**CHAPTER ONE**

**Introduction**

This chapter describes the project and provides some background information. Furthermore, this chapter follows the project's problem statement to clearly understand the project's scope and objectives. This chapter will serve as a blueprint for all subsequent phases of development.

**1.1 Background of The Study**

Information and communication technology are one of the many sectors throughout the world that are growing in Nigeria. An examination is a formal exam that students take to demonstrate their knowledge of a specific subject, which is usually done in written form at Kaduna polytechnic that comprises a set of questions to be answered and will be used in grading the student.

The formal examination is the assessment of a person's performance when confronted with a series of questions, problems, or tasks to determine the amount of knowledge that s/he has acquired, the extent to which she/he can apply it, or the quality and effectiveness of the skills that s/he has developed. Exams are also increasingly being used to choose candidates for public service, professions, and positions in industry and commerce. Standardized testing has been the most popular practice throughout history, although the validity and legitimacy of the enlarged range of modern assessment methodologies have been called into doubt. (Ahmed & Abdulaziz, 2017).

An examination is credible if it is free and fair, free of bias, cheating, and other types of examination malpractice. One of the most common types of test misconduct is candidate impersonation. The idea is to engage a more competent individual as machinery to write the exam for the original candidate. An invigilator recognizes a real applicant by his identity card, which includes his name, photo, and other pertinent information. Only the candidate's photo is verified on the spot out of all the information on the Identity card. That is, the invigilator examines the candidate's face and compares it to the image on the identity card. Unknown to him, the impostor's photo might be on the identity card, while other information belongs to the true owner. Rufai et al. (2017)

According to a recent study by (Patrick et al., 2019) The process of determining the truth, correctness, or validity of anything, such as the verification of official papers, is known as verification. Realistic authentication such as biometrics is a type of physical or behavioral human features that may be used to digitally identify a person to get access to systems, devices, or data. (Korolov, 2019).

Korolob, (2019) relates to studies conducted recently that biometrics can significantly improve business security by providing a fair degree of confidence in authenticating a person with reduced friction for the user. When computers and gadgets recognize the fingerprints of an authorized user, they can unlock automatically. When trusted system administrators' faces are recognized, server room doors can swing open. When a help desk system recognizes an employee's voice on the support line, it may instantly pull up all pertinent information.

The security of biometric authentication data is critical, perhaps more so than password security, because passwords may be quickly altered if they are revealed. A fingerprint or retinal scan, on the other hand, is unchangeable. The publication of this or other biometric information might endanger users indefinitely and expose the corporation that loses the data to considerable legal liability (Korolob, 2019).

As there are several forms of biometric verification fingerprint biometrics verification will be employed in carrying out the research topic. Biometrics is a technology that identifies a person (uniquely) based on physiological or behavioral traits. It may be used to produce an identification with a high level of confidence, such as a 0.001% mistake rate. Fingerprint technology based on biometrics has the benefit of eliminating the problem of examination impersonation by allowing the measurement of who you are to complete the security activities of student participation in examinations. (Ahmed & Abdulaziz, 2017).

**1.2 Statement of The Problem**

Impersonation happens frequently in the computer science department at Kaduna polytechnic students can attest to this, but no one would want to sell out the person, even if the management makes sure there’s no loose end for students to carry out such dubious acts like laminating the examination card, the student can still make ways to manipulate things. For example, identical twins from different departments can come in and write exams for his/her second without the invigilator knowing. Students can change passports on the examination card to any other person’s passport so the person can come into the examination hall to write the exam for them just to attain a good result even though the examination card has been laminated but still students can do anything to get what they want, But with the help of an examination biometric verification system, such acts will be difficult to carry out because each student will need to verify his/her identity before going to the exam hall.

**1.3 Aim and Objectives of the Study**

To develop an **examination verification system using biometrics** for the department of computer science at Kaduna Polytechnic.

**Objectives**

The objectives of this research work are as follows:

1. Upon opening the newly admitted student file, the administrator would register the student and include their fingerprint in the system, this is how the data set will be generated.
2. The modern languages used in implementing this system is VB.net, and the UareU (SDK) for finger identification to connect with the Digital Persona U 4500 fingerprint scanner.
3. In storing and retrieval of the collected dataset; Microsoft SQL Server Management which is an open-source relational database, will be used as the database technology.
4. Vital testing will be carried out in ensuring the efficacy of the research work

**1.4 Scope of the Study**

This research work would include an investigation of the current methods used to verify the identity of students during exams, and an evaluation of the feasibility and potential benefits of implementing a biometric-based verification system. The research work will only be on an examination base and not on any other type of assessment

**1.5 Limitations of the Study**

This study's scope has been constrained by several core issues, including:

**Access to literature** – Access to some material was restricted, although the available material was optimized.

**Time** - The researcher's everyday busy academic pursuits limited the time allotted for research for this study.

**1.6 Significance of Study**

With the rising occurrence of examination malpractice in the educational sector, school administrators must implement strict security measures to guarantee that exam impersonators' activities cease. The study may influence preventing corruption in the educational system among students and between students and instructors.  Every registered student understands that he or she will have to write the exam on his or her own. The mimicry that has eaten the educational system by promoting student laziness would be abolished, and the level of student educational achievement would be raised.

**1.7 Project Organization**

The project is divided into five chapters. The outlines are presented below:

**Chapter One: Introduction**

Chapter one introduces this project work, the study's background, the problem statement, the purpose and objectives, the scope of the study, the constraints of the study, the relevance of the study, the project organization, and the definition of terms.

**Chapter Two: Literature review**

This chapter focuses on the literature review, and the contributions of other scholars on the subject matter being discussed.

**Chapter Three: Methodology and Design**

This chapter is concerned with the presentation of the results of system analysis and design. It presents the research methodology used in the development of the system to facilitate an understanding and effective future implementation of the system.

**Chapter Four: System Implementation Evaluation**

This chapter describes the system implementation and documentation, analysis of modules, and system requirements for implementation.

**Chapter Five: Summary, Conclusion, and Recommendation**

The chapter provides a summary of major findings, conclusions, and recommendations based on the study conducted.

**1.8 Definition of Terms**

1. **Biometrics:** The use of unique physical characteristics (such as fingerprints, facial features, or iris patterns) to identify individuals.
2. **Verification:** The process of confirming the accuracy or truth of something.
3. **Examination:** A formal test or assessment, typically in a school or university setting**.**
4. **Authorization:** theprocess of granting access or permission to a person or system to perform a specific action or access a particular resource**.**
5. **Impersonation**: General process of acting on behalf of a client.
6. **Impersonator**: A performed skilled at copying the manner or expression of another mime.
7. **fingerprint**: An impression on the surface of the curves formed by the ridges on a fingertip.

**CHAPTER TWO**

**Literature Review**

**2.1 Introduction**

This chapter's goal is to demonstrate how the topic under study relates to previous research, current practice, or other areas of knowledge by citing pertinent works by other scholars that have dealt with a similar issue. In addition, this chapter will provide a synthesis of the existing research on the topic, highlighting areas of agreement, disagreement, and gaps in the literature, to establish the importance of the project topic in the field and to identify areas for further research.

**2.2 Literature Review**

Haruna (2018). sVeriTool: A Verification Tool for Preventing Impersonation of Students in Examination Halls Using Fingerprints. Despite worldwide growth and the use of information technology in many parts of human activities, students are manually validated and admitted into the examination hall through the display of their examination cards under the current system. The procedure is completely onerous, time-consuming, and deceptive. Furthermore, at certain schools, students are only partially verified when writing their exams, which may eventually lead to impersonation as a form of exam malpractice and, as a result, a lower grade in education.

Furthermore, the methodology of research might be quantitative or qualitative. The data was gathered through interviews with both students and faculty at Yusuf Maitama Sule University in Kano, as well as careful analysis and comprehension of the entire process, as well as research on examination and other related activities at Nigerian institutions of higher learning. The existing technique of student verification was determined to be laborious and ineffective after a thorough evaluation. The system was created utilizing Visual Basic (VB), a Microsoft SQL server for database services, and the GrFinger Software Development Kit (SDK) for finger identification.

In conclusion, when compared to their manual equivalents, automated methods have shown to be more intuitive and efficient. Because of the naturalness and uniqueness of fingerprints, they serve as a credible identification and verification tool. This research has developed a trustworthy student verification method based on their fingerprints, preventing impersonation and simplifying the required activities. The tool may also cause lecturers (staff) to focus more on other crucial areas of examinations.

Garko and Ahmad (2017). Design And Modeling of a Student Verification System in an Examination in Nigeria using Biometric Fingerprint Technology. All old methods of examination verification have the problem of being unable to distinguish between an authorized person and an imposter who illegally obtains the authorized person's access right. Students' authentication is not secure. The inefficiency of the procedure is due to student population or class size, nevertheless, the manual process is time-consuming.

Moreso, the system used the internationally known software engineering model to get very decent acceptance of the research effort; this system is created utilizing the SSADM (Structured System Analysis and Design Methodology) and Prototype Model, both of which are object-oriented. In this study, Visual Basic 6.0 was used to create the interfaces, and MySQL was used as the back end.

Finally, when compared to manual systems, the proposed solution has proven to be more successful. Fingerprints are a solid access control approach due to their authenticity. The fact that a user no longer has to carry identity cards or other identifying papers explains the convenience of usage. The student verification system reinvents the manual verification approach, preventing academic fraud as well as illegitimate student certificates and documents.

Traoré et al. (2017). Ensuring Online Exam Integrity Through Continuous Biometric Authentication. Online education is a common area where unlawful credential sharing happens. Students may easily cheat on tests using existing learning management systems (LMS) by revealing their credentials to others who can take the tests in their place. While certain Exam Management Systems (EMS) enable biometric strong authentication, such authentication occurs only statically at login time, leaving the door open for impersonation to occur after the first login period.

Furthermore, using a local binary pattern and chi-square distance, we conceived and developed our continuous face biometric authentication system. The model learns the user's facial characteristics entirely through positive reinforcement and stores the extracted patterns in XML files. We created a set of heuristics to increase the system's accuracy and reduce the false rejection rate. Existing options include sending recorded frames to a facial recognition server using communication protocols such as WebSocket.

In conclusion, the system proposes a multimodal biometric architecture for online test takers' ongoing authentication. The framework is a key component of the ExamShield platform, a new online exam monitoring system, in addition to continuous authentication, offers live video streaming and recording of test settings, as well as key exam management capabilities.

Math and Prasanna (2019). Bio-Metric Enabled Examination Student Verification System. Due to the old examination method, which uses pen and paper to verify and is primarily focused on human interactions, impersonation is relatively easy at some point during the examination attendance verification process. The method is built on trust and loyalty, much as at steak. Anyone with some degree of manipulation may impersonate a candidate taking the test.

Moreso, the Fingerprint module used in this project is R307, which is a modified version of the Fingerprint module R305. An Arduino Mega was used, which is a board with a built-in microprocessor that was inspired by the Arduino Mega 2560, and an SD Card Interface to enable the reading or writing of files from the Arduino to SD cards.

In conclusion, this project employed a fingerprint biometric to authenticate the original applicant and quickly transfer the information to the examination office using a ZigBee transceiver. We gather the candidate's fingerprint when he applies for the test, validate it when he takes the exam, and cross-check it again when he receives the certificate, if necessary.

Ojo et al. (2019) Deterring Malpractice in a Networked Computer-Based Examination Using Biometric Control Attendance Register. Some students who are afraid of CBT tests for one reason or another utilize a third party to write the exams for them, especially if the attendance record is done manually and there is little or no supervision over the students' access to the examination system in the computer room. Personal identification numbers (PINs) are a frequent strategy that may be supplied to the imposter to sit and write exams for the other student.

Furthermore, the suggested system consists of a camera that captures photos of students and sends them to an image enhancement module. Following that, the enhanced photos are compared to persons sitting or taking the examination (Face Detection and Recognition) modules. The database server will then record the attendance. Face recognition biometric technology was used in this study to detect various faces. The collected picture database was developed using the K-means/hierarchical algorithm model and EM algorithms to begin and refine the database model, respectively. Skin segmentation, candidate face search, and verification were used for face recognition, whereas face image processing and classification were used for face recognition. The complete procedure was written in java.net.

In conclusion, this study used face recognition to discourage students from impersonating others during exams, which is common in several institutions. The researchers implemented the developed facial recognition system on the server of the networked CBT computer networked setup for the purpose of the study activity. The system was evaluated, and the results reveal that the recognition test for candidates/students utilized in the training and testing phase is highly accurate.

**2.3 Summary of Related Literature Reviews**

|  |  |  |
| --- | --- | --- |
| **Author & Year** | **Title & Description** | **Merit and Demerits** |
| Haruna (2018). | sVeriTool: A Verification Tool for Preventing Impersonation of Students in Examination Halls Using Fingerprints.  E-Invigilation is a biometric technology based on fingerprints that may be used for student verification during examinations with the primary goal of eradicating impersonation as a type of test misconduct. | The system provided reliable identification and  verification mechanism  The verification can only be done with the system that has the program installed |
| Garko and Ahmad (2017). | Design and Modeling of a Student Verification System in an Examination in Nigeria using Biometric Fingerprint Technology.  The research will assist in quickly identifying students who have registered for a certain course and in quickly identifying individuals who are qualified to enter the test hall. | When compared to the manual approach of student verification, the system is more secure, and efficient.  Only unit testing was done. |
| Traoré et al. (2017). | Ensuring Online Exam Integrity Through Continuous Biometric Authentication.  This article proposes a multimodal biometric architecture for continuous authentication of online test takers | The system allows for live video broadcasting as well as the recording of exam environments.  Changes in lighting circumstances, such as shutting off the light during the exam might have a negative impact on identification accuracy. |
| Math and Prasanna (2019). | Bio-Metric Enabled Examination Student Verification System.  In this research, the researchers offer Location Finder, a mobile Web application that allows users to explore their surroundings by exploiting contexts that are significant to them | The gadget is small and simple to use.  A large SD Card is needed to store the file produced by the Arduino. |
| Ojo et al. (2019) | Deterring Malpractice in a Networked Computer-Based Examination Using Biometric Control Attendance Register.  This study focuses on the development of a biometric control examination attendance register to prevent impersonation during examinations. | The system discouraged students from impersonating others during exams.  Poor user interface. |

**2.4 Analysis of the Current System**

The existing systems make no use of the biometrics idea. In the department, students must first register for their courses, after which the recording officer will issue an exam card containing their passport photograph as well as the registered courses. The exam card must be brought to the exam hall for each exam, but this is still not a strong measure of security because the eyes are used in this case to check for the occurred passport and the physically occurring human. A student who is unable to write the recommended course due to academic laziness may pay someone to come and write the courses for him. The individuals involved are impersonators who are conducting exam malpractices. When it comes time for exams, students are required to come to the exam hall with their exam card, which acts as authorization for them to enter the exam hall and fully participate in the exam. The impostor can easily extract the actual passport from the exam card and attach his or her own, which the invigilators may never notice. However, this eye-matching verification has shown to be ineffective and contains several loopholes.

**2.4.1 Problem Inherent in** **the Current System**

Several issues arise while using the existing system, including:

1. Inefficiency in its use and comprehension of the act of exam impersonation.
2. Matching to build security measures happens through the physical eye, which is a major issue and requires a high level of recognition capacity, so an impostor can be present with recognition.
3. Identical twins from different departments can come in and write exams for his/her second without the invigilator knowing

**2.5 Analysis of the Proposed System**

Fingerprint biometric examination verification is a method of verifying a person's identity by analyzing their fingerprints. This method is considered to be one of the most reliable forms of biometric identification because fingerprints are unique to each individual and do not change over time. The process of fingerprint verification typically involves capturing an image of the person's fingerprint and then comparing it to a previously recorded image to confirm the person's identity.

One of the advantages of fingerprint biometric examination verification is that it can be performed quickly and easily, making it a convenient method for identity verification. It is also relatively inexpensive compared to other forms of biometric identification such as facial recognition or iris scanning. Another advantage is that fingerprints are unique to each individual, which means that the chances of a false match are extremely low. This makes fingerprint verification a very secure method of identification.

However, one of the drawbacks to fingerprint biometric examination verification. For example, if a person's fingerprints are dirty or damaged, it may be difficult to capture a clear image for verification.

Overall, fingerprint biometric examination verification is a reliable and secure method of identity verification that has many practical applications.

**CHAPTER THREE**

**Methodology and Design**

**3.1 Introduction**

A methodology is a rigorous study or inquiry, particularly to unearth new facts or information; thus, research methodology should be good enough to enable the achievement of the specified objectives, which are achievable using specific components, such as data collection and design procedures, and system modeling (use case, activity, and class diagrams). This chapter provides the input/output specifications as well as the system requirements for the examination verification system using biometrics for the department of computer science at Kaduna polytechnic.

**3.2 Methods of Data Collection**

Before developing any system, collecting data and facts about the existing system is critical to understand what is going on. This research was carried out using three methods.

1. Observation of the Work Environment
2. Interview
3. Documentation

**3.2.1 Observation of the Work Environment**

This strategy was used to collect information and data for this study by observing how the manual system functioned. Detailed inspection revealed the most obvious weaknesses in the present system. The setting in which the observation is made can be altered in a variety of ways when using the observational technique.

**3.2.2 Interview**

The primary goal of utilizing interviews as a data-gathering strategy is to get information comprehensively and rigorously. Based on the questions supplied by the researcher, the researcher met with certain students and staff members and gathered accurate information.

**3.2.3 Documentation**

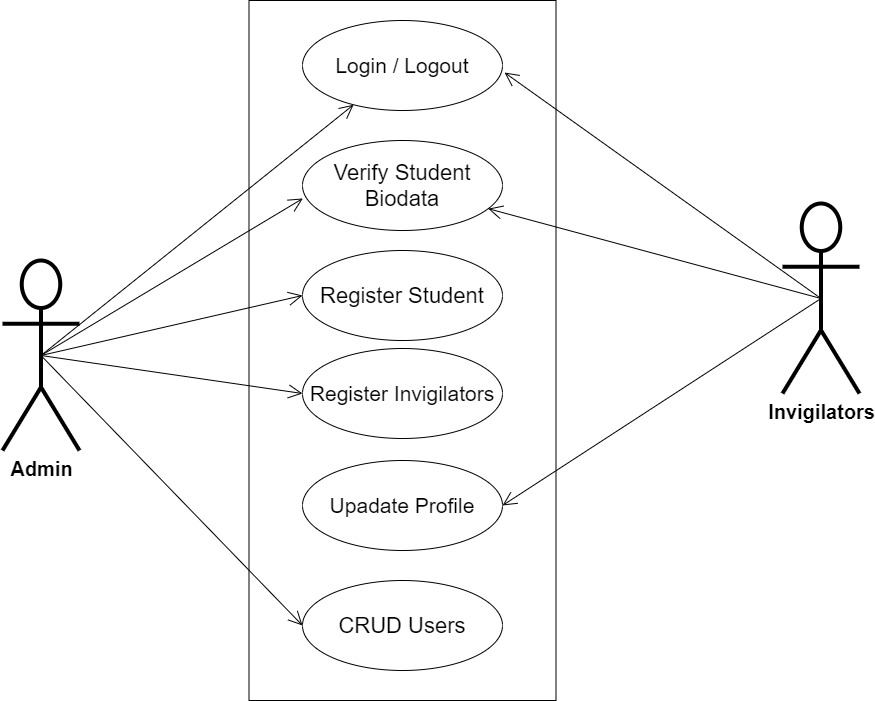
Secondary data gathering includes documentation. Journals, manuals, previous work, publications, and other sources are used in this manner. This data-gathering strategy is chosen because it allows for comparison with previous research. This includes the internet, which is a tool for data collecting. The internet was utilized to research complex or unclear problems.

**3.3 System Modeling**

A system model is a conceptual model of a system that explains and represents it. A system is any interaction between a set of components that work together to achieve a common purpose. Visual models of object-oriented software-intensive systems may be created utilizing a set of visual notation techniques included in the Unified Modeling Language, which is used in the creation of this contemporary system. UML diagrams utilized in this new design include use case diagrams, class diagrams, and activity diagrams.

**3.3.1 Use Case Diagrams**

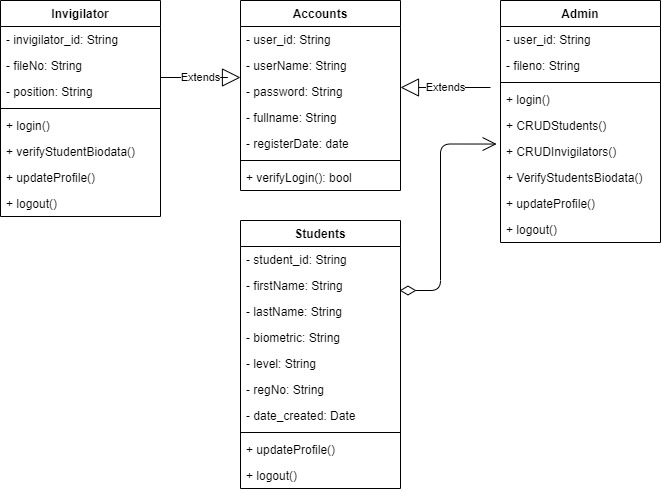
Use cases are collections of interactions between the system and the user. Use case diagrams are used to graphically depict a system's functionality in terms of its actors, goals (represented as use cases), and dependencies among those use cases.



**Fig 3.1 System Use Case Diagram**

**3.3.2 Class Diagrams**

The Unified Modeling Language (UML) class diagram is an implementation of an independent view of how the system interface might appear, with each class having its own set of properties and displaying how they interact with one another. Class diagrams use the Unified Modeling Language standards to visually depict the static structure and composition of a given system (UML).



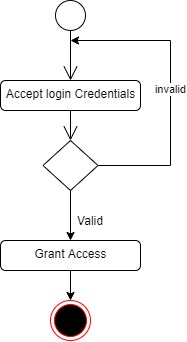
**Fig 3.2 System Class Diagram**

**3.3.3 Activity Diagrams**

An activity diagram, like a flowchart or a data flow diagram, visually illustrates a series of events or the flow of control in a system, but it acts more like an enhanced version of both.

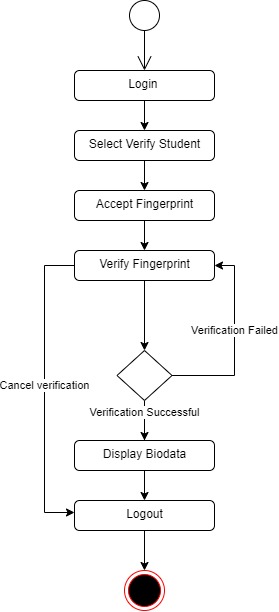
**Login**

The process for gaining access to the system is depicted in the diagram below; the email address and password must be accurate to gain access.



**Fig 3.3.1 Login Activity Diagram**

**Biodata Verification**

The process for verifying student biodata is depicted below, to verify the invigilator has to be authenticated before accepting student fingerprints for verification.

**Fig 3.3.2 Biodata Verification Activity Diagram**

**3.4 Database Design**

The logical explanation of how data is kept in the computer's memory is called input specification. The freedom experienced in using the system, as well as the convenience of retrieving and reading the data and assuring applicability across the internet, make SQL standards essential for ensuring that structured data is uniform and independent of applications. Some of the input specifications employed in this project work are presented below.

1. Invigilators Table: contains basic information about all invigilators.
2. Students Table: contains every system-saved student information.

**Table 3.1 Invigilators** **Input Specification Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Null** | **Key** | **Length** | **Description** |
| invigilator\_id | Varchar | No | PK | 32 | Unique string for identifying invigilators |
| username | Varchar | No |  | 100 | Invigilators email address |
| password | Varchar | No |  | 128 | Invigilators Password |
| fullName | Varchar | No |  | 60 | Invigilators full name |
| position | Varchar | No |  | 60 | Invigilators full name |
| Register data | DateTime | No |  | 20 | Invigilators registration date |

**Table 3.2 Students** **Input Specification Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Field Name** | **Data Type** | **Null** | **Key** | **Length** | **Description** |
| student\_id | Varchar | No | PK | 32 | Unique string for identifying students |
| firstName | Varchar | No |  | 100 | Student first name |
| lastName | Varchar | No |  | 100 | Student last name |
| biometric | Varchar | No |  | 128 | Student captured biometrics |
| Level | Varchar | No |  | 10 | Student Level |
| regNo | Varchar | No |  | 14 | Student registration number |
| date\_created | Varchar | No |  | 20 | Date the student account was created |

**3.5 Output Design**

This declares and displays the outcome of the given input. This automated system's output is dependent on its input. The output specification is listed below.

**Table 3.3 Users** **output design table**

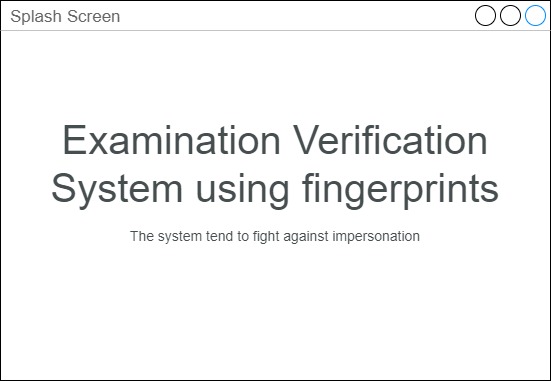
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Invigilator\_id** | **Username** | **Password** | **FullName** | **Position** | **registerDate** |
| XXXX | XXXX | XXXX | XXXX | XXXX | XXXX |
| XXXX | XXXX | XXXX | XXXX | XXXX | XXXX |
| XXXX | XXXX | XXXX | XXXX | XXXX | XXXX |
| XXXX | XXXX | XXXX | XXXX | XXXX | XXXX |

**Table 3.4 Students** **output design table**

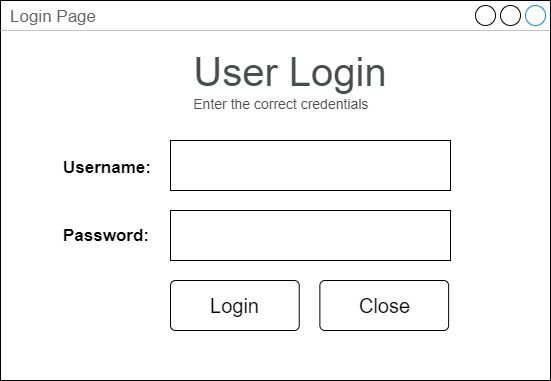
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Student\_id** | **FirstName** | **LastName** | **Biometric** | **Level** | **RegNo** | **Date\_Created** |
| XXXX | XXXX | XXXX | XXXX | XXXX | XXXX | XXXX |
| XXXX | XXXX | XXXX | XXXX | XXXX | XXXX | XXXX |
| XXXX | XXXX | XXXX | XXXX | XXXX | XXXX | XXXX |
| XXXX | XXXX | XXXX | XXXX | XXXX | XXXX | XXXX |

**3.6 Input & User Interface Design**

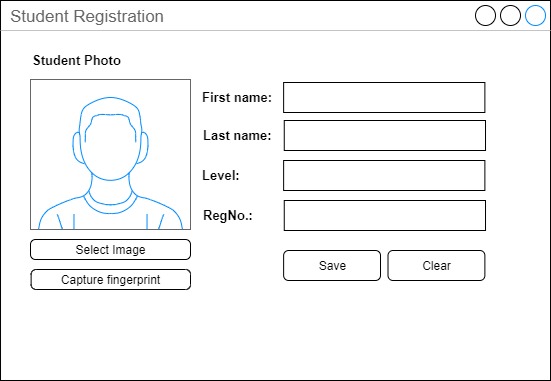
This is a graphic depiction of the system interface; it will be designed to be user-friendly, responsive, and visually beautiful. Furthermore, it will be fully secured, thus authentication will be required to see various levels of the information. To help with the designs, a mid-fidelity wireframing program called Draw.io is employed.



**Fig 3.6.1 Splash Screen**



**Fig 3.6.2 User Login Screen**



**Fig 3.6.2 Student Registration Screen**

**3.7 System Requirement**

Every piece of software that is generated has predefined system requirements that it must fulfill to function properly. The system requirements, on the other hand, are the bare minimum of hardware and software required for the system's intended operation.

**3.7.1 Hardware Requirement**

System Hardware Requirement Include:

1. Minimum of 8 GB of RAM (Random Access Memory) installed.
2. Minimum of intel core i3 processor.
3. Minimum of 250GB HDD (Hard Disk Drive).
4. Fingerprint Reader

**3.7.1 Software Requirement**

The software requirements include:

1. At least windows 10 OS (Operating System).
2. Microsoft SQL Server Management Studio Installation
3. UareU (SDK) Installation
4. Microsoft Visual Studio Installation.

**3.8 Choice of Programming Language**

This research work will be a desktop-based application and will be implemented on a relational database system, VB.net, and the UareU (SDK) for finger identification to connect with the Digital Persona U 4500 fingerprint scanner. The above are the modern languages used in implementing this system.

**CHAPTER FOUR**

**System Implementation Evaluation**

**4.1 Introduction**

This section provides a comprehensive explanation of the implementation process for the new system, highlighting its efficiency and effectiveness. It presents practical instances of the functional aspects of the system and outlines the steps involved in its implementation.

* 1. **System Testing and Evaluation**

Testing the developed system is crucial for several reasons. One key purpose is to uncover any potential flaws within the system and devise appropriate solutions. In this project, a combination of unit and integration testing was employed to verify the effectiveness and efficiency of the design, ensuring that the new system fulfills its functional requirements without any errors.

**Unit Testing**

This part examines specific units or single components of the system individually to confirm that specific phases function properly and without problems.

**Integration Testing**

Integration testing was performed on the software, wherein all components were brought together and operated as a unified system. The objective of this testing was to validate the connectivity and proper integration of the various parts, ensuring seamless collaboration among the units.

**4.3 System Installation**

In order to use the proposed application on any computer system, the following steps need to be taken:

1. Make sure, Microsoft Visual 2010 or greater is installed on the system.
2. Make sure Microsoft SQL Server Management Studio 2017 or greater is installed on the system
3. Make sure UareU digital persona SDK is as well installed and the fingerprint scanner plugged to the system.
4. Copy your project folder to any location of your choice.
5. Find and launch the “EVS.sln” file in the project directory
6. Run the program by clicking on the start button.

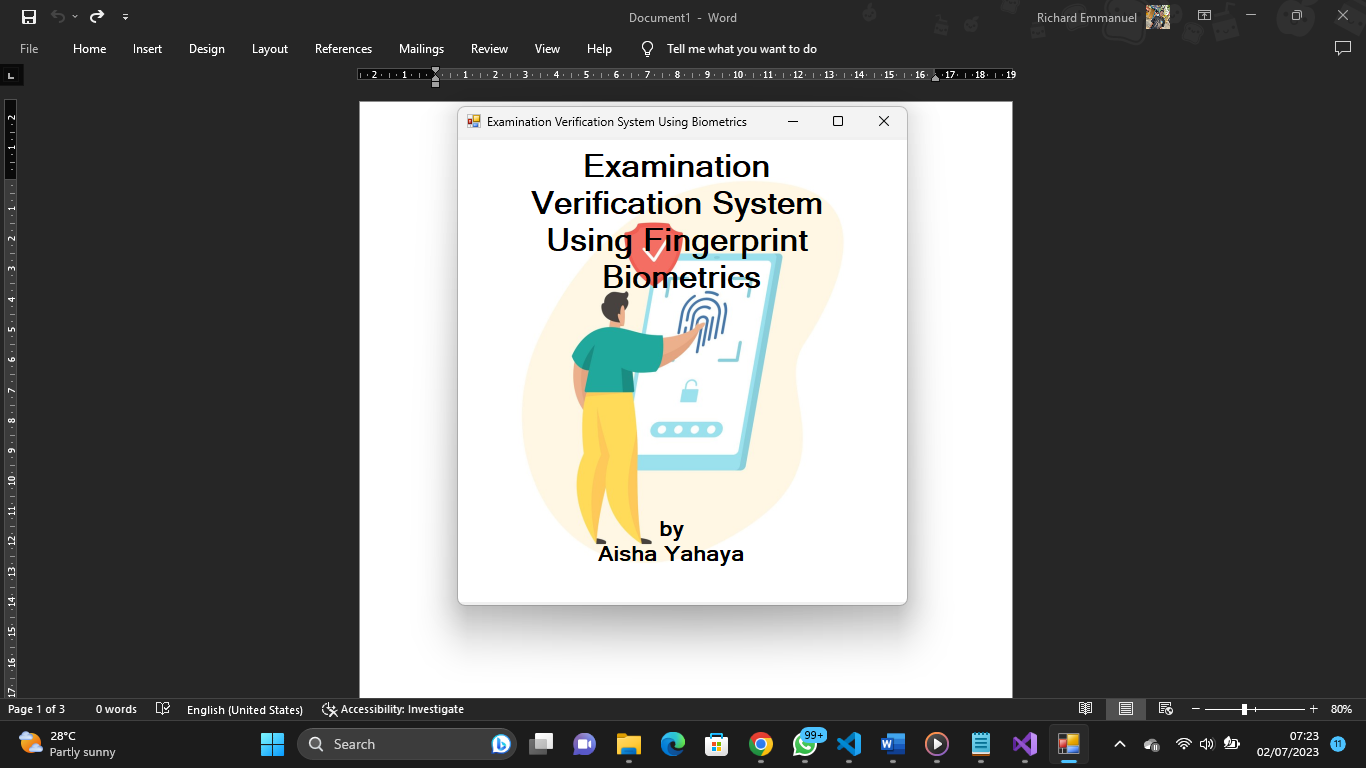
**4.4 Security Measures**

The application has a public scope, allowing exam invigilators to access the available information. However, certain functionalities are restricted to the admin, such as registering the students and invigilators. Access to these restricted functionalities is protected by passwords, ensuring that only authorized individuals can access the admin pages. Additionally, certain functionalities within the application may be restricted based on the specific user type, providing tailored access and permissions as needed.

**4.6 Sample Outputs**

These describe and give the pictorial representation of the program or software; it shows and gives a clear understanding of the design, and displays all the interfaces.

**4.6.1 Splash Screen**

 This is the first screen displayed to every user that wishes to make use of the application

.

Fig 4.6.1: Homepage

**4.6.2 Login Screen**

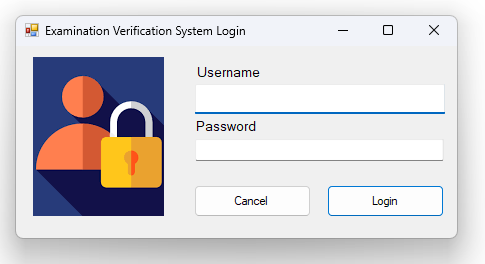
****The screen grants users access (invigilators, admin) to the application only if the correct credentials are provided

Fig 4.6.2 Login Screen

**4.6.3 Admin Main Menu**

The screen presents the various functionalities that can be performed by an admin

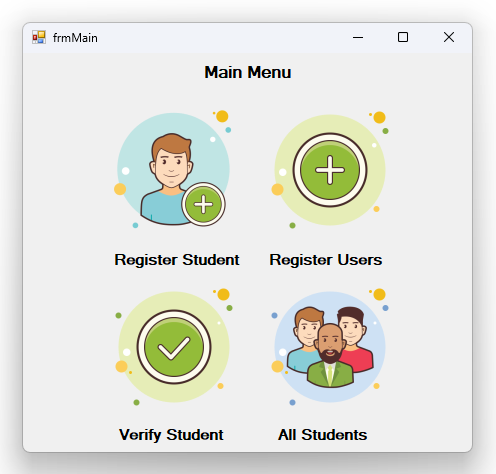
****

Fig 4.6.3 Admin Main Menu

**4.6.4 Register Student**

The screen present a form that is used to register student, this is where the fingerprints of the students are captured, and vital information that can be used for verification are collected

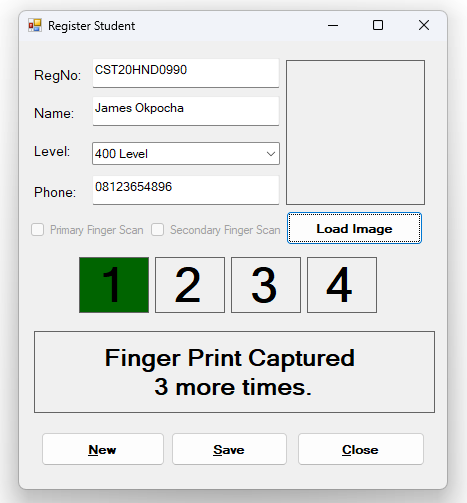


Fig 4.6.3 Register Student

**4.6.4 Register System Users**

The screen present a form to create an account for either the admin or the invigilators

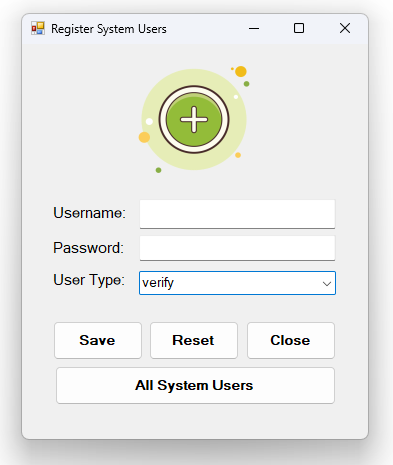
****

Fig 4.6.4 Register System Users

**4.6.5 All Register Students**

The screen present a list of all student where delete operation can be performed on any of the student

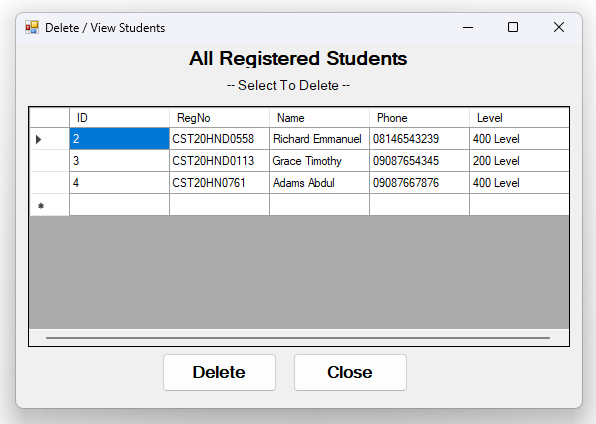


Fig 4.6.5 Register System Users

**4.6.6 Student Verification Screen**

It is on the screen that students are verified, it await the recognition of any placed finger, if recognized the details of the student displays otherwise the appropriate message is displayed

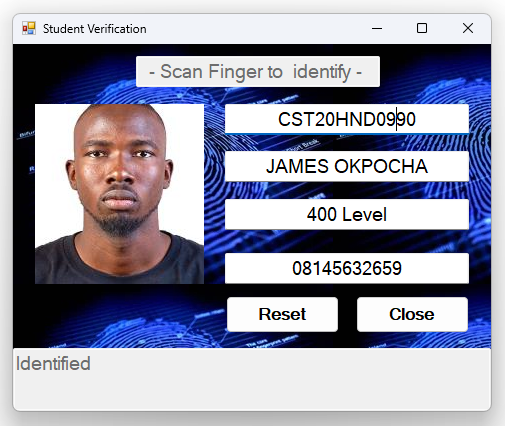


Fig 4.6.6 Student Verification Screen

**4.6.7 Invigilator Main Menu**

The screen presents the various functionalities that can be performed by an invigilator

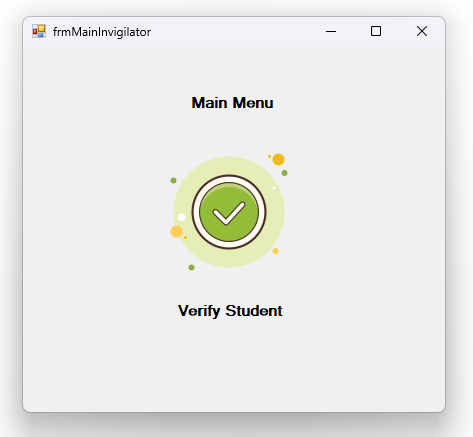
****

Fig 4.6.7 Invigilator Main Menu

**CHAPTER FIVE**

**Summary Conclusion and Recommendation**

**5.1 Summary**

The research focuses on developing an examination verification system using biometrics for the Department of Computer Science at Kaduna Polytechnic. The system aims to address the issue of exam impersonation by implementing advanced biometric technologies, specifically fingerprint identification. By incorporating this system, the goal is to enhance the security and integrity of the examination process, ensuring that only authorized students are allowed to take the exams. This innovative solution will significantly reduce fraudulent activities and promote a fair and transparent evaluation system.

**5.2 Conclusion**

In conclusion, the research project has successfully explored the development of an examination verification system using biometrics for the Department of Computer Science at Kaduna Polytechnic. By leveraging the power of fingerprint identification, the system aims to combat exam impersonation and enhance the overall security of the examination process. Through the implementation of this innovative solution, the integrity and fairness of the evaluation system will be strengthened, ensuring that only authorized students can participate in exams. The utilization of biometric technology offers a robust and reliable method for verifying student identities, mitigating the risks associated with fraudulent activities. With the introduction of this system, Kaduna Polytechnic can create a more secure and trustworthy environment for conducting examinations.

**5.2 Recommendation**

Based on the findings of the research, the following recommendations are made:

1. Implementation of the Examination Verification System: The Department of Computer Science at Kaduna Polytechnic should proceed with the implementation of the examination verification system using biometrics. This system will enhance the security and integrity of the examination process by ensuring that only authorized students are allowed to participate.
2. Regular System Maintenance and Updates: The examination verification system should be regularly maintained and updated to ensure its optimal performance. This includes routine checks on the biometric devices, software updates, and data backups.
3. Continuous Evaluation and Improvement: The implementation of the biometric verification system should be accompanied by a continuous evaluation process. Feedback from students and staff should be gathered to identify any areas of improvement and address any challenges or issues that may arise. This will help in refining the system and ensuring its effectiveness in the long run.

By following these recommendations, the Department of Computer Science at Kaduna Polytechnic can enhance the examination process, strengthen security measures, and create a more reliable and trustworthy environment for conducting exams.

**REFERENCES**

Garko, A. B., & Ahmad, A. (2017). Design and modelling of a student verification system in an

examination in Nigeria. *International Journal of Advanced Academic Research*, *3*(7), 1-16.https://www.mendeley.com/catalogue/a08dd69f-537a-3f19-b2563cf37987f014/#abstract-title

Haruna, U. S. (2018). sVeriTool: A Verification Tool for Preventing Impersonation of Students

in Examination Halls using Fingerprints. *SVeriTool African Journal of Computing & ICT Reference Format: U. S. Haruna*, *11*(2), 37–52.

https://afrjcict.net

Ojo, O., Yekini. N. A., Aigbokhan., E. E., & Onadokun, I. (2019). Deterring Malpractice in a

Networked Computer Based Examination Using Biometric Control Attendance Register. *International Journal of Advanced Networking Applications, 10*(06), 4061–4064. https://doi.org/10.35444/ijana.2019.10062

Math, D. & Prasanna, K. M. (2019). Bio-Metric Enabled Examination Student Verification

System. *International Journal for Research in Applied Science and Engineering Technology, 7*(1), 603–610.

https://doi.org/10.22214/ijraset.2019.1097

Traoré, I., Nakkabi, Y., Saad, S., Sayed, B., Ardigo, J.D., de Faria Quinan, P.M. (2017). Ensuring

Online Exam Integrity Through Continuous Biometric Authentication. In: Traoré, I., Awad, A., Woungang, I. (eds) Information Security Practices. Springer, Cham. https://doi.org/10.1007/978-3-319-48947-6\_6

**APPENDIX**

**Verify.frm**

Imports Neuro.Business

Imports DPUruNet

Imports DPUruNet.Constants

Imports System.IO

Public Class frmVerify

    Dim ds, ds1 As DataSet

    Dim dsFingerPrint As DataSet

    Dim userIDlist1 As List(Of Integer) = New List(Of Integer)

    Dim userIDlist2 As List(Of Integer) = New List(Of Integer)

    Dim fmdListFP1 As List(Of Fmd) = New List(Of Fmd)

    Dim fmdListFP2 As List(Of Fmd) = New List(Of Fmd)

    Dim fmds As New List(Of Fmd)

    Dim fpReader As DPUruNet.Reader

    Private Sub frmVerify\_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles MyBase.Load

        Try

            dsFingerPrint = New DataSet

            dsFingerPrint = VerifyManager.getStudentFingerPrintData

        Catch ex As Exception

            MsgBox(ex.Message)

            Return

        End Try

        Try

            For Each dr As DataRow In dsFingerPrint.Tables(0).Rows

                If Not IsDBNull(dr("FingerPrint1")) Then

                    Dim printXML As String = dr("FingerPrint1")

                    fmdListFP1.Add(Fmd.DeserializeXml(printXML))

                    userIDlist1.Add(dr("ID"))

                End If

                If Not IsDBNull(dr("FingerPrint2")) Then

                    Dim printXML As String = dr("FingerPrint2")

                    fmdListFP2.Add(Fmd.DeserializeXml(printXML))

                    userIDlist2.Add(dr("ID"))

                End If

            Next

        Catch ex As Exception

        End Try

        Indentify()

    End Sub

        Try

            GetStatus(fpReader)

        Catch ex As Exception

            MsgBox(ex.Message, MsgBoxStyle.Exclamation, "Error!")

            Return

        End Try

        fmds.Clear()

        Dim captureCallBack As Reader.CaptureCallback

        captureCallBack = New Reader.CaptureCallback(AddressOf onCapture)

        AddHandler fpReader.On\_Captured, captureCallBack

        result = fpReader.CaptureAsync(Formats.Fid.ANSI, CaptureProcessing.DP\_IMG\_PROC\_DEFAULT, 500)

        If result <> ResultCode.DP\_SUCCESS Then

            MsgBox("Error starting capture")

            Return

        End If

    End Sub

        If captureResult.Quality = CaptureQuality.DP\_QUALITY\_FAKE\_FINGER Then

            BeginInvoke(Function()

                            lblInfo.Text = "Capture failed due to fake finger detection. " & vbCrLf & "try again." & captureResult.ResultCode.ToString()

                            Return True

                        End Function)

            Return

        End If

        Dim resultConversion As DataResult(Of Fmd) = FeatureExtraction.CreateFmdFromFid(captureResult.Data, Formats.Fmd.DP\_VERIFICATION)

        If resultConversion.ResultCode <> ResultCode.DP\_SUCCESS Then

            BeginInvoke(Function()

                            lblInfo.Text = "Could not create fmd." & captureResult.ResultCode.ToString()

                            Return True

                        End Function)

            Return

        End If

        BeginInvoke(Function()

                        Me.txtLevel.Text = Nothing

                        Me.txtPhone.Text = Nothing

                        Me.txtStudName.Text = Nothing

                        Me.txtRegNo.Text = Nothing

                        Me.studImage.Image = Nothing

                        Me.lblInfo.Text = "Awaiting Fingerprint...."

                        Return True

                    End Function)

        Dim idResult As IdentifyResult

        If (fmdListFP1.Count > 0) Then

            idResult = Comparison.Identify(resultConversion.Data, 0, fmdListFP1, &H7FFFFFFF / 100000, 4)

            If idResult.ResultCode <> ResultCode.DP\_SUCCESS Then

                BeginInvoke(Function()

                                lblInfo.Text = "Unable to Identify, scan different. finger"

                                Return True

                            End Function)

                Return

            End If

            If (idResult.Indexes.Length >= 1) Then

                BeginInvoke(Function()

                                Try

                                    ds1 = New DataSet

                                    ds1 = VerifyManager.getStudentInformationByID(userIDlist1(idResult.Indexes(0)(0)))

                                    Try

                                        Dim b() As Byte = ds1.Tables(0)(0)("StudentImage")

                                        Me.studImage.Image = Image.FromStream(New MemoryStream(b))

                                    Catch ex As Exception

                                    End Try

                                    Me.txtRegNo.Text = ds1.Tables(0)(0)("RegNo")

                                    Me.txtStudName.Text = ds1.Tables(0)(0)("Name")

                                    Me.txtPhone.Text = ds1.Tables(0)(0)("Phone")

                                    Me.txtLevel.Text = ds1.Tables(0)(0)("Level")

                                    Me.lblInfo.Text = "Identified"

                                Catch ex As Exception

                                    lblInfo.Text = "Can not Identified"

                                End Try

                                Return True

                            End Function)

                Return

            End If

        End If

        If (fmdListFP2.Count > 0) Then

            idResult = Comparison.Identify(resultConversion.Data, 0, fmdListFP2, &H7FFFFFFF / 100000, 4)

            If idResult.ResultCode <> ResultCode.DP\_SUCCESS Then

                BeginInvoke(Function()

                                lblInfo.Text = "Unable to Identify, scan different. finger"

                                Return True

                            End Function)

                Return

            End If

            If (idResult.Indexes.Length >= 1) Then

                BeginInvoke(Function()

                                Try

                                    ds1 = New DataSet

                                    ds1 = VerifyManager.getStudentInformationByID(userIDlist2(idResult.Indexes(0)(0)))

                                    Try

                                        Dim b() As Byte = ds1.Tables(0)(0)("StudentImage")

                                        Me.studImage.Image = Image.FromStream(New MemoryStream(b))

                                    Catch ex As Exception

                                    End Try

                                    Me.txtRegNo.Text = ds1.Tables(0)(0)("RegNo")

                                    Me.txtStudName.Text = ds1.Tables(0)(0)("Name")

                                    Me.txtPhone.Text = ds1.Tables(0)(0)("Phone")

                                    Me.txtLevel.Text = ds1.Tables(0)(0)("Level")

                                    Me.lblInfo.Text = "Identified"

                                Catch ex As Exception

                                    lblInfo.Text = "Can not Identified"

                                End Try

                                Return True

                            End Function)

                Return

            End If

        End If

    End Sub

    Private Sub GetStatus(ByVal currentReader As DPUruNet.Reader)

        Dim result = currentReader.GetStatus

        If result <> ResultCode.DP\_SUCCESS Then

            Throw New Exception(result.ToString())

        End If

        If currentReader.Status.Status = ReaderStatuses.DP\_STATUS\_BUSY Then

            Threading.Thread.Sleep(50)

        ElseIf currentReader.Status.Status = ReaderStatuses.DP\_STATUS\_NEED\_CALIBRATION Then

            currentReader.Calibrate()

        ElseIf currentReader.Status.Status <> ReaderStatuses.DP\_STATUS\_READY Then

            Throw New Exception("Reader Status - " & currentReader.Status.Status.ToString())

        End If

    End Sub

    Private Sub btnReset\_Click(sender As Object, e As EventArgs) Handles btnReset.Click

        Me.txtLevel.Text = Nothing

        Me.txtPhone.Text = Nothing

        Me.txtStudName.Text = Nothing

        Me.txtRegNo.Text = Nothing

        Me.studImage.Image = Nothing

        Me.lblInfo.Text = "Awaiting Fingerprint...."

    End Sub

    Private Sub btnClose\_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles btnClose.Click

        Try

            fpReader.CancelCapture()

            fpReader.Dispose()

        Catch ex As Exception

        End Try

        Me.Close()

    End Sub

End Class