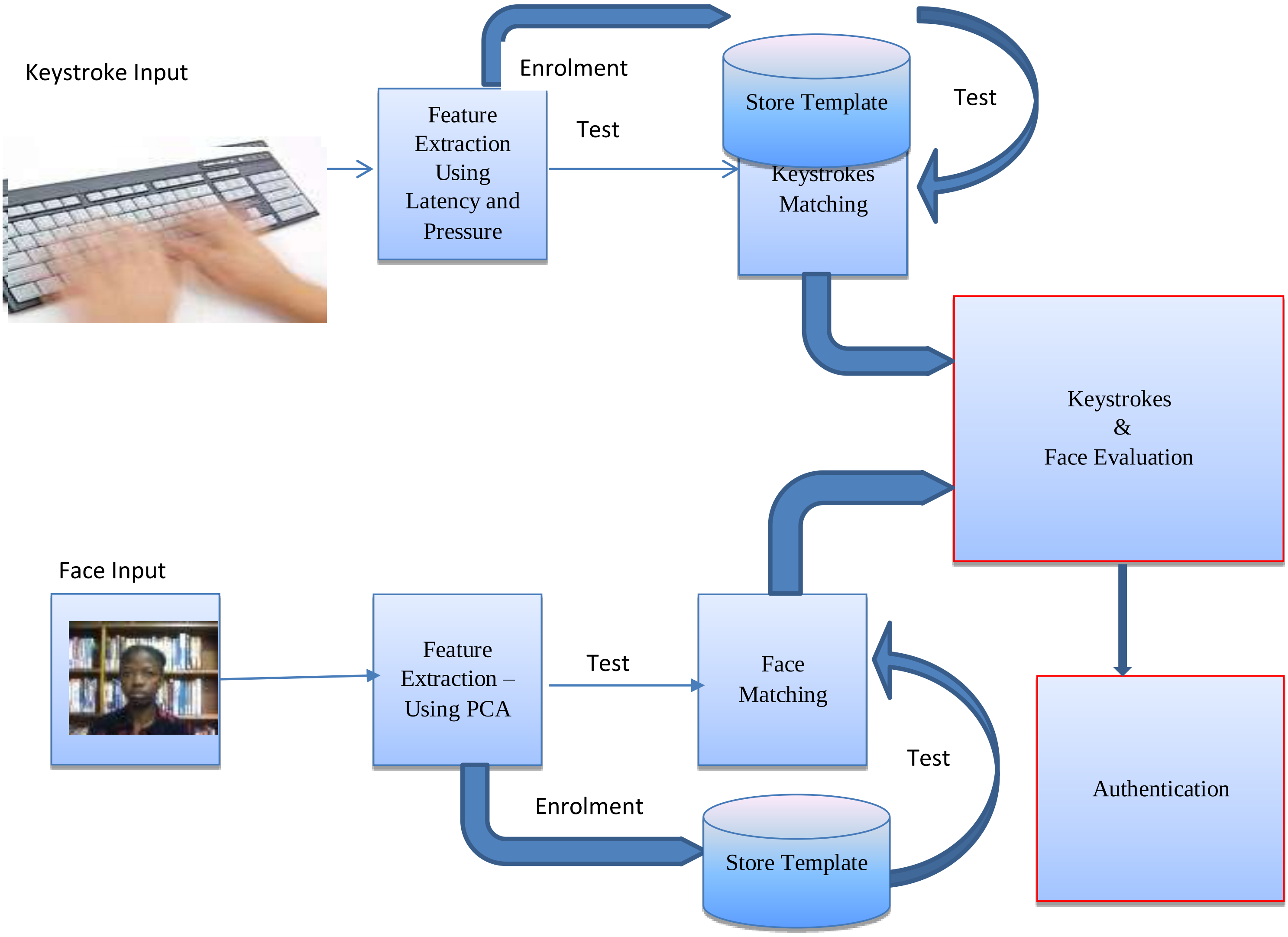


Figure 3-1: Bimodal biometrics model for face and keystroke biometric authentication (Ghosh & Dutta, 2012)

3.2 Keystroke Authentication

The publicly available database used for the keystroke images is the keystroke100 benchmark dataset, the description of the database is explained further in section 3.7. The development phase of the keystroke authentication system, are characterized by very important steps which are critical to the overall success of the system. Figure 3-2 shows the block diagram of keystroke authentication process clearly shows the phases that were used in implementing the system and these are explained in section 3.2.1-3.2.3 respectively.

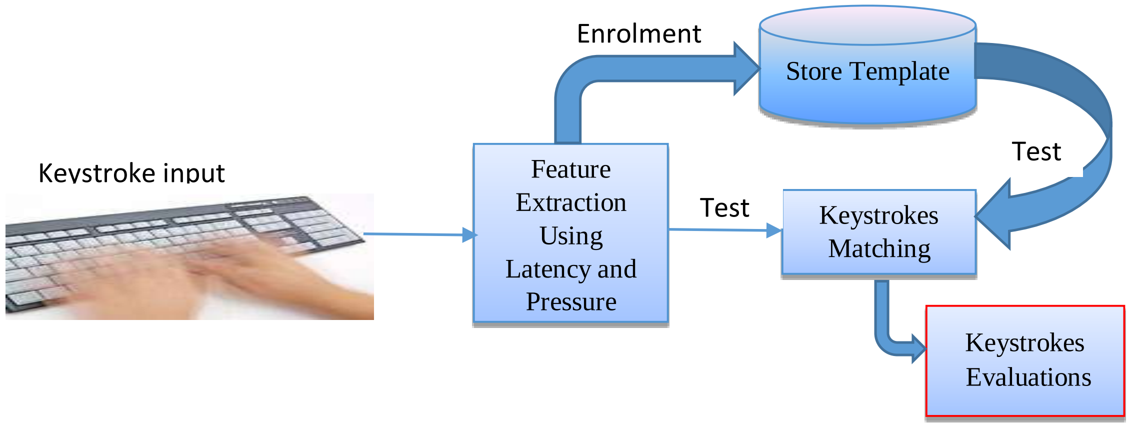


Figure 3-2: Keystroke authentication using latency and pressure (Ghosh & Dutta, 2012)

As indicated in Fig. 3-2, the keystroke authentication phase is divided into two modules, namely:

- Enrolment phase
- Authentication phase

3.2.1 Enrolment phase

During the enrolment phase as shown in Fig. 3-1, the user's biometric data was acquired, processed and stored as reference file in a database. This is treated as a template for future use by the system in subsequent authentication operations. The enrolment module was sub-divided into the following phases:

3.2.1.1 Image acquisition phase

In order to perform the keystroke assessment and capture the typing pressure patterns, a normal keyboard was improved upon into a keyboard that is sensitive keyboard pressure by observing pressure resistive force sensors beneath the matrix of the keyboard. A pressure sensor is equivalent to a flexible resistor in which its resistance changes in line with the amount of force exerted on its sensing surface.

3.2.1.2 Feature extraction

Feature extraction process is a process whereby unique data are mined from the sample to create a template. It is expected that the templates for any two individuals should be different while the different samples for the same person should be identical. As shown in Figure 3-1, the process feature extraction is one of the vital processes in the proposed system. During the process of feature extraction, the biometric data is converted to feature vector, which can be used for classification.

There are several different characteristics of the keystroke dynamics, which can be used when the user presses the keyboard keys. Some of these possible features are as follows:

- Overall speed of typing.
- Duration of the keystroke hold-time.
- The latency between consecutive keystrokes.
- The frequency of errors (This is signified by how often the user uses the backspace).
- The force used when hitting keys while typing (requires a special keyboard).
- The habit of using additional keys in the keyboard. For instance, when writing numbers with the num-pad.
- The order that user press keys when writing capital letters, (is shift or the letter key released first).

The proposed system features the combination of the characteristics of the maximum pressure and latency as the main feature since the combination of both characteristics is considered to be a highly effective feature which can be employed in the keystroke-based authentication system. Data acquisition and processing would also be carried out using the moving average, which would be explicitly indicated and explained, in subsequent sections.

3.2.1.2.1 Feature extraction using keystroke latency

The time between a key was released and the next key was pressed is referred to as keystroke latency. The latency of a single character indicates the time interval between the times from which the key being released to the next key being pressed. On the other hand, latency is the time between keystrokes, is expressed as the difference between the first key's key-up time from the next key's key-down time (see Equation 3-1). The latency can be negative while the duration is always positive. Furthermore, the time between the two key-downs can be obtain by finding the sum of the duration for the first key with latency between the keys and time between key-up of one key and key-up of the next with the duration of the second key added to latency between the keys.

$$latency = T_{i+1}^{d} - T_{i}^{u} \qquad (3\text{-}1)$$

Where T_i^u is the key-up time (min), T_i^d is the key-down time (min), T_i is the first key and T_{i+1} is the next key (min)

3.2.1.2.2 Feature extraction using keystroke pressure

The amount of force exerted on each key pressed is referred to as keystroke pressure.

In order to perform the keystroke assessment and capture the typing pressure patterns, a normal keyboard was improved upon into a keyboard that is sensitive keyboard pressure by observing pressure resistive force sensors beneath the matrix of the keyboard. A pressure sensor is equivalent to a flexible resistor in which its resistance changes in in line with the amount of force exerted on its sensing surface. The conversion of resistance into discrete voltage signals ranging from 0 to 10 volts was achieved with the aid of a force to- voltage circuit. Next, is the acquisition of the voltage signals into the processing unit using a data acquisition card for further analysis such as pre-processing and extraction of features.

3.2.2 Authentication/verification phase

During the authentication/verification phase, the user's biometric data was acquired, and processed. The authentication decision shall be based on the outcome of a matching process of the newly presented biometric to the pre-stored reference templates.

3.2.3 Analysis of the proposed latency and pressure using moving average

The moving average is referred to as a mathematical system which is used mainly to remove anomaly and reveal the real development in a collection of data points (equation 3-2).

$$yM[n]=\frac{1}{M}\left(\sum_{k=0}^{M-1}[n-k]\right) \quad (3\text{-}2)$$

In order to make average for (M) number of points and represent them with one point, the algorithm was written for convenience and an interpolation algorithm was applied. The interpolation was completed in order to get the average between each two consecutive data points. The scope was to diminish the data points without altering or losing any important information in the signal. Simple test on the algorithm have shown that this can improve patterns. The experimental representation of the moving averages is further described in section 4.2.

3.2.4 Distance metrics used in the keystroke authentication experiment

The following are the distance metrics used in the keystroke authentication experiment:

- Euclidean distance metric
- Diagraph

3.2.4.1 Euclidean distance metric

The Euclidean distance metric was universally used and very common, and it happens to be used in measuring authentication in keystroke analysis.

The Euclidean distance metric can be calculated from equation 3-3.

$$D(X,Y) = \sqrt{\sum_{i=1}^{n}(X_i - Y_i)^2} \qquad (3\text{-}3)$$

X is the authentication vector; Y is the stored reference vector.

3.2.4.2 Diagraph

This is a very dynamic part of the keystroke biometric recognition. It can often be defined as the time between keystrokes. In order to match the data of the keystroke gotten with the templates already captured in a database, the correlation equation is used (equation 3-4). The correlation coefficient r can be calculated thus (Flior & Kowalski, 2010).

$$r = \frac{\sum_{i=1}^{n}(k_i * t_i)}{\sqrt{\sum_{i=1}^{n}(k_t^2) * \sum_{i=1}^{n}(t_t^2)}} \qquad (3\text{-}4)$$

Where:

k is the vector of length n which stores the flight time of the stored template, t is the vector of length n which stores the flight time between keystrokes of a biometric sample.

ALGORITHM 1: FEATURE EXTRACTION ALGORITHM IN KEYSTROKE AUTHENTICATION

INPUT: A stream g(t), top diagraphs d_n, cluster centroids $\mathbf{m}_f\ (k)$

OUTPUT: A feature set **F**

```
Locate keystrokes t = $[t_1,.....ti]$ at times of high energy using FFT,
for each $keystroke\ time\ t_i$ do
                $f_i =$ MFCC(g($t_i,....,t_i + L$))
$l_i = \arg\min_k \|m_f(k) - f_i\|_{2,}$
for each $diagraph\ d_n$ do
```

```
$\mathrm{T}=\{t_i - t_{i-1} : l_i = kn_2 \, \& \, l_{1-i} = kn_{1,} \, \forall_i \in [2,|t|]\}$,
$m_n = mean(\mathrm{T})$,
$\sigma_n = std(\mathrm{T})$,
Compute histogram of digraphs $h_n$
for each letter $k$ do
Compute $\overline{f_k}$
return F = $\{m_n, \sigma_n, h_n, \overline{f_k}\}$.
```

ALGORITHM 2: AUTHENTICATION ALGORITHM IN KEYSTROKE AUTHENTICATION

INPUT: A probe streaming $g'(t)$, biometric template $\mathbf{F}$,

top digraphs d_n, cluster centroids $m_f(k)$,

score distribution m_{sv}, σ_{sv}, threshold τ.

OUTPUT: An authentication decision d,

```
Compute feature set $\mathbf{F}'$ for probe $g'(t)$ via Alg. 1,
Compute digraph statistic score $S_1$,
Compute histogram of digraphs score $S_2$,
Compute intra-letter distance score $S_3$,
Compute normalized score $S$,
if $S > \tau$ then
    return $d =$ genuine.
else
    return $d =$ impostor
```

3.3 Face Recognition

The publicly available database used for the facial biometrics are Faces96 (Faces96, nd). The description of the database is explained further in section 3.7. In order to obtain the biometric feature of the face, the Kanade-Lucas-Tomasi (KLT) approach is used. The images captured using the web camera are represented as vectors and the mean examined is given by equation 3-4.

$$\mu = \sum_{n=1}^{K} Y_n \qquad (3\text{-}4)$$

Where:

$Y = (y_{1,}\, y_{2.....,}\, y_{i,.......}\, y_K)$ and signifies a $k \, \mathrm{X} \, K$ data matrix

$K =$ Number of facial images being examined

Y_n = a vector with dimension k made up of an $r \times s$ image

$$k = r \times s \qquad (3\text{-}5)$$

The development of face recognition system are characterized by important phases that are central to the overall success of the system. Figure 3-3 shows the system architecture of face recognition process. The Figure clearly shows the phases that were used in carrying out the system.

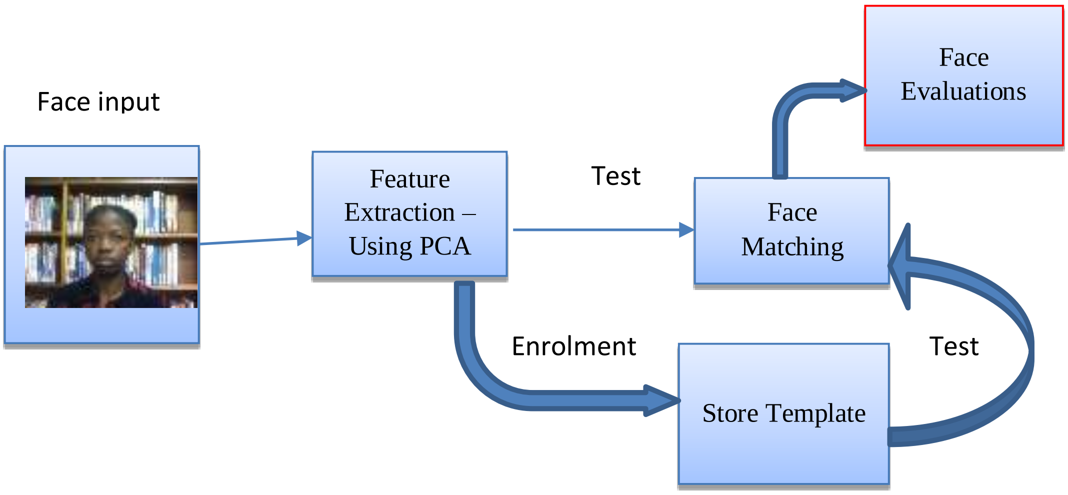
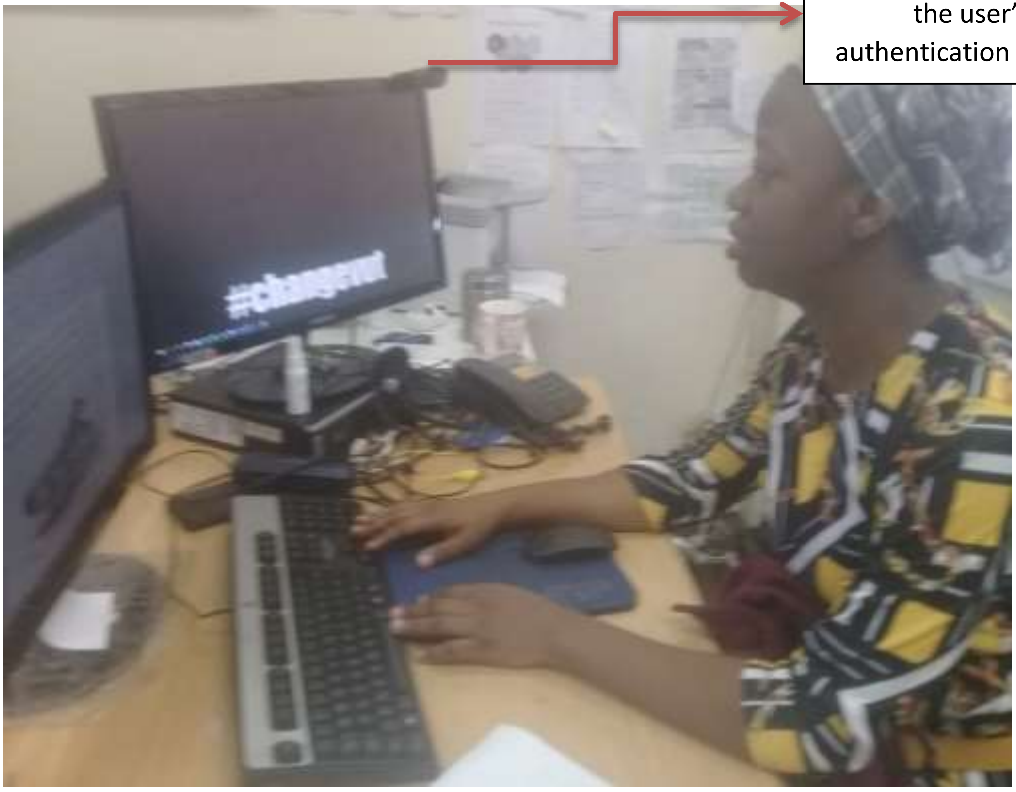


Figure 3-3: Face recognition model using Principal Component Analysis (PCA) (Ghosh & Dutta, 2012)

3.3.1 Image acquisition phase

The database used for the face images are the publicly available database (Faces96, nd) (Spacek, 2015). In order to acquire facial image(s) from diverse persons, there was a need to carry out this process from diverse angle using Logitech camcorder C920 which was used for obtaining samples for the facial biometric during e-assessment. The image of the web camera can be seen in Figure 3-4.



Attached webcam is focused on the user's face for authentication and assessment

Figure 3-4: LOGITECH camcorder used for capturing different face images.

In the course of the experiment, the camera in figure 3-4 was used for capturing and the logitech camcorder used produces resulting images that are 196 ×196 pixels in size.

With the aid of a fixed camera, a sequence of 20 images for each individual was taken. The web camera mounted to the top of the computer screen was employed for the facial biometric. During the sequence the user looks directly on the computer system, focussing on the web camera. This posture is used to introduce substantial head variations between the images of same individual. The time interval between successive frames in the sequence was observed as 0.5 seconds. Prior the computer based assessments, the scanning of the computer user was carried out and it was being harmonized with the stored image. When the scanning of the face is going on, the appearance of the face is being validated by the camera, and broadcast the indicator to the systems server wherever the facial appearance was administered for computer assessment. However, if the camera does not recognise the facial appearance, keystroke biometric recognition shall be used to ascertain the authentication of the user. If the problem persists, the image would be sent to the server.

The different division of phases, which characterizes the face recognition, are presented as follow:

- The image pre-processing phase.
- The feature extraction phase using a fast PCA.

3.3.2 Image pre-processing phase

At this stage, the images acquired are first align and the cropping operations are performed before face image is passed onto the feature extraction phase. The main purpose of pre-processing process is to enhance or improve the image, in usual cases; the enhanced image would be presented in pixels. The enhancement process was done to remove data on the image that causes distortion, for both input and output images.

3.3.3 Feature extraction using fast Principal Component Analysis

At this stage, the image of the face was passed through training and testing phases usually carried out in order to extract the facial features.

3.3.3.1. Training phase

In the training phase, the image acquired was made to pass through an image pre-processing phase such as histogram normalization so as to adjust the contrast process of the image. This is to ensure that the outputs of the image have uniform distribution of grey values and also to ensure significant reduction in the light intensity variation level in the grey.

With the aid of a fixed camera, a sequence of 20 images for each individual was taken. The web camera mounted to the top of the computer screen was employed for the facial biometric. During the operational sequence, the user is made to take a step forward towards the camera. The essence of this movement was to introduce substantial head variations between the images of same individual. The time interval between successive frames in the sequence was observed as 0.5 seconds. Prior the computer based assessments, the scanning of the computer user was carried out and it was being harmonized with the stored image. Once the scanning of the face is carried out, the camera authenticates the facial appearance, and broadcast the signal to the server where the facial appearance is treated for computer assessment. However, if the camera does not recognise the facial appearance, keystroke biometric recognition shall be used to ascertain the authentication of the user. If the problem persists, the image happens to be sent to the server.

. **ALGORITHM 3:** TRAINING PHASE IN FACE RECOGNITION USING PCA

INPUT: Face image F

OUTPUT: Trained face

```
STEP 1: input face image $F$
STEP 2: for each $x_1$ , calculate its estimate $\{u_1\}_1^f = 1 \in R^Z$ for image
        vector dimension $d$
STEP 3: calculate the weight $w$ from each vector
STEP 4: calculate the mean vector $v$
STEP 5: subtract each $x_1$ by $v$ to get $\varphi_1$
STEP 6: compute the variance matrix $\sum$ of all $\varphi_1$ ($Z - by - Z$) matrix
STEP 7: compute set of $\sum(Z - by - F - 1)$ matrix
STEP 8: Preserve the $V$ largest Eigen vector based on the Eigen value
STEP 9: $U\ \varphi_1$ is Eigen face representation
```

From the above, the algorithm V is vector dimensional representation while V projection is the Eigen face which has a basis ($V << Z$). The Z-dimensional vector was employed for the measurement reduction. For the period of the training phase, the same process is followed before matching the image vector acquired with the database images in order to ascertain their equivalent matches.

3.3.3.2. Testing Phase

In the course of this phase, the feature of image to be identified was made to pass through the testing phase by ensuring the image was again passed through the phases of image pre-processing and features extraction of features, just like the training phase.

In addition, the images of the extracted features are converted to an image vector and the image is then proposed to the Eigen space. The Euclidean distance between the image tested and all the proposed trained images are likely to find the equivalent one which is close and this was thereafter used for the recognition purpose.

ALGORITHM 4: TESTING PHASE IN FACE RECOGNITION USING PCA

```
TEST FACE IMAGE
        INPUT:  T = $\varphi_1 \times \gamma, \mu = \tau^T \times v$, $\gamma =$ eigenvector, $E_1$ = normalised image,
                Euclidean distance, $E_2$, T = proposed eigenfaces
                $\mu =$ space vector
        OUTPUT: Test face image
STEP 1: input trained image
STEP 2: reshape and centred image v=reshaped-mean
STEP 3: centre project test vector into face space $\mu = T^{\tau} * V$
STEP 4: Comput square norm of $E_1, E_1 = [norm(\eta - \mu)]^2$
STEP 5: Project $\mu$ to another space by multiplying it by $T, \varsigma = \mu$ X $T$
STEP 6: Compute Euclidean distance, $E_2$ between v and ς
            $$E_2 = V - \varsigma = \sqrt{V^2} + \varsigma^2 - 2*V\varsigma$$
STEP 7: Normalize $E_1$ and $E_2$ for classification
            $$\frac{E_1}{T}, \frac{E_2}{T}$$
STEP 8: Compare $E_1$ to $E_2$
STEP 9:  If $E_1 > E_2$
STEP 10:  Image is face
STEP 11:  Otherwise
STEP 12:  Non face
```

Using algorithm 2, the feature of the face image was made to pass through the phases of image pre-processing and the features are extracted for a second time. The extracted features of the images are therefore characterized in a vector form. The vector acquired in the course of the testing phase was classified. This is necessary to determine if the normalized feature of face image E_1 was greater than Euclidean distance E_2 feature of the image accepted as face and if otherwise, it was accepted as non-face.

3.4 Matching Phase

The face and keystroke biometric model for computer based assessment was simulated in the MATLAB 8.1.0.604 (R2016) environment. MATLAB functions were written and run to carry out the biometric based bimodal assessment authentication model. MATLAB is a branded product of Math Works incorporation. It is a high-performance language, which can be used for methodological computing. It incorporates programming, computations and visualization in a stress-free background where problems and solutions are articulated in acquainted mathematical symbolization and terms.

In the matching phase, biometric matching was carried out. The information from both biometric modes are joined and sent to the decision module and then the validation module where the user would be authenticated.

3.5 Bimodal Authentication Decision

In order to develop a bimodal authentication system, the authentication decision should not be left out. To improve effectiveness, the facial biometric was used as the first authentication mode of to acquire a set of possible models, which have met the threshold. From the list, the keystroke biometric can then be employed to scrutinise the lesser subset of expected users identities. Fusion was carried out at the matching module. More precisely, serial mode would be used to realize fusion of the two biometric approaches. The keystroke biometric was acquired through a keyboard while the facial biometric was obtained with the use of a web camera mounted to the top of the computer screen. The process involves the feeding of the biometric data into the feature extraction module and subsequent passing it onto the matching module where the biometric data was matched with the templates in the biometric database containing the captured templates for both the facial and keystroke biometric. The comparison scores are generated for the keystroke biometric mode, which was passed onto the facial matching module. The keystroke biometric was given the preference of gaining an initial set of possible identities, which meets the threshold due to the fact that it is more accurate when compared with the facial biometric. The outcomes of possible identities signify a declined list of users, which the facial biometric can match its biometric data against. This can be said to be the bimodal authentication decision for this study.

3.6 Data Collection (Biometrics Database Sources)

The publicly available database for keystrokes biometrics used for this research work is the keystroke 100-benchmark dataset, which can be a dataset for research on pressure-sensitive keystrokes and typing dynamics. This dataset is a compilation of keystroke/typing patterns of 100 users typing the password "**try4-mbs".** In order to achieve this research work, a program was developed to gather the keystroke latency and pressure from a whole of 100 computer users. Prior to the authentic data collection session, the participants were obliged to acquaint themselves with the passwords "**try4-mbs**". The uniformity of password among all participants was to ensure comparative analysis of the typing patterns of the same password from diverse individuals. From each participant, a total of ten timing samples and ten pressure samples were gotten. Furthermore, there exist two files in the folder of each participants (latency.txt and pressure.txt). Each row of the matrix in latency.txt matches to a sample whilst each column matches to latency (time gap between two keystrokes). The latency data samples of the keystroke were captured at a precision of milliseconds (ms). Each column in the pressure .txt corresponds to a sample, i.e. a time-series of pressure (measured in volt) exerted on a key.

The database for the facial biometrics which was used was the publicly available database used for this research work is the Faces96 (Faces96, nd). The images are mainly of first year undergraduate students, so the majority of individuals are between 18-20 years old but some older individuals were also present. The Faces96 database was provided in order to encourage comparative research. Table 3-1 indicates the features and users of the Faces96 database for facial recognition and their settings.

Table 3-1: Features and users of the Faces96 database for facial recognition and their settings.

Total number of users	Number of images per users	Total number of images	Gender	Race	Age range	Glasses	Beards	Image format	Camera used	Lighting
395	20	7900	Both male and female	Various racial origins	18 to 20+	Yes	Yes	24bit colour JPEG	LOGITECH camcorder	artificial, mixture of tungsten and fluorescent overhead
Source: (http://cswww.essex.ac.uk/mv/allfaces/)										

3.7 Chapter Summary

In this chapter the system model for the bimodal biometrics was explained, algorithms for feature extraction and authentication in keystroke biometrics were reviewed, likewise, the algorithms for training and testing phase in face recognition using PCA was also reviewed. The publicly available database that was used for the study for both facial and keystroke biometrics was extensively discussed. The performance evaluation was carried out using the accuracy, FAR and FRR respectively.

This bimodal biometrics can be used to continuously authenticate a user in a computer based assessment. In the event that the camera is unable to capture the face of the user, then keystroke can be used to authenticate the user. If the user is not typing, then face biometric can be used for the authentication.

The next chapter would reveal the experimentation and main results of the study of the computer assessment system.

CHAPTER FOUR: EXPERIMENTATION AND RESULTS

4 INTRODUCTION

This chapter describes the experiments that were conducted during the implementation of the bimodal biometric, which is to test the authentication system of a user in bimodal biometrics for computer based assessments. Experimental performance was carried out quantitatively using MATLAB for simulation and Excel application package for data analysis. System performance was measured using the following evaluation schemes: False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) and Accuracy (AC), for a comparison between the biometric computer based assessment system with and without the keystroke and face recognition alongside other biometric computer based assessment techniques proposed in the literature.

The bimodal biometric authentication was validated experimentally, the results obtained are presented in subsequent sections of this chapter. The results obtained from the individual biometric models are presented and discussed along with the results gotten from combination of the two biometric models for the bimodal biometric authentication. The ultimate purposes of the experiments were to:

- Measure the effectiveness of authentication system using bimodal biometric system.
- Estimating the clarity of latency and pressure in keystroke biometric recognition using moving average.
- Integrating bimodal biometric system into computer based assessment.

With the aid of a fixed camera, a sequence of 20 images for each individual was taken. The web camera mounted to the top of the computer screen was employed for the facial biometric.

During the sequence the user looks directly on the computer system, focussing on the camera. This posture is used to introduce significant head variations between images of same individual. There is about 0.5 seconds between successive frames in the sequence. Prior the computer based assessments, the scanning of the computer user was carried out and it was being harmonized with the stored image.

When scanning the face, the camera authenticates the facial appearance, and broadcast the signal to the server where the facial appearance was processed for computer assessment. However, if the camera does not recognise the facial appearance, keystroke biometric recognition can be used to ascertain the authentication of the user. If the problem persists, the image would be sent to the server.

Prior to the authentic data collection session, the participants were obliged to acquaint themselves with the password "**try4-mbs"** during the keystroke biometric recognition experiment. The uniformity of password among all participants was to ensure comparative analysis of the typing patterns of the same password from diverse individuals. From each participant, a total of ten timing samples and ten pressure samples were gotten. Furthermore, there exist two files in the folder of each participants (latency.txt and pressure.txt). Each row of the matrix in latency.txt matches to a sample whilst each column matches to latency (time gap between two keystrokes). The latency data samples of the keystroke were captured at a precision of milliseconds (ms). Each column in the pressure .txt corresponds to a sample, i.e. a time-series of pressure (measured in volt) exerted on a key.

One of the objectives of this research was to apply the theoretical concept from the developed approach in practice by highlighting the applications and performing practical works on the keystroke biometric recognition as well as face recognition using MATLAB.

4.1 Experiment1: Performance of Fast PCA on face Image

In this experiment, the study seek to determine the performance of the fast PCA on query face images. Figure 4-1(a) depicts a query face image while Figure 4-1(b) shows the image that was retrieved. This showed the manner through which the system was able to produce the authenticated image of the query face images.

(a) Query face image (b) Output of face image

Figure 4-1: Facial image with query and trained using fast PCA technique

From the result of the experiment, Figure 4-2 shows the resulting ROC curve with the AUC for the facial biometric found to be 0.9258 (92.58%) which denotes the accuracy of the facial biometric authentication process. The ROC curve in Figure 4-2 shows that an average of 92.58% accuracy was obtained for the facial biometric when matching facial biometric samples against the templates in the database.

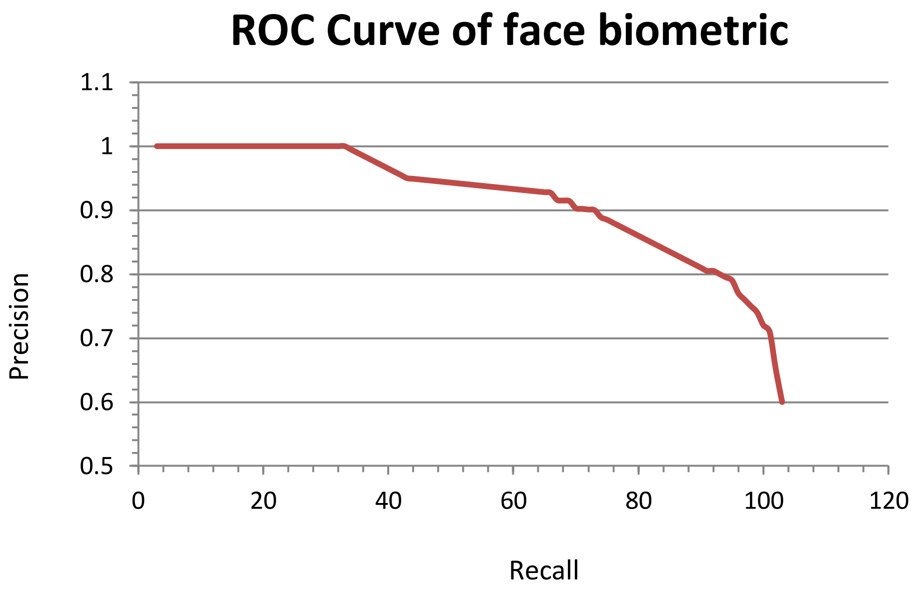


Figure 4-2: ROC curve of facial biometrics with AUC of 0.9258

Table 4-1: Results of face biometric model showing average FAR, FRR and percentage accuracy

S/N	Biometric Model	Average FAR	Average FRR	Accuracy
1	Face	6.927	7.91	92.58

The table in Table 4-1 above indicate that at least 92% of accuracy was maintained throughout the authentication process using face biometrics in computer based assessment. This implies that the face biometrics in computer based assessment ensures the continuous monitoring of an individual during the examination.

4.2 Experiment 2: Performance of Moving Averages on Keystrokes Biometrics

In this experiment, the study endeavour to compare performance of the system by using moving averages. Figure 4-3 shows the graphical performance and interpolation of training and testing data on keystroke latency after applying the moving averages. From the graph, it was observed that there is similarity between the testing data and the training data. Likewise, the graph showing the moving averages (for both 5 moving averages and 10 moving averages) indicate that the training data and testing data for both moving averages began at the same level. Based on the above scenario, the user was likely to be an authentic computer user and not an impostor.

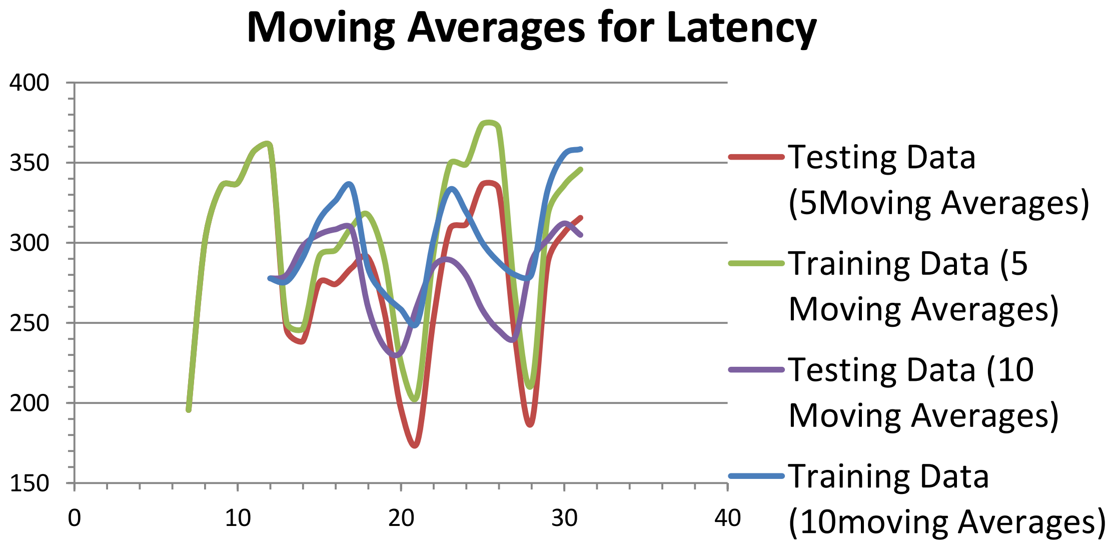


Figure 4-3 shows the interpolation of training and testing data on keystroke latency after applying the moving averages

In the keystroke experiment as shown in Fig. 4-3 above; it can be seen that the user was following a distinct stroking rhythm by applying the moving averages. A general pattern is easily recognizable from the graph. This proves that the user may not likely be an impostor but a genuine user.

In Figure 4-4 shown below, the graphical performance and interpolation of training and testing data on keystroke pressure after applying the moving averages. From the graph, it can be observed that there happens to be similarity between the testing data and the training data. Likewise, the graph showing the moving averages (for both 5 moving averages and 10 moving averages) also show similarities between them. Based on the above scenario, the user may likely to be an authentic computer user and not an impostor.

Better results from keystroke latency as compared with keystroke pressure are obtained. However, the best results are achieved by combining both keystroke pressure and latency as a single profile. From the graph in Figure 4-4 below, it is evident that the training data and testing data for 5 moving averages and 10 moving averages began at the same level.

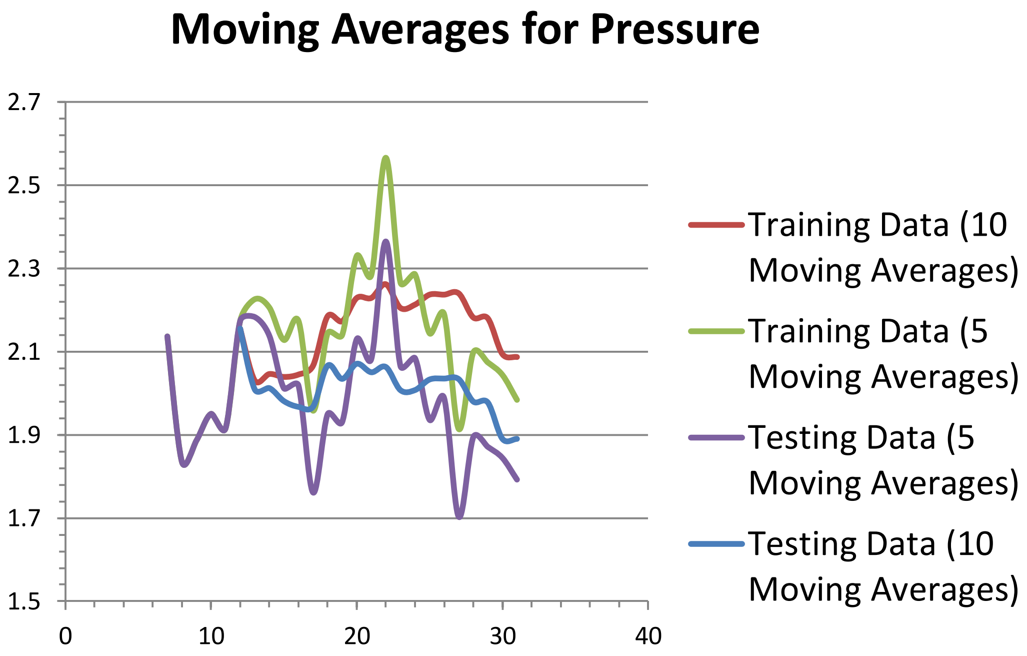


Figure 4-4 shows the interpolation of training and testing data on keystroke pressure after applying the moving averages

In Fig. 4-4 above, it is clear that there was a lot of similarity between the keystroke patterns, hence, the system was able to satisfactorily authenticate the originality of the user.

In Figure 4-5 below, the experiment shows the resulting ROC curve with the AUC for the keystroke biometric found to be 0.92025 (92.025%) which denotes the accuracy of the keystroke biometric authentication process. The ROC in Figure 4-5 shows that an average of 92.025% accuracy was obtained for the keystroke biometric when matching keystroke biometric samples against the templates in the database.

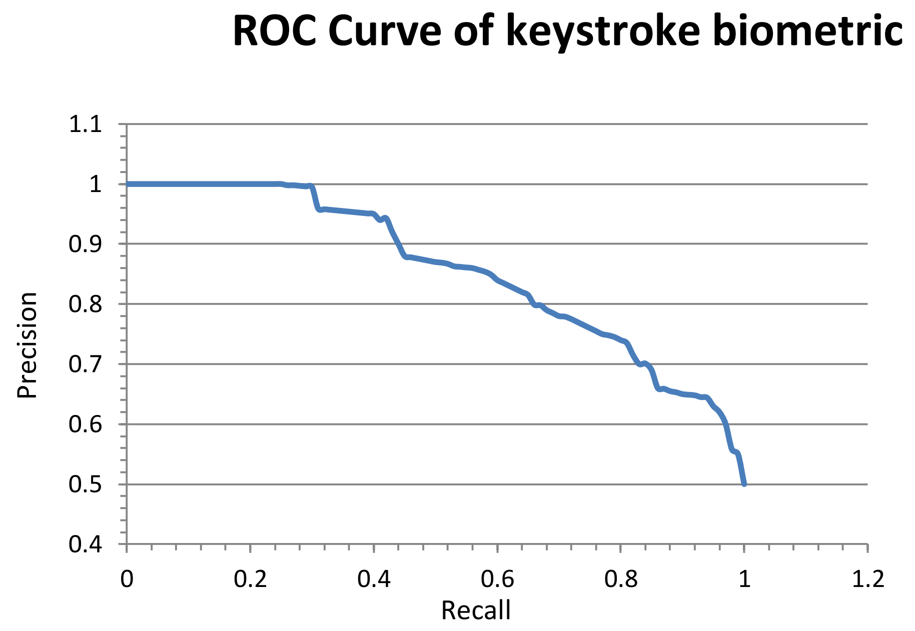


Figure 4-5: ROC curve of keystroke biometrics with AUC of 0.92025

Table 4-2: Results of keystroke biometric model showing average FAR, FRR and percentage accuracy

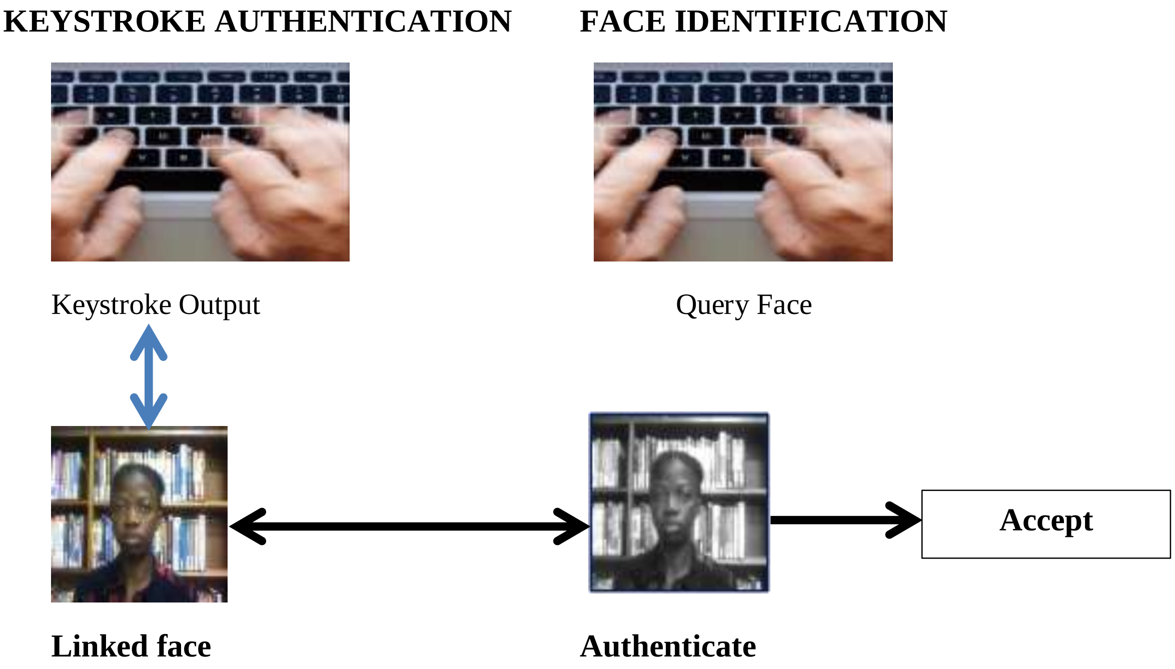
S/N	Biometric Model	False Acceptance Rate (Average)	False Rejection Rate (Average)	Percentage Accuracy (%)
1	Keystroke Biometric	7.12	8.13	92.025

The table in Table 4-2 above indicate that at least 92% of accuracy was maintained throughout the authentication process using keystroke authentication in computer based assessment. This implies that the keystroke biometrics in computer based assessment ensures the continuous monitoring of an individual during the examination.

4.3 Experiment 3: Performance of Bimodal Biometrics System

4.3.1 Authorized user attempt

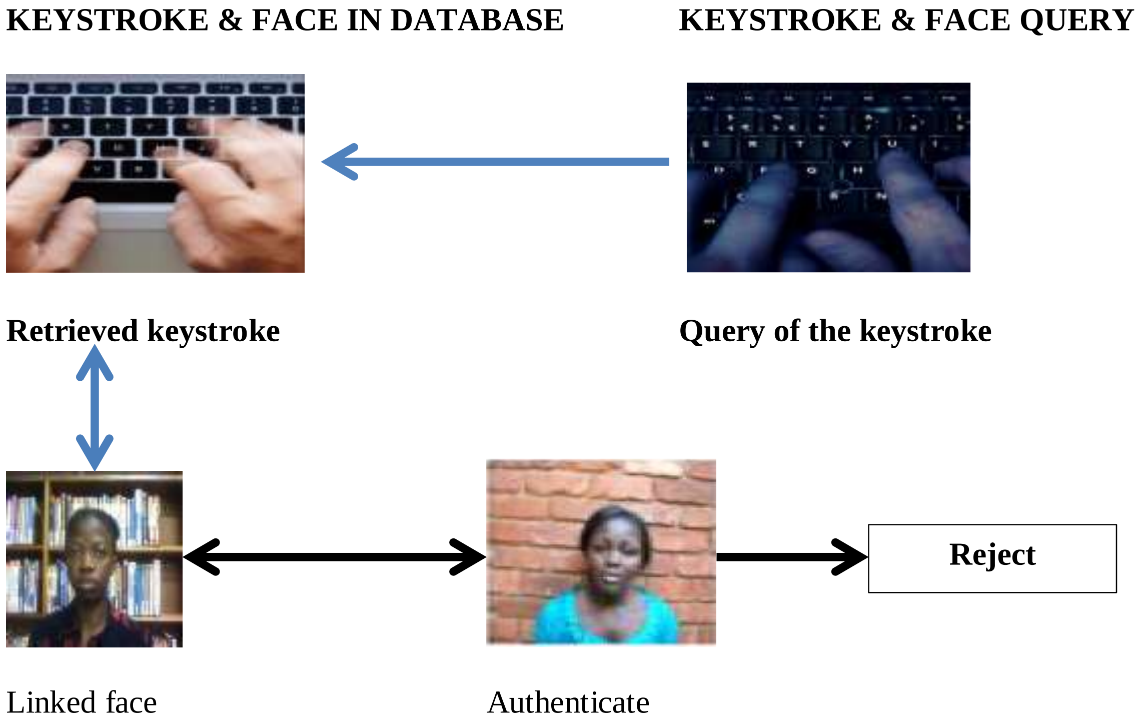
Figure 4-6 (a) and (b) show the combined face with keystroke image for authorized user as well as the combined face with keystroke image accessed by unauthorized user.



(a)

Figure 4-6 (a): Combined face with keystroke image for authorized user

4.3.2 Impostor attempt



(b)

Figure 4-6(b): Combined face with keystroke image accessed by unauthorized user

In Figure 4-7 below, the experiments shows the resulting ROC curve for both facial and keystroke biometrics which denotes the accuracy of both the keystroke and face biometric authentication process. The ROC in Figure 4-7 shows that the bimodal model integrating keystroke and face in computer based assessment confirms the continuous monitoring of an individual during the examination.

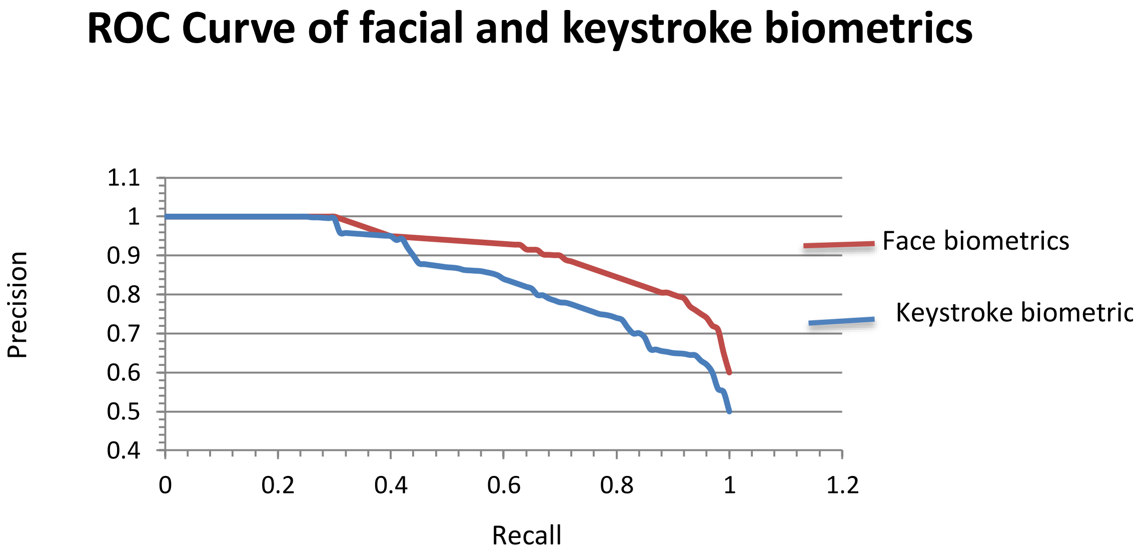


Figure 4-7: ROC curves for facial and keystroke biometrics

4.4 Performance Evaluation

The system's performance and evaluation was done via the accuracy metric as proven in equation (4-1) - (4-3):

$$AC = \left(100 - \frac{(FAR(\%) + FRR(\%))}{2}\right) \tag{4-1}$$

$$\text{Where } FAR = \frac{\sum_{i=1} W_{ai}}{T} \times 100\% \tag{4-2}$$

$$FRR = \frac{\sum_{i=1} W_{ri}}{T} \times 100\% \tag{4-3}$$

W_a is the falsely accepted individual

W_r is the falsely rejected individual

T is overall numbers of users that participated in the experiment

During the bimodal experiment, every single facial image was mapped to the keystroke data. As a result, a total number of 100 sample members were used since the keystroke had 100 users. The starting point of the classification was reserved continuous. The bimodal system functioned in sequence as a result; a face was queried at that moment the keystroke data was also demanded via the system if the face image was considered affirmative. The keystroke and face biometric systems were meant to show positive for a precise identification. As shown in Table 4-3 below, the result for FAR, FRR and Accuracy of keystroke and face biometrics are evident.

Table 4-3: Results showing the FAR, FRR and Accuracy of keystroke and face biometrics.

S/N	Biometric Model	False Acceptance Rate (Average)	False Rejection Rate (Average)	Percentage Accuracy (%)
1	Keystroke Biometric	7.82	8.13	92.025
2	Face Biometric	6.927	7.91	92.58

The table in Table 4-3 above indicate that at least 92.58% of accuracy (Face biometric) was maintained throughout the authentication process in computer based assessment. This indicates that the bimodal model integrating keystroke and face in computer based assessment ensures the continuous monitoring of an individual during the examination.

Table 4-4 above indicate that the values for the 10 moving averages of both the mean and the standard deviation gives a lesser value compared with the values from the 5 moving averages. This implies that the 10 moving averages perform better than 5 moving averages on keystroke latency and pressure.

Table 4-4: Results showing the average mean and standard deviation of the moving averages

KEYSTROKE DATA AUTHENTICATION								
	Training Data for Latency		Testing Data for Latency		Training Data for Pressure		Testing Data for Pressure	
	5 Moving Averages	10 Moving Averages	5 Moving Averages	10 Moving Averages	5 Moving Averages	10 Moving Averages	5 Moving Averages	10 Moving Averages
Aver. Mean	301.45	301.22	280.10	278.49	2.16	2.12	1.99	1.06
Std. Dev.	53.62	31.38	53.43	26.37	0.98	0.16	0.6	0.15

4.5 Experiment Discussion

Figures 4-7 shows the bimodal curves and their AUC values. The plots show the ROC curves for the keystroke biometric individually (blue), face biometric individually (red). For each curve, the area beneath the curve was given showing the accuracy of each biometric mode when authenticating a learner. This shows the ROC: AUC value of keystroke biometrics to be (0.92025 = 92.025%) and facial biometrics alone to be (0.9258 = 92.58%). In conclusion, the graph shows that by combining the two biometric modes, namely keystroke and facial biometrics, in a bimodal system, a higher percentage of accuracy can be obtained for authentication. The results obtained agreed significantly with the findings of Tey *et al.* (2013), for a group of 84 participants who played the role of attackers with 2 eight-character passwords of different difficulty. The result indicates that the false acceptance rate (FAR) of the easy and difficult password increases from 0.24 and 0.20 respectively before Mimesis training to 0.63 and 0.42 after the Mimesis training with partial information of the victim. Furthermore, the FAR increases to 0.99 for both passwords for the 14 best attackers.

4.6 Chapter Summary

The results of the experiments are presented and discussed. From the results, the facial biometric was observed as a less accurate biometric for authentication when compared with keystroke biometric. By merging two biometric modes; the accuracy of the authentication process was improved. Furthermore, when a small dataset was obtained as a result from the keystroke biometric and it was used as input to the facial biometric, the quantity of time spent authenticating a learner drastically reduced due to the reduction in the number of templates with the facial biometrics. The results in Table 4-3 show that the best results are achieved by combining both keystroke biometric and facial biometrics as an effective model for authentication in computer based assessment. This is said to be consistent with other work from the literature (Chellappan e*t al.,* 2015) which found that bimodal biometrics was more accurate than unimodal biometrics for authentication.

CHAPTER FIVE: CONCLUSION, CONTRIBUTION AND FUTURE WORK

5 INTRODUCTION

This chapter gives the conclusion, contribution and future work of the research work. In chapter one the goal of the research was stated as follows: "The goal of this study was to conduct studies on various computer based assessment systems proposed in the literature, to propose the use of facial and keystrokes techniques for bimodal computer based assessment authentication and to measure the effectiveness of a bimodal authentication computer based assessment systems." There is a need to evaluate whether the goal was achieved or not and also evaluate the contribution of the research work and then discuss the direction for future work.

5.1 Objectives Revisited

In order to fulfil the first objective of this research work, which is to conduct studies on various computer based assessment systems proposed in the literature, the reviews of the existing literature, as well as the methodology involving the system's model development was done. The second objectives, which is to propose the use of facial and keystrokes techniques for bimodal computer based assessment authentication was also achieved. A prototype biometric system which integrates the keystroke and face biometrics suitable for the authentication of a person for computer based assessment has been developed. The system was able to overcome the limitations of both the keystroke authentication system and the face recognition systems. The proposed system works in the authentication mode. The outcome of the experimental results demonstrate that the proposed system is highly suitable for the intended purpose having perform satisfactorily under the test conditions with high degree of accuracy and precision without any security breaches. The third objectives, which is to evaluate the performance of the developed system, was achieved. This was done to measure the effectiveness of a bimodal authentication computer based assessment systems.

Following the assembly of the bimodal biometric system for authentication, the performance evaluation indicates satisfactory performance as per the design and functional requirements although with minimal challenges. The system model was simulated on computer based assessments and also benchmarked with publicly available datasets (e.g. keystroke100 benchmark dataset and Faces96 database, nd) and methods.

It would be commendable to note that keystroke biometrics and face biometric recognition both display a number of individual challenges. For instance, the way in which the keystrokes are organized depend greatly on the keyboard design, posture and device. Among the factors that regulates the typing speed and pressure of a computer user was the responsive state of the user. It was recognised that as soon as a user happens to be in an awfully bad disposition, this would lead to a decrease in typing pressure and speed when likened to a rise in the typing pressure and speed when the user is in extremely stable mood. This denotes that the way a user feel could have a foremost effect on typing. Likewise, face recognition could be very delicate to light conditions, because it produces bad outcomes as soon as the light in the environment happens to be in low state. Similarly, for a very long time, visible changes may take place. For instance, wearing spectacles, growing of beard, face distortion, etc., which can lead to inappropriate, images classification.

To solve this challenge, the hierarchal structural check algorithm was employed for matching the query face image with the ones stored in the database and this only use the available query face image for comparison with the image for authentication. The proposed technique can help the user in matching the available feature with that in database during authentication without rejection. Hence, the situational problem in chapter one was revisited. The proposed technique can help the user in matching the available feature with that in database during authentication without rejection as unauthorized user. In case of laxity, the user's face also with the keystroke was used for authentication during assessment. The goal of the research was fulfilled. The issue of keystroke recognition were addressed using moving average for latency and pressure.

5.2 Conclusion

In this research, the bimodal biometric system for authenticating a user during computer based assessment was the main area of interest.

The system employs the facial and keystroke biometrics for the authentication of learners during computer based assessment. In answering the research questions, the study was able to introduce keystroke techniques and facial biometrics recognition into the system by acquiring data template from both facial and keystroke database respectively. Furthermore, the computer based assessment biometric technique was improved upon by integrating a bimodal biometric of face and keystroke in order to authenticate a user during assessment. The evaluation method used to measure keystroke was the latency and pressure while the evaluation method used to measure face was the Principal Component Analysis (PCA).

The following conclusions were drawn following the successful completion of this research.

- The bimodal biometric authentication systems are suitable technique for improving computer based assessment.
- The bimodal biometric authentication system when applied to computer assessment such as online examination, electronic assessment etc. demonstrated the capability to improve the security level.
- The computer based assessment biometric technique can be improved upon by integrating a bimodal biometric of face and keystroke in order to authenticate a user during assessment.

- The issue of security laxities can be addressed by developing a robust bimodal biometric system using keystroke and face authentication system using keystroke latency and pressure and fast PCA approach.
- Among the factors that regulates the typing speed and pressure of a computer user was the responsive state of the user.
- The proposed technique can help the user in matching the available feature with that in database during authentication without rejection.

5.3 Contribution to Knowledge

The main contributions of this research are as follows:

- Presentation and publication of a research article in international conference.
- Comprehensive reviews of keystroke biometrics and face image enhancement techniques were done. The challenges, open issues, advantages and disadvantages were highlighted. Standard evaluations of these techniques were recommended for easy comparison.
- A bimodal biometric using keystroke latency and pressure with fast PCA was proposed and a comprehensive evaluation was done. The technique was suitable for authentication in computer assessment such as online examination. The technique allows an individual physically present during any online examination.
- The research contributed in showing the practicality of incorporating face images and keystroke biometrics for authentication in computer based assessment. This removes issues of security breaches as compared with what would have happened when the transaction is assessed with password, token or Identification Numbers (IDs).

5.4 Future Work

This study investigated the bimodal biometric authentication system for computer based assessment using keystroke latency and pressure and fast Principal Component Analysis

(PCA) approach. The result presented in this study has shown that using bimodal biometric authentication systems are suitable technique for improving computer based assessment. However, based on the findings reported in this research work, it is recommended that:

- Further work should be carried out using real people to perform the experiment.
- The use of a web camera equipped with a monitor sensor can be considered to follow a user's head movement as this would allow for continuous authentication.
- The speed of bimodal biometric system can be increased for user's conveniences.
- More studies similar to this research work should be in the direction of appraising the act of the recommended system on an immeasurably huge database so as to control the numerous parameters such as system's complexity, rate of verifying a user, cost of application, true negative rate, equal error rate, etc. which is the main brain behind a result to accept a model of authentication.

5.4 Chapter Summary

In this chapter, the conclusion of the study was reached mostly with respect to how the study indicates the combination of the keystroke and facial biometrics that could be used to authenticate computer users during computer based assessments. Future recommendations on how further work should be carried out were stated.

References

ABOALSAMH, H. A. 2009. Vein and Fingerprint Biometrics Authentication-Future Trends. *International Journal of Computer and Communications,* 3(4)**,** pages 149-155.

ADAMSKI, M. S., K. 2008. Online Signature Classification and its Verification System. *7th Computer Information Systems and Industrial Management Applications,* 5(4)**,** pages189-194.

AGARWAL, M., JAIN, N., KUMAR, M. & AGRAWAL, H. 2010. Face Recognition Using Eigen Faces and Artificial Neural Network. I*nternational Journal of Computer Theory and Engineering,* 2(4), pages 1793-8201.

AGULLA, E. G., RÚA, E. A., ALBA-CASTRO, J. L. & JIMÉNEZ, D. G. 2009. Multimodal Biometrics-Based Student Attendance Measurement in Learning Management Systems. *Conference Paper · January 2009: Source: DBLP,* 12, pages 45-51.

AL-KHAZZAR, A. S., N. 2010. Behavioural Authentication Using Computer Games. *The School of Computing and Mathematical Sciences, Liverpool John Moores Universit, PGNet Liverpool, UK,* 3(4)**,** pages 139–143.

ALL, Y. D, G-Y. & SUN, F.-X. 2006. A Model for User Authentication Based on Manner of Keystroke and Principal Component Analysis. *Proceedings of the 2006 International Conference on Machine Learning and Cybernetics***,** 5(6), pages 2788-2792.

AL-SALEEM, S. M. & ULLAH, H. 2014. Security Considerations and Recommendations in Computer Based Testing. *Science World Journal,* 11(5)**,** pages 89-95.

ALWI, N. & FAN, I. 2010. E-learning and Information System Management. *International Journal of Digital Society,,* I(2)**,** pages 148-156.

APAMPA, K. M., WOULDS, G. & ARGELS, D. 2010. User Security Issues in Summative e-Assessment security. *International Journal. Digital Society,* 1**,** pages 1-13.

ARAUJO, L. C. F., SUCUPIRA, L. H. R., LIZARRAGA, M. G. LING, L. L. & YABUUTI, J. B. T. 2004. User Authentication through Typing Biometrics Features in Biometric Authentication. Proceedings, 2, pages 694–700.

ASHA, S. & CHELLAPPAN, C. 2008. Authentication of e-learners using Multimodal Biometric Technology. *Biometrics and Security Technologies International Symposium, 2008***,** 1(5), pages 7-13.

AWAD, A. 2012. Machine Learning Techniques for Fingerprint Identification: A Short Review. *Journal of Informing Science,* 2(1)**,** pages 524–531.

CHELLAPPAN, A. A., KARIM, N. A. & SHUKUR, Z. 2015. Review of User Authentication Methods in Online Examination. *Asian Journal of Information Technology,* 14 (5)**,** pages 166-175.

CHIN, T-J. AND SUTER, D. 2006. A New Distance Criterion for Face Recognition using Image Sets. In Proc. Asian Conference on Computer Vision, pages 549–558.

CLARKE, N. L., DOWLAND, P., & & FURNELL, S. M. 2013. E-Invigilator: A Biometric-Based Supervision System for e-Assessments. *Proceedings of International Conference on Information Society. Toronto, Canada.***,** 9, pages 238-242.

DARWISH, A. A., ABDELGHAFAR, R., & ALI, A. F. 2009. Multimodal Face and Ear Images. *J. Comput. Sci. 5*(5), pages 374–379.

DAS, S. S. & DEBBARAMA, S. J. 2010. Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System. *International Journal of Information and communication Technology Research,* 1(5), pages 39-45.

EL-ABED, M., GIOT, R., HEMERY, B. & ROENBERGER, C. 2012. Evaluation of Biometric Systems: A Study of Users' Acceptance and Satisfaction. *International Journal of Biometrics* 4(3), pages 265-290.

ESAN, O. A., NGWIRA, S. M. & T. ZUVA 2014. Bimodal Biometrics for Health Care Infrastructure Security, Proceedings of the International MultiConference of Engineers and Computer Scientists Vol. I, pages 1-7.

EVENO, N. & BESACIER, L. 2005. Co-inertia Analysis for Liveness Test in Audio-visual Biometrics. *Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis, IEEE*, 3(4), pages 26-32.

FACES96 (nd) [Online] http://cmp.felk.cvut.cz/~spacelib/faces/faces96.html, assessed on January 15, 2020.

FACE RECOGNITION AND SETTING [Online] http://cswww.essex.ac.uk/mv/allfaces, assessed on January 15, 2020.

FLIOR, E. & KOWALSKI, K 2010. Continuous Biometric User Authentication in Online Examinations. *7th International Conference on Information Technology*, *International Conference on Information Technology: New Generations*, Las Vegas, NV, pp. 488-492, doi: 10.1109/ITNG.2010.250.

FORSEN, G., NELSON, M., & STARON, R. J. 1977. Personal Attributes Authentication Techniques. *Technical Report RADC-TR-77-333, Rome Air Development Center, Rome Air Development Center,* 2(1), pages 1-5.

GAINES, R. S., LISOWSKI, W., PRESS, S. J. & SHAPIRO, N. (1980). Authentication by Keystroke Timing: Some Preliminary Results. Technical Report R-2526-NSF. Santa Monica, CA: Rand Corporation.

GAO, Q. 2012. Biometric Authentication to Prevent E-cheating. *Instructional Technology,* 3, pages 17-23.

GHOSH, P. & DUTTA, R. 2012. A New Approach Towards Biometric Authentication System in Palm Vein Domain. *International Journal of Advanced Information Technology (IJAITI),* 1(2), pages 1-10.

GOURIER, N., HALL, D. & CROWLEY, J. L. 2004. Estimating Face Orientation from Robust Detection of Salient Facial Features *Proceedings of Pointing 2004, ICPR, International Workshop on Visual Observation of Deictic Gestures, Cambridge, UK,* 2(1), pages 1-6.

GOWDA, H. D. S., KUMAR, G. H. & IMRAN, M. Multimodal Biometric Recognition System Based on Nonparametric Classifiers. *Data Anal. Learn. 43*, pages 269–278.

GUPTA, S., MARKEY, M. K. & BOVIK, A. C. 2010. Anthropometric 3D Face Recognition. *International Journal of Computer Vision*, 90(3), pages 331-349

HILLIER, M. & FLUCK, A. 2013. Arguing again for e-exams in High Stakes Examinations. *30th ascilite Conference 2013 Proceedings, Macquarie University, Sydney*, 3(1), pages 385-389.

HONG, L & JAIN, A. 1998. Integrating Faces and Fingerprints for Personal Identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 20(12), pages 1295-1307.

HU, W-C., YANG, C-Y., HUANG, D-Y. AND HUANG, C-H. 2011. Feature-based Face Detection against Skin-color Like Backgrounds with Varying Illumination. *Journal of Information Hiding and Multimedia Signal Processing,* 2(2), pages 123-132.

JAIN, A. K. & KUMAR, A. 2010. Biometrics of Next Generation: An Overview to Appear in Second Generation Biometrics. *Springer*, 2(1), pages 25-31.

JAIN A. K., PRABHAKAR S. & & ROSS A. 2004. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology,* 14(1), pages 4-20.

JAZAHANIM, K. S., IBRAHIM, Z. & MOHAMED, A. 2009. Online Zones' Identification using Signature Baseline. *Second International Conference on the Applications of Digital Information and Web Technologies, 2009, IEEE*, 3(4), pages 20-26.

JEAN, P. 2017. Invigilators Observing Online Exam Test takers *Inside Higher Education,* 1(1), pages 1-5.

JISC 2006. Effective Practice with E-assessments. *Journal of online education,* 2(1), pages 13-18.

JORTBERG, B. 2009. Online Learner Authentication: Verifying the Identity of Online User's. *Journal of Online Learning and Teaching,* 5(2), pages 197-207.

KARAMI, M., HEUSSEN, N., SCHMITZ-RODE, T. & BAUMANN, M. 2009. Advantages and Disadvantages of Electronic Assessments in Biomedical Education. *IFMBE Proceedings,* 25(12)**,** pages 61-64.

KARIM, N. A., SHUKUR, Z. & GHAZAL, M. 2016. Proposed Features of Online Examination Interface Design. *Asian Journal of Information Technology,* 15(16):2733-2736.

KILLOURHY, K. AND MAXION, R. 2009. Keystroke Dynamics - Benchmark Data Set Accompaniment to "Comparing Anomaly-Detection Algorithms for Keystroke Dynamics [Online] [Accessed 8th February, 2021].

LAI, J., YUEN, P. & FENG, G. 2001. Face Recognition Using Holistic Fourier Invariant Features, *Pattern Recognition,* 34(1), pages 95–109.

LATHA P., GANESAN L.& ANNADURAI S., 2009. "Face Recognition using Neural Networks", *Signal Processing: An International Journal,* 3(5), pages 153 –160.

LIN, S.H., S.Y. KUNG AND L.J. LIN, 1997. Face Recognition/Detection By Probabilistic Decision-Based Neural Network. IEEE T. *Neural Network,* 8: pages 114-132.

LOY, C. C., LAI, W. K. AND LIM, C. P. 2007. "Keystroke Patterns Classification Using the ARTMAP-FD Neural Network," *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007)*, Kaohsiung, 2007, pages 61-64.

LUCAS, B. D. AND KANADE, T. (1981). An Iterative Image Registration Technique with an Application to Stereo Vision. Proceedings of Imaging Understanding Workshop, pages 121—130.

LUMINI, A. & NANNI, L. 2007. When Fingerprints are Combined with Iris – A Case Study: FVC2004 and CASIA. *International Journal of Network Security,* 4(1)**,** pages 27–34.

MESHOUL, S. & BATOUCHE, M. 2010. Combining Fisher Discriminant Analysis and Probabilistic Neural Network for Effective On-line Signature Recognition. *IEEE 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA)*. 7(1), pages 17-25.

MITTAL, N. & WALIA, E. 2008. Face Recognition Using Improved Fast PCA Algorithm. 2008 Congress on Image and Signal Processing CISP '08. 1, pages 554-558.

MOHSEN, F. M.A., HADHOUD, M. M., AMIN, K. 2010. A New Optimization-Based Image Segmentation Method By Particle Swarm Optimization. *Int. J. Adv. Comput. Sci. Appl.* 7 (4), pages 10–18.

MONROSE & RUBIN (2000). Keystroke Dynamics As A Biometric For Authentication. *Future Generation Computer Systems,* 16(4), pages 351-359.

NADER A. K. & ZARINA S. 2016. Using Preferences as User Identification in the Online Examination. *International Journal of Advanced Science Engineering Information Technology, 6(6), pages 1026-1032.*

NAGI, J., AHMED, S. K. & NAGI, F. 2008. A MATLAB based Face Recognition System Using Image Processing and Neural Networks. In: *Proceedings of the 4th IEEE International Colloquium on Signal Processing and its Applications*, Kuala Lumpur, Malaysia, 7–9 March 2008, pp.83–88. Piscataway: IEEE, 2008.

NANDINI, M., BHARGAVI, P. & SEKHAR, G. R. 2013. Face Recognition Using Neural Network. *International Journal of Scientific and Research Publications,* 3(3), pages 1-5.

NEAGOE, V., MITRACHE, J. & PREOTESOIU, S. 2006. A Feature-Based Face Recognition Approach Using Gabor Wavelet Filters Cascaded with Concurrent Neural Modules. *2006 World Automation Congress*, Budapest, 2006, pages 1-6.

OUERHANI, Y., JRIDI, M., & ALFALOU, A. 2010. Fast Face Recognition Approach Using A Graphical Processing Unit "GPU". In Proceedings of the 2010 IEEE International Conference on Imaging Systems and Techniques, Thessaloniki, Greece, 1–2 July 2010; IEEE: Piscataway, NJ, USA, 2010; pages. 80–84.

PELLEGRINO, J. W., CHUDOWSKY, N., & GLASER, R. (2001). *Knowing what students know: The science and design of educational assessment.* Washington, DC: National Academy Press.

PENTEADO, B. E. & MARANA, A. N. 2006. A Video-Based Biometric Authentication for e-Learning Web Applications. *In: Enterprise Information Sytems Filipe, J. and J. Cordeiro (Eds.). Springer, Berlin, Heidelberg, Germany***,** 2(1), pages 770-779.

PERES, P., LIMA, L. & LIMA, V. 2014. B-Learning Quality: Dimensions, Criteria and Pedagogical Approach. *European Journal of Open, Distance and e-Learning,* 17(1)**,** pages 56-75.

RAMU, T., SUTHENDRAN, K. & ARIVOLI, T. (2000). Machine Learning Based Soft Biometrics For Enhanced Keystroke Recognition System. *Multimed Tools Appl* **79, pages** 10029–10045.

RANI, J. S. & DEVARAJ, D. 2012. Face Recognition Using Krawtchouk Moment. *Sadhan*, 37, Part 4, Pages 441–460.

RAVI, J, RAJA, K. B., VENUGOPAL. K. R. 2009. Fingerprint Recognition Using Minutia Score Matching. *International Journal of Engineering Science and Technology,* 1(2), pages 35-42.

ROBITAILLE, D.F., SCHMIDT, W.H., RAIZEN, S.A., MCKNIGHT, C.C., BRITTON, E., AND NICOL, C. (1993). *TIMSS Monograph No. 1: Curriculum Frameworks for Mathematics and Science*. Vancouver, Canada: Pacific Educational Press.

ROSS, A., PRABHAKAR, S. & JAIN, A. K. 2004. An Introduction to Biometric Recognition. *International Journal of Information and communication Technology,* 1(3), pages 10-17.

RUDRAPAL, D., DAS., S., DEBBARMA., S., DEBBARMA, N. & KAR., N. 2012. Voice Recognition and Authentication as a Proficient Biometric Tool and its Application in Online Exam for PH People. *International Journal Computing Application,* 39**,** pages 6-12.

SAHOOLIZADEH, A. H., HEIDARI, B. Z., DEHGHANI, C. H. 2008. "Face Detection using Gabor Wavelets and Neural Networks" World Academy of Science, Engineering and Technology, 45, pages 552- 554.

SALIL, P. & SHARATH, P. 2003. Biometric Recognition: Security and Privacy Concerns. *IEEE Security and Privacy*, 10, pages 49-55.

SAYEED, S., HOSSEN, J. KALAIARASI, S. M. A., JAYAKUMAR, V., YUSOF, I. & SAMRAJ, A. (2017). Real-Time Face Recognition for Attendance Monitoring System. *Journal of Theoretical and Applied Information Technology, 4, pages 1-9.*

SHARIF M., AYUB K., SATTAR D. AND RAZA M. (2012). "Real TimeFace Detection", *Sindh Univ. Res. Jour.* (Sci. Ser.) 44(4), pages 597- 600.

SHAVER, C. D. & ACKEN, J. 2009. Effects of Equipment Variation on Speaker Recognition Error Rates. *International Conference on Acoustics Speech and Signal Processing (ICASSP), IEEE*.1(2), pages 8-14.

SHENDE, P. M., SARODE, D. M. V. & GHONGE, P. M. M. 2014. A Survey Based on Fingerprint, Face and Iris Biometric Recognition System, Image Quality Assessment and Fake Biometric. *International Journal of Computer Science Engineering and Technology (IJCSET) / April 2014,* 4, pages 129-132.

SOGUKPINAR, I. & YALÇIN, L. (2004). "User Identification Via Keystroke Dynamics, *Ist. Üniv. Journal of Electrical and Electronic Engineering,* 4(1), pages 995-1005.

SOUHEIL, B. Y. 2007. Multi-Modal Data Fusion for Person Authentication using SVM. *IDIAP Research report***,** 5, Pages 1 – 9.

SPACEK, L. 2015. Face Recognition Data. *Informing Science Journal,* 5(6), pages 9-16.

STEWART, J.C., MONACO, J.V., CHA, S., & TAPPERT, C.C. 2011. An Investigation of Keystroke and Stylometry Traits for Authenticating Online Test Takers. In Proceedings of the international joint conference on biometrics (IJCB'11) Washington, DC, pages 1-7.

STÉN, A., KASEVA, A. & VIRTANEN, T. 2003. Fooling Fingerprint Scanners – Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner. *4th Australian Information Warfare and IT Security Conference***,** 8(1), pages 333–337.

SUHAS, S., KHURLE, A. & KHANALE, P. 2012. Face Recognition Using Principal Component Analysis and Linear Discriminant Analysis on Holistic Approach in Facial Images Database. *IOSR Journal of Engineering,* 02(12), pages 15-23.

ŚLUZEK, A. & PARADOWSKI, M. 2012. Visual similarity issues in face recognition. *International Journal of Biometrics,* 4(1), pages 22–37.

TEH, P.S., TEOH, A.B.J., TEE, C., & ONG, T.S. 2011. A Multiple Layer Fusion Approach on Keystroke Dynamics. *Pattern Analysis and Applications*, 14(1), pages 23–36.

TEY, C-H, GUPTA, P. & GAO, D. (2013) I Can Be You: Questioning the Use of Keystroke Dynamics as Biometrics. Annual Network and Distributed System Security Symposium 20th NDSS 2013, 24-27 February, 2013, Pages 1-16.

TENREIRO DE MAGALHÃES, S. & SANTOS, H. M. D. (2005). An Improved Statistical Keystroke Dynamics Algorithm. IADIS Virtual Multi Conference on Computer Science and Information Systems, Malta. Pages 1-5.

THAKUR S., SING J.K., BASU D.K. & NASIPURI M. 2009. Face Recognition using Fisher Linear Discriminant Analysis and Support Vector Machine. In: Ranka S. et al. (eds) Contemporary Computing. IC3 2009. Communications in Computer and Information Science, vol 40. Springer, Berlin, Heidelberg.

TOMASI, C. & KANADE, T. (1992). Shape and Motion from Image Streams under Orthography: a Factorization Method. *International Journal of Computer Vision,* 9(2), pages 137-154.

ULLAH, A., XIAO, H., LILLEY, M. & BARKER, T. 2012. Using Challenge Questions for Student Authentication in Online Examination. *International Journal information,* 5(1), pages 59-65.

VACLAV, M., J. & RIHA, Z. 2003. Toward Reliable User Authentication Through Biometrics. *IEEE Security & Privacy,* 1(1)**,** pages 45-49.

VIOLA, P AND JONES, M. (2001). "Rapid Object Detection Using a Boosted Cascade of Simple Features," *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001*, Kauai, HI, USA, 2001.

WANG, Y., MU, Z. & ZENG, H. 2008. Block-Based and Multi-Resolution Methods for Ear Recognition Using Wavelet Transform and Uniform Local Binary Patterns. In *Proceedings of the 19th IEEE International Conference on Pattern Recognition (ICPR)*. pages 1–4.

WONG, K., LAM, K. & SIU, W. 2001. An Efficient Algorithm for Human Face Detection and Facial Feature Extraction Under different Conditions. *Pattern Recognition*, 34:1993-2004.

YANG, M., WANG, X., ZENG, G. & SHEN, L. 2017. Joint and Collaborative Representation with Local Adaptive Convolution Feature for Face Recognition with Single Sample Per Person. *Pattern Recognition,* 66, pages 117–128.

ZHANG, D. 2008. Automated Biometrics Technologies And System. *Proceedings of International Conference on Information Society,* 3(4)**,** pages 13-17.

ZHENLIANG H., JIE Z.**,** MEINA K., SHIGUANG S. & XILIN C. 2017. Robust fec-cnn: A High Accuracy Facial Landmark Detection System, 30th 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), USA.

ZHONG, Y., DENG, Y. & JAIN, A. K. (2012). Keystroke Dynamics for User Authentication, *2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, Providence, RI, 2012, pp. 117-123.

ZVIRAN, M. & ERLICH, Z. 2006. Identification and Authentication: Technology and Implementation Issues. C*ommunications Assoiation Information Systems,* 17, pages 11-16.