International Journal of Advanced Research in Physical Science (IJARPS)
Volume 3, Issue 5, 2016, PP 29-39
ISSN 2349-7874 (Print) & ISSN 2349-7882 (Online)
www.arcjournals.org

Design and Construction of a Biometric Examination Authentication Device

Ogherohwo E.P[1], Ezeoba E.O.[2]

Department of Physics, University of Jos, Plateau State, Nigeria

Abstract: *Although student's performance in examination may not be the true reflection of their ability, examination still remains the best tool for an objective assessment and evaluation of what a learner has achieved after a period of training. The menace of examination malpractice in our education system at all levels has compromised the integrity of our educational system. The need to use a unique, measurable and universal marker to identify every student for an examination arises especially in large classes, where facial recognition may not be practical or effective. This reduces, or completely eliminating examination malpractice by impersonation.*

This project designed and constructed a biometric device to be used for the authentication of the student's eligibility for an examination. The system requires that the students, during their registration for a particular course will have their finger prints taken and registered against their name. Subsequently, during an examination or a test, the students are verified using their finger prints. The system was also designed with an external display unit, which displays information about the validity of the finger scan.

Keywords: *design, construction, biometric, examination, authentication*

1. Introduction

The term "Biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure) (Rood and Hornak, 2008). Biometrics is referred to measurements related to human characteristics. They are biological pieces of information that are peculiar to an individual. They have been introduced to modern technology as forms of identification and access control. Biometric identifiers are the distinctive and measurable characteristics used to label (distinguish between individuals) and describe individuals (Jain, Hong and Pankanti 2000). They are often categorized as physiological and behavioral characteristics (*Anil and Arun, 2008*). Physiological characteristics are related to the shape of the body. Examples include, fingerprint, palm veins, face recognition, deoxyribonucleic acid (DNA), palm print, hand geometry, iris/retina pattern, and body scent, while behavioral characteristics are acquired traits possessed by an individual and are related to the pattern of behavior of a person. They include typing rhythm, manner of walking, temperament and voice (Sahidullah, 2015).

Of the two biometric identifiers, the physiological characteristics are the most utilized in modern technologies. The use of fingerprints, palm prints, DNA and facial recognition in the identification of criminals are the most frequently applied techniques in forensic science. Fingerprint evidence is one of the most reliable forms of identification, even though there are challenges to its use. However, these problems or errors can be neglected compared to the outstanding history of success recorded in using biometrics in identifying individuals. (Jackson and Jackson, 2008). Uludag, Pankanti and Prabhakar (2004) defined biometric technique as an automated methodology for the recognition of a person based on behavioral or physiological characteristics. These characteristics include features such as hand geometry, handwriting, face, fingerprints, vein, voice, retina, and iris. He concluded that biometric technologies are now the key to an extensive array of highly secured identification and personal verification solutions.

The earliest form of conscious use of Biometrics appeared on the scene back in the 1800's (Duane, 2004). Alphonse Bertillon, a French anthropologist and police desk clerk, developed a method for identifying criminals that was known as Bertillonage (Duane, 2004). This system was a form of anthropometry (the study of human body measurement), a system by which measurements of the body are taken for classification and comparison purposes. Bertillon's system of anthropometry required numerous and precise measurements of the bony parts of a humans anatomy for identification. It also involves recording shapes of the body and differential markings on the surface of the body such as scars, birth marks, tattoos, etc. (Ted, 2011). Bertillon’s system of identification was not without fault. For example, it relied heavily on precise measurements for identification purposes, and yet two people working on measurements for the same person would record different findings. The measurements taken were also thought to be unique and accurate in adulthood. Therefore, someone who committed a crime prior to adulthood would not have their measurements on record. Additionally, it turned out to be the case that the features by which Bertillon based his identification system were not unique to any one individual. With this, it is possible for one person to be convicted of another person’s crime. This possibility became abundantly clear in 1903 when a Will West was confused with a William West, who was later found out to be identical twins (Ted, 2011).

Because of the amount of time and effort that went into collecting measurements and the overall inaccuracy of the process, Alphonse Bertillon’s system was quickly replaced when fingerprinting emerged on the scene as a more efficient and accurate means of identification. Finger printing, as a means of identification, proved to be infallible. It was accepted that each individual possessed a uniquely identifiable and unchanging fingerprint. This new system of identification was accepted as more reliable than Alphonse Bertillon’s system (Aviation Security).

Fingerprinting can be traced as far back as the 14th century in China (Patricia, Janusz and Witold 2009). Though, the use was most likely as a signature but the unique identification ability of the fingerprint was not entirely known. Fingerprints were first looked at as a form of criminal identification by Dr. Henry Fauld’s who noticed fingerprints on ancient pottery while working in Tokyo (Patricia, Janusz and Witold, 2009). He first published his ideas about using fingerprints as a means of identifying criminals in the scientific journal, ***Nature*** in 1880. William Herschel, while working in colonial India, also recognized the unique qualities that fingerprints had to offer as a means of identification in the late 1870's. He started using fingerprints as a form of signature on contracts with locals (Komarinski, 2004). Sir Francis Galton, who had been informed of Fauld’s research through his uncle, Charles Darwin, would also be credited as making significant advancement to fingerprint identification. Galton ascertained that no two fingerprints were alike, not even on a set of identical twins (Patricia, Janusz and Witold, 2009). He noted that differentiating characteristics could be best observed in the ridge of a fingerprint and that this fingerprint would remain reliable and unchanging and could be used for identification throughout an individual’s life time. However, it had never been officially recognized as to which of these three men was the first to discover fingerprinting as a means of identification.

The Henry’s Classification system, named after Edward Henry who developed and first implemented the system in 1897 in India, was the first method of classification for fingerprint identification based on physiological characteristics. The system assigns each individual finger a numerical value (starting with the right thumb and ending with the left pinky) and divides fingerprint records into groupings based on pattern types. The system makes it possible to search large numbers of fingerprint records by classifying the prints according to whether they have an "arch," "whorl," or "loop".

Examination is defined as a formal test of one's knowledge or ability in a particular subject especially by means of answering questions or practical exercises (Benard, 1998). Therefore, it is through examination that students are evaluated or tested to find out the quality and quantity of knowledge they have acquired within a specific period. Thus, examination could be either internal, external, oral, written or both. Continuous assessment scores, terminal, semester, annual or promotion examinations are examples of internal examinations (Benard, 1998).

Although student’s performance in examination may not be the true reflection of their ability, up till now, examination still remains the best tool for an objective assessment and evaluation of what a learner has achieved after a period of schooling/training. In fact, it is one of the most reliable indicators used to determine the extent of students' performance in a given training.

Examination malpractice is not a new phenomenon in Nigeria. The first examination malpractice in Nigeria occurred in 1914 during the Senior Cambridge Local Examination papers which were leaked before the scheduled date of examination (Maduemezia, 1998). Thus, examination malpractice which started at a low trend became more pronounced in 1970, involving persons other than the candidates. Since then examination malpractice became more advanced and sophisticated. Examination malpractice is an illegal act committed by a single student or in collaboration with others like fellow students, parents, teachers, supervisors, invigilators, computer operators or secretarial staff and anybody or group of people before, during, or after examination in order to obtain undeserved marks or grades (Awanbor, 2004).

In recent times, examination malpractice has gone from simple ‘giraffing’ where students occasionally stretch their necks to catch glimpse of what they want to copy from other students scripts to a variety of sophisticated ones. These include;

i. Use of ‘Micro-chip’: writing very tiny summaries on pieces of paper, parts of the body, or on material is found within the venue.

ii. Sorting: in which students negotiate with corrupt examiners for scores by rewarding the examiners in cash or kind.

iii. ECOMOG/ECOWAS/OAU: This is an alliance among classmates, to communicate via coded language during the examinations.

iv. Hand-held smart devices such as modern cell phones.

It has developed to the level where friends can impersonate their friends and sit for an exam for them. These irregularities have in no doubt posed a vital question on the credibility of the examination system and standard.

The examination bodies like the schools have not turned a blind eye to all these practices and have introduced various policies like strict invigilation of the students during the examination exercise to cut down student’s communication during the examinations. Also, the spacing pattern during the examination is aimed at reducing any form of communication amongst students, even “girrafing”. Institutions have gone as far as motivating the examiners and encourage them to cut down the excesses of the students during the examination.

However, in a very large class like PHY202 in university of Jos, having a number of examination candidates averaging about 400 to 450 students, it has been discovered that some of these policies against examination malpractices introduced by the institutions may not be so effective due to the large number of students.

Take for instance, in a PHY202 examination, due to the number of students and the limited number of halls, the examiners may not be able to check all the excesses of the students. They examiners may also have to reduce the spacing between the candidates so that the hall will accommodate their large number. Because of the largeness of the class size, the students can maneuver the process and friends get to sign for each other in the absence of their colleagues. This practice goes to the extent of students writing examinations for each other because there is no way the examiner will know the eligible student facially.

This project is geared towards harnessing the idea in modern biometric security technologies to authenticate the eligibility of a student to sit for an examination. This can be achieved by taking the fingerprint of whoever that will be coming to register the course. The project would help stop the practice of students sitting for examination for their friends to some extent.

The term fingerprint is used to describe a reproduction of the friction ridge arrangement present on the tips of the fingers when an impression is deposited on a touched surface. This arrangement of the friction ridge skin is permanent due to the underlying structure of the skin and unique because of complex physiological events, both genetic and environmental, that occur during fetal development.

Jain and Uludag (2003) noted that an ideal biometrics system should be universal, unique, permanent and collectable. It must be universal that every person possesses the characteristic, uniqueness; where no two persons share the characteristic, permanency; where the characteristic should neither be changed nor be alterable; and finally the characteristics must be collectable and be readily presentable to a sensor and is easily quantifiable. The finger print satisfies these conditions for an ideal biometrics. No two fingerprints can have the same print, and it is an overwhelming mathematical probability that two fingers will ever match. The ridge pattern is formed in the human fetus before birth and remains the same throughout a person’s life and even after death until they are lost through decomposition. Moreover, fingerprints are made up of a number of easily recognizable features that permit them to be classified

Research on biometric methods has gained renewed attention in recent times which has necessitated increase in security awareness. The world attitude in recent times towards terrorism has influenced people and their governments to take action and be more proactive in security issues. The need for security also extends to the need for individuals to protect, among other things, their working environments, homes, personal possessions and assets. The technologies used in these security systems are now being employed to serve other purposes such as authentication as in the case of this project. Many biometric techniques have been developed and are being improved upon with the most successful being applied in everyday law enforcement and security applications. Fingerprint recognition is considered to be one of the most powerful techniques for utmost security authentication.

Welzl (2004) states that the biometric system is a pattern recognition technology that makes personal identification of an individual by determining the authenticity of a specific physiological or behavioral characteristics possessed by the user.

Jain and Uludag (2003) described the significant differences between the physiological and behavioral biometrics. The physiological biometrics consists of measurements and data collected from direct measurement of a part of the human body. Samples of these include hand geometry, facial recognition, fingerprint, iris pattern, etc. On the other hand, the behavioral characteristics originate from the actions of an individual, and it indirectly measures unique characteristics of the human body. Samples of these include signature-scan, keystroke-scan, voice recognition, etc. Time can act as a metric for behavioral biometrics, because it measures behavior by considering the timeline of a given process (Ratha, Connell and Bolle, 2001).

Automated biometric systems have only become available over the last few decades, due to the significant advances in the field of computer and image processing.

Today, the focus is on using biometric; face recognition, iris recognition, retina recognition, thumb prints and other identifying characteristics to verify and authenticate an individual’s identity.

There are five stages involved in finger-scan enrolment and identification: Fingerprint image acquisition, Image processing, Location of distinctive characteristics, Template creation and Template matching (Asha, 2012).

A scanner (sensor) takes a mathematical snapshot of a user's unique biological traits. This snapshot is saved in a fingerprint database as a minutiae file. The first challenge facing a finger-scanning system is to acquire high-quality image of a fingerprint. Image acquisition can be a major challenge for finger scanner, since the quality of print differs from person to person and from finger to finger. Some populations are more likely than others to have faint fingerprints, due to wear or tear or physiological traits.

Image processing is the process of converting the finger image into a usable format. This results in a series of thick black ridges (the raised part of the fingerprint) contrasted to white valleys. At this stage, image features are detected and enhanced for verification against the stored minutia file. Image enhancement is used to reduce any distortion of the fingerprint caused by dirt, cuts, scars, sweat and dry skin.

The next stage in the fingerprint process is to locate distinctive characteristics. There is a good deal of information on the average fingerprint and this information tends to remain stable throughout one’s life. Fingerprint ridges and valleys form distinctive patterns which can be categorized as whorl, loops, and arches.

Most fingerprints have a core, a central point around which whorls, loops, or arches are curved. These ridges and valleys are characterized by irregularities known as minutiae, the distinctive feature upon which finger scanning technologies are based. Template of the minutiae is then created, which is accomplished by mapping minutiae and filtering out distortions and false minutiae. For example, anomalies caused by scars, sweat, or dirt can appear as minutiae. False minutiae must be filtered out before a template is created.

In comparing an enrollment template to a verification template, positions of a minutia point may change by a few pixels, some minutiae will differ from the enrollment template, and false minutiae may be seen as real. Many finger-scan systems use a smaller portion of the scanned image for matching purposes. One benefit of reducing the comparison area is that there is less chance of false minutiae information, which would confuse the matching process and create errors.

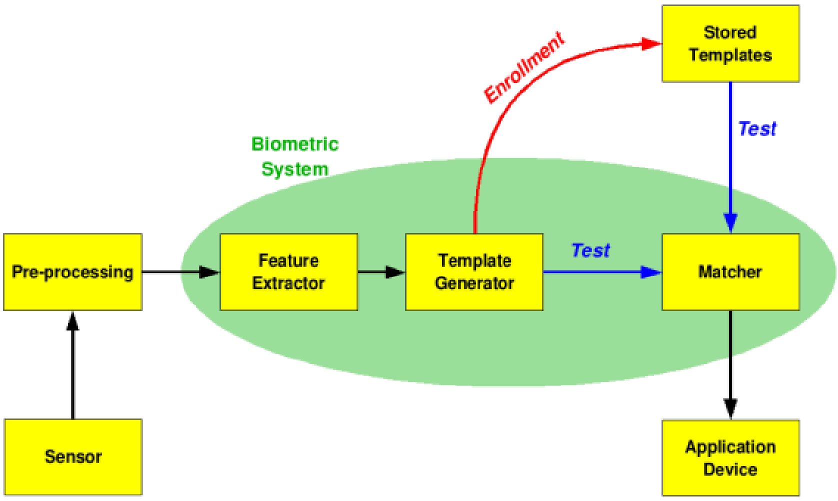


Figure2.1. *Stages of operation of a biometric system*

2. Materials and Methodology

Materials used for the construction of a Biometric Examination Authentication Device are as follows; Resistors, Transistors, Capacitors, Crystal oscillators, PIC16F628A microcontroller, an LCD unit.

2.1. Design Stages

Power supply (5vdc)

The device is designed to draw its power supply from the USB port of the laptop through a USB cable. This supplies a constant 5vdc to the device which is appropriate for optimum operation. The power supply could be designed to be from a external source like DC batteries, but this may make the device more cumbersome.

Signal Amplification

One of the most powerful transistor applications involves amplification: turning a low power signal into one of higher power. Amplifiers can increase the voltage of a signal, taking something from the µV range and converting it to a more useful mV or V level. Transistors can also amplify current. It can amplify µA of current produced by a photodiode into a current of much higher in magnitude. Transistors are a key component to many amplifying circuits.

The aim of the small signal amplifier is to amplify all of the input signal with the minimum amount of distortion possible to the output signal, in other words, the output signal must be an exact reproduction of the input signal but only bigger (amplified).

In this project, the amplifier sections functions to amplify signals coming from the module through the laptop to the microcontroller. There is also a reverse amplifier that functions to amplify signals from the microcontroller to the laptop. This is necessary for the very little signal coming directly from the serial port of the laptop and the output pins of the microcontroller. The amplifier is operated in the common emitter mode due to the following reasons; it has a very high voltage gain and the highest power gain amongst other configurations of amplifier.

The collector emitter voltage, V_{CE} =0.25volts (max). This value is gotten from the data sheet of the C1815 transistor. The collector current, I_C was measured to be 4.82mA. The voltage supply V_{CC} is 5volts.

To calculate the biasing resistor for the collector, I applied Kirchhoff's voltage law on the collector circuit.

$$V_{CC} = V_{CE} + I_C R_C \qquad 2.1.1$$

$$R_C = \frac{V_{CC} - V_{CE}}{I_C} \qquad 2.1.2$$

Substituting the values into the expression above, I found the biasing resistor of the collector to be:

$$R_C = \frac{5 - 0.25}{5.07 \times 10^{-3}} = 936.88\Omega$$

I approximated this value of resistance to 1000Ω. Therefore, I used a 1kΩ resistor to bias the collector of the transistors.

The base emitter voltage, V_{BE} has a maximum expected value of 1volt according to the specifications on the data sheet of the transistor. The signal voltage from the serial port is 3volts and the base current, I_B is measured to be 204.31µA. To calculate the value of the base resistor R_B, we apply the Kirchhoff's voltage law on the base circuit.

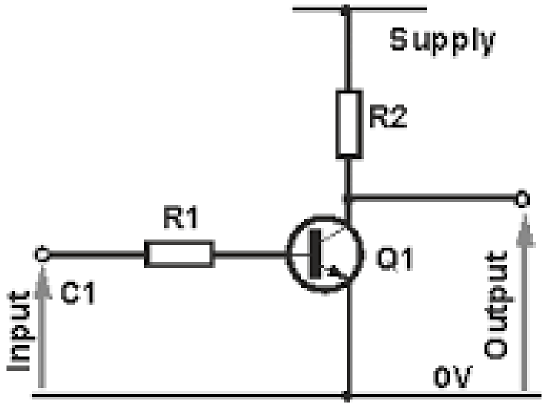
$$R_B = V_{BE} + I_B R_B \qquad 3.5$$

$$R_B = \frac{V_{BB} - V_{BE}}{I_B} \qquad 3.6$$

Substituting the values into the expression above, I found the value of the base resistor to be;

$$R_B = \frac{3 - 1}{204.31 \times 10^{-6}} = 9789\Omega$$

I approximated this value to 10,000 Ω. Therefore, I used 10k resistor as the biasing resistor for the base of the transistor.



Oscillation

Electronic components such as crystal oscillator can be used to generate electrical signals of precise frequency by utilizing the vibrating crystals mechanical resonance made of piezoelectric material. Crystal oscillator circuit work on the principle of inverse electric effect. It is the mechanical deformation of the crystal material is produced by applying an electric field across the material. Thus, it utilizes the vibrating crystals mechanical resonance which is made up of a piezoelectric material for generating an electrical signal of a specific frequency. The quartz crystal oscillators are highly stable and precise. This is to keep the microcontroller vibrating at a specific frequency. This is very important because of the sensitivity of the device. Crystals are usually used in conjunction with a phase locked loop circuit to provide the required system clock frequency. The maximum clock frequency of the microcontroller is 20MHz. Load capacitance, C_L refers to the capacitance external to the feedback loop of the oscillator circuit.

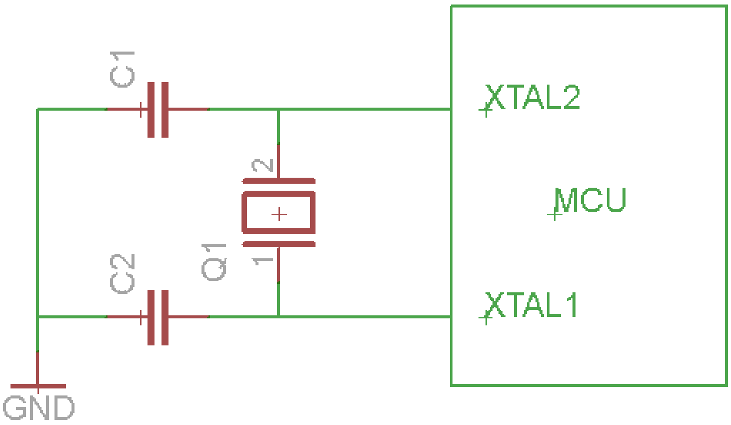
Using a crystal of 4MHz, this is still in the range of the requirement of the microcontroller, and a set load capacitance of 18pf (within range on the data sheet), I calculated the value of the external load capacitors, C using the formula:

$C = 2C_L - C_{stray}$ (Atmel AVR042, pp12), where $C_1 = C_2 = C$

Stray capacitance, C_{stray} is an unavoidable and usually unwanted capacitance that exists between the parts of an electronic component or circuit simply because of their proximity to each other. Its value ranges from 2 to 5 pF. Taking C_{stray} = 3pF and substituting into the above expression, we now have:

C = (2 x 18) -3 = 33pF.

Therefore, the external capacitors, C = C_1 =C_2 33pF



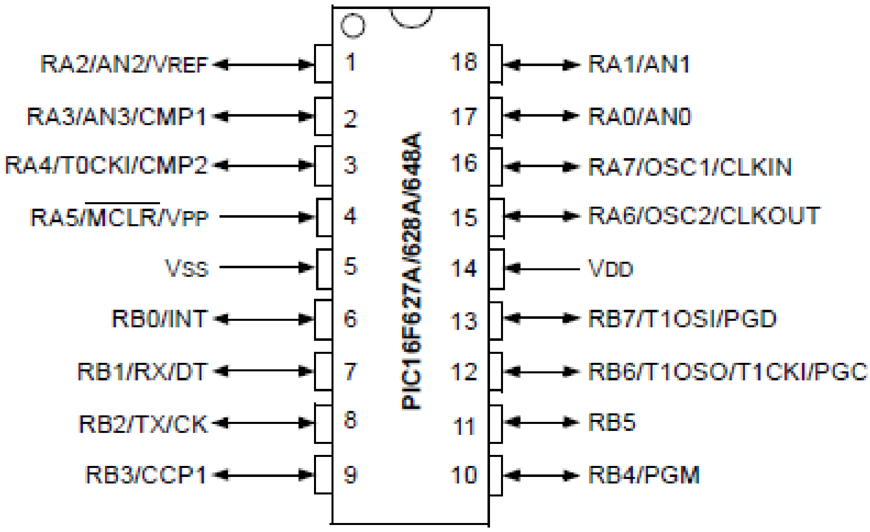
The Microcontroller

The device is design is such a way that the microcontroller which has been programmed communicates with the fingerprint scanner through the serial port of the computer (pin 2) and also gets feedback through the same port (pin 3). Pin 7 of the microcontroller is programmed to receive information about a student’s fingerprint, be it during registration or verification. The signal is sent from pin 2 of the serial port of the computer and then amplified by the transistor before it is processed by the microcontroller and displayed. The same process is repeated when the operation sequence is read on the microcontroller. The signal is sent from pin 8, amplified by the transistor and then sent to pin 3 of the serial port. Pin 5 of the serial port is grounded.

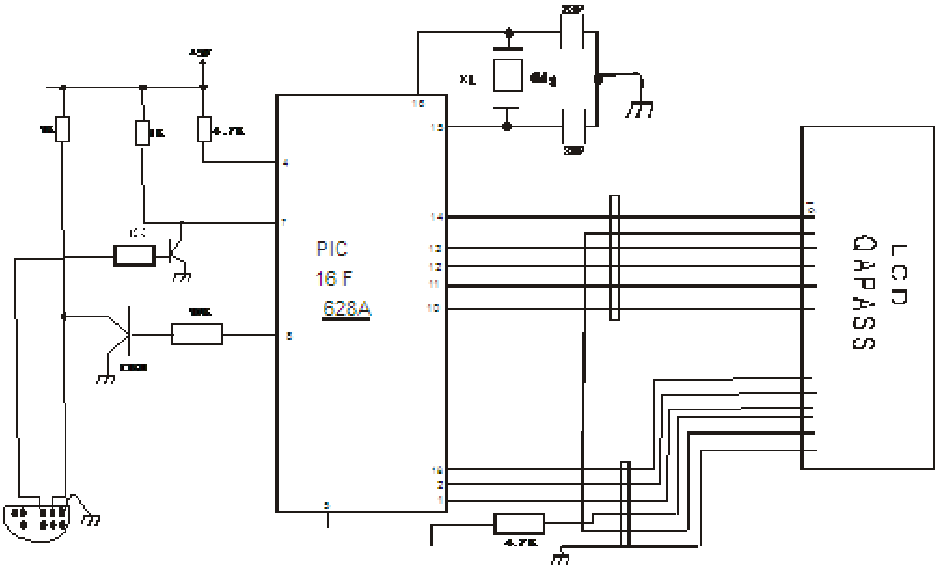
From the data sheet of PIC16f628A microcontroller, pin 4 can function as the reset, master clear or the programming or operation voltage pin of the microcontroller. This pin has been designed by its manufactures to perform this function. In the circuit, pin 4 is functioning as the controller voltage source V_{pp} of 5V. Again, pin 5 is labeled V_{ss} by the manufacture and is thus grounded together with the emitter of the transistors.

Also, pin 15 and 16 of the microcontroller is labeled OSC1/CLKIN1 and OSC2/CLKIN2 respectively and is thus connected to an external crystal. Because the internal clock or oscillator of the microcontroller can be affected by external factors, the need for a crystal in the clock pins. Crystals also provide much more accurate resonation during communication because of the timing that is required for effective communication. Therefore, to achieve stability, an external crystal will be needed to set the clocks to a precise frequency. The crystal oscillator is used to generate clock pulses required for the synchronization of all the internal operation of the microcontroller.

From the data sheet of PIC16f628A, it can be seen that pins 1, 2, 10, 11,12,13,14 and 18 are bidirectional input/output ports and have been used in this project to send output data to the display screen.



Complete Circuit Diagram



3. Result

The following results were obtained when the device was used to register 20 students for 4 different courses. Graphical representation of the result for each course is also given using the name initials of each student.

Table3.1. *Results obtained from Phy401 students*

Name of Student	Mat. Number	Registration Status	Display on screen
Ezeoba Emmanuel Onyeka.401	UJ/2011/NS/0035	registered	student verified
Ani Basil Emeka.401	UJ/2012/NS/0496	registered	student verified
Ejiro Oghenechovwen.401	UJ/2011/NS/0712	registered	student verified
Obikili Jennifer Chioma.401	UJ/2011/NS/680	registered	student verified
Reuben Samson Dawah.401	UJ/2011/NS/0403	registered	student verified
Oheitonye Ejembi Boniface.401	UJ/2011/NS/0078	registered	student verified
Saba M. Dabilong.401	UJ/2011/NS/0453	registered	student verified
Ekeakhogbe Gloria Omonye.401	UJ/2011/NS/0444	registered	student verified
Owoeye Peter Emmanuel.401	UJ/2011/NS/0154	registered	student verified
James Nanfwang.401	UJ/2011/NS/0780	registered	student verified
Kwada Douglas.401	UJ/2011/NS/0505	registered	student verified
Olushola Kemi Joyce.401	UJ/2011/NS/0413	registered	student verified
Pam Victor.401	UJ/2011/NS/0162	registered	student verified
George Abel Inadu.401	UJ/2011/NS/0394	registered	student verified
Tarkumbul Ladi Sharon.401	UJ/2011/NS/0123	registered	student verified
Adebukola Joseph.401	UJ/2011/NS/594	registered	student verified
Micheal Emeka.401	UJ/2011/NS/0320	registered	student verified
Gyang David.401	UJ/2011/NS/375	registered	student verified
Joseph Peter Ochai.401	UJ/2011/NS/0074	registered	student verified
Joshua Akande.401	UJ/2011/NS/0525	registered	student verified

Table3.2. *Results obtained from Phy412 students*

Name of Student	Mat. Number	Registration Status	Display on screen
Ezeoba Emmanuel Onyeka.412	UJ/2011/NS/0035	Registered	Student verified
Ani Basil Emeka.412	UJ/2012/NS/0496	Not registered	Student not verified
Ejiro Oghenechovwen.412	UJ/2011/NS/0712	Not registered	Student not verified
Obikili Jennifer Chioma.412	UJ/2011/NS/680	Registered	student verified
Reuben Samson Dawah.412	UJ/2011/NS/0403	Registered	Student verified
Oheitonye Ejembi Boniface.412	UJ/2011/NS/0078	Registered	Student verified
Saba M. Dabilong.412	UJ/2011/NS/0453	Not registered	Student not verified
Ekeakhogbe Gloria Omonye.412	UJ/2011/NS/0444	Not registered	Student not verified
Owoeye Peter Emmanuel.412	UJ/2011/NS/0154	Not registered	Student not verified
James Nanfwang.412	UJ/2011/NS/0780	Registered	Student verified

Kwada Douglas.412	UJ/2011/NS/0505	Not registered	Student not verified
Olushola Kemi Joyce.412	UJ/2011/NS/0413	Registered	student verified
Pam Victor.412	UJ/2011/NS/0162	Not registered	Student not verified
George Abel Inadu.412	UJ/2011/NS/0394	Not registered	Student not verified
Tarkumbul Ladi Sharon.412	UJ/2011/NS/0123	Not registered	Student not verified
Adebukola Joseph.412	UJ/2011/NS/594	Not registered	Student not verified
Micheal Emeka.412	UJ/2011/NS/0320	Not registered	Student not verified
Gyang David.412	UJ/2011/NS/375	Registered	Student verified
Joseph Peter Ochai.412	UJ/2011/NS/0074	Not registered	Student not verified
Joshua Akande.412	UJ/2011/NS/0525	Not registered	Student not verified

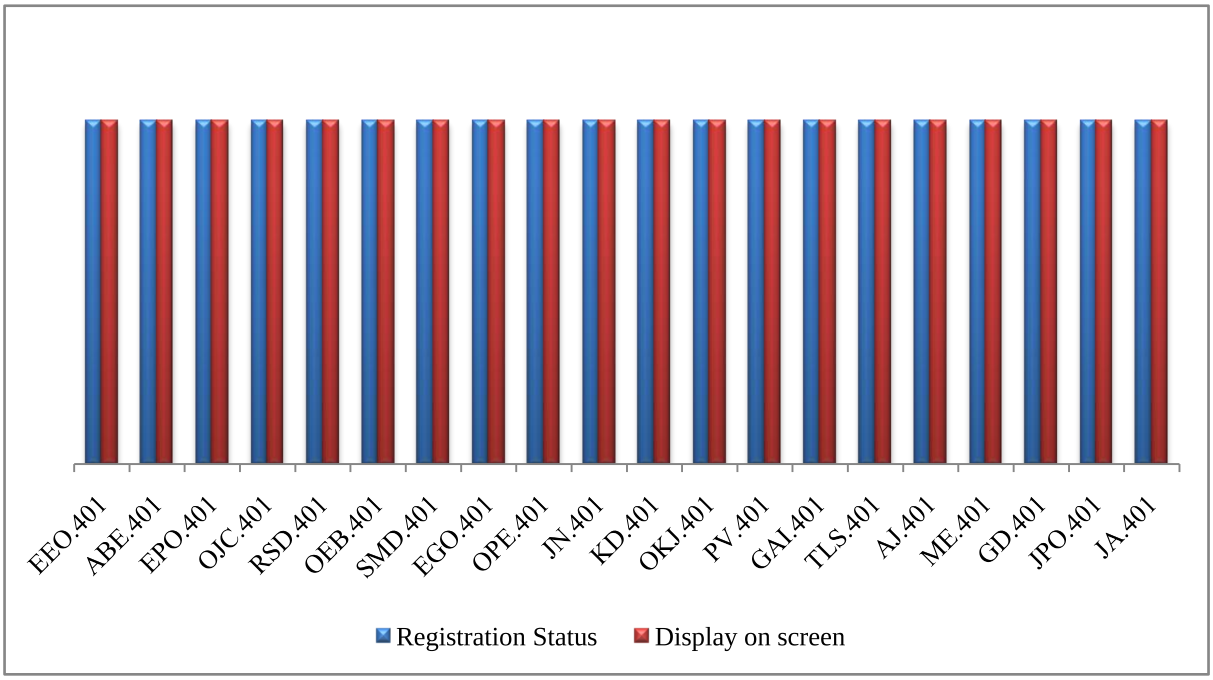


Figure3.1. *Graphical representation of the result obtained for Phy401*

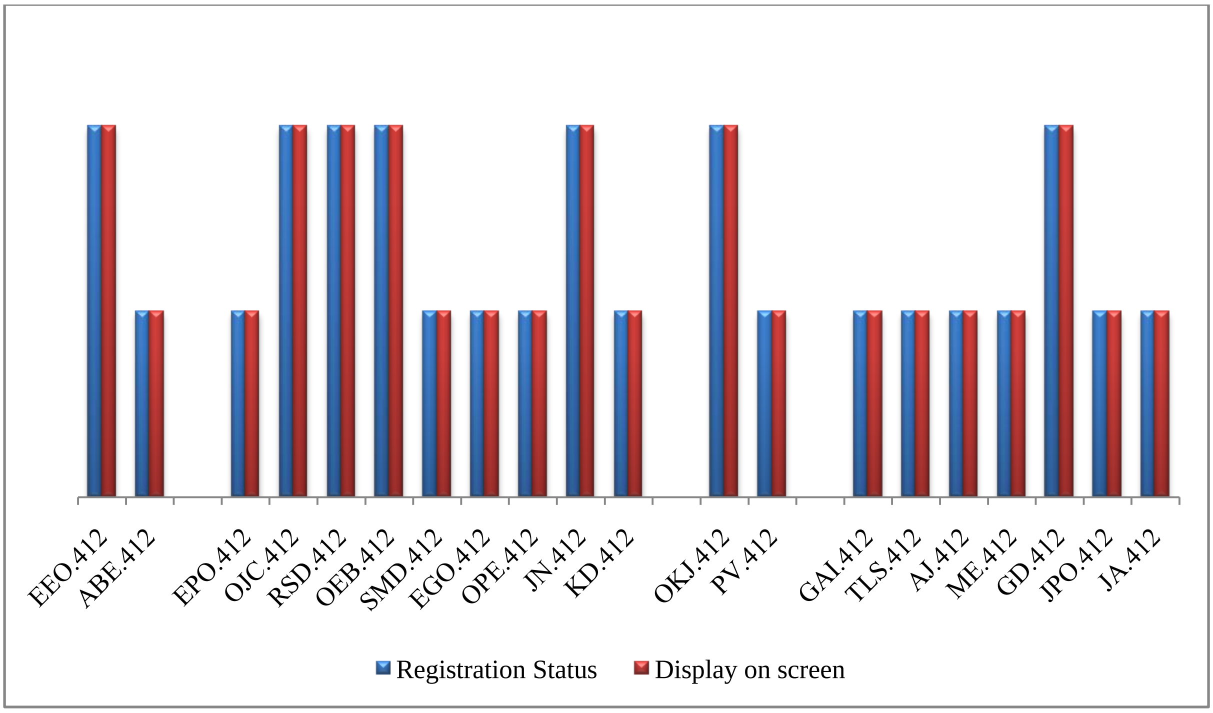


Figure3.2. *Graphical representation of the result obtained for Phy412*

It can be seen that the results obtained from the output of the LCD of the device corresponds to the real registration status of the student in the particular course he is being verified for. In other words, the device has given a 100% correct value for the registration status of all 20 student in the particular course.

4. DISCUSSION

This research is to design and construct a device that uses the unique, distinguishable and permanent marker, in this case, the fingerprint to automatically verify the identity of a student during examination. After the whole construction had been completed, I used the device to run test verification on different persons. In other for the same system to be able to register the same person, for more than one course using the same finger during enrollment,, say Phy401, Phy402, Phy412, Phy466, etc, I used a registration format, taking the form Name. Course code. For example, If Ezeoba Emmanuel Onyeka is registering for phy401,, the name to be entered on the name field will be Ezeoba Emmanuel Onyeka.401. With this format, Ezeoba Emmanuel Onyeka can register for Phy401, Phy402, Phy412, Phy466 etc on the same system with the same fingerprint.

The power supply cable and the serial port cable of the device are connected to the appropriate port in a laptop. The USB port provides the required 5V for the system to work while the to and fro communication between the device and the computer is made possible through the serial port of the computer. The sensor (thumbprint module) is also connected to one of the USB port. The registration plat form is then launched on the computer. This brings you to an environment where you choose the maker of the fingerprint scanner you intend to use. This is enable effective communication between the module and the computer.

After choosing the maker of the sensor, the program now opens to the registration environment. On this environment, the operator chooses what operation he wants to carry out. To register a student for a course, the operator goes to “User” and chooses the enroll option. A field comes out where the name of the student is entered using the format “Name. Course code”. When this is entered, the system requires for the finger print of the student being enrolled. This is gotten from the finger scanner that has already plugged in the USB port. The system automatically extracts distinguishing features from the finger print, and then registers it against the name of the student.

To perform a verification operation during examination, the operator again launches the program and selects the maker of the scanner he will be using for the exercise. This will lead to the same environment used during the enrollment exercise. “User” is selected and the verification option is chosen. A filed where the students name will be typed in the same format comes out. When this entered, the system will require the students fingerprint to match it against what is already stored in its database. If the finger print matches the name as stored in the data base of the system, the system displays “Student Verified” on the display unit of the device and “Not Verified” is displayed if the name entered does not match the fingerprint captured as stored in the database.

5. CONCLUSION

After observing from the results obtained in using the device to verify students, and also considering the time taken for the enrollment and verification exercise to be achieved, despite the challenges encountered with people with low fingerprint image quality, biometrics (fingerprint) have proven to offer a good and reliable way of automatically verifying students for an examination, especially for large classes where facial recognition of every student will not be practical to avoid student impersonation during examination or tests.

REFERENCES

[1] Anil, K.J. and Arun, R. (2008). Introduction to Biometrics, *Unpublished*

[2] Awanbor, D. (2004). Examination Malpractice and the Degenerative Effects on Quality of Education Examination/Assessment and Certification. *Unpublished*

[3] Bernard M.O (1998). Examination Malpractice in Tertiary Institution in Nigeria: Types, Causes, effects and Solution. *Unpublished*

[4] Duane, M. B. (2004). Biometrics 101, version 3.1 Tech. rep., Federal Bureau of investigation.

[5] Jackson, A. and Jackson, J. (2008). *Forensic Science*, 3rd edition, Harlow, Pearson Education.

[6] Jain, A. K. and Uludag, U. (2003). Hiding biometric data. *IEEE Transactions on pattern Analysis and Machine Intelligence*, vol. 25 (11), pp. 1494-1498.

[7] Jain, A.K, Hong, L. and Pankanti, S. (2000). Biometric Identifications. *Communications of the ACM*, Vol. 43(2), p. 91–98.

[8] Komarinski, P. (2005). Automated fingerprint identification system (AFIS).

[9] Maduemezia, M.U (1998). Examination Malpractice in the Senior School Certificate Examination: Current Trends, Problems and Prospects. Paper presented at the WAEC monthly seminar.

[10] Patricia M., Janusz K. and Witold P. (2009). Bio- inspired hybrid intelligent systems for image analysis and pattern recognition.

[11] PIC16F627A/628A/648A Data Sheet.

[12] Ratha, N. K., Connell, J. H. and Bolle, R. M. (2001). An analysis of minutiae matching strength, Proceedings. AVBPA 2001. *Third International Conference on Audio – and Video-Based Biometric Person Authentication*, pp. 223-228.

[13] Rood, E.P. and Hornak,L.A. (2008, Nov 11th) Are you who you say you are? Retrieved from *http://www.worldandicollege.com/public/2003/august/nspub1.asp,*

[14] Sahidullah, M. (2015). Enhancement of Speaker Recognition Performance Using Block Level,Relative and Temporal Information of Sub-band Energies. *PhDThesis (Indian Institute of Technology Kharagpur).*

[15] Ted, T. (2011, May 30). Spot the difference? The strange case of the criminal doppelgängers that sparked the need for fingerprinting. Retrieved from *http://www.dailymail.co.uk/news/article-1392418/The-amazing-pictures-sparked-need-fingerprinting.html*

[16] Uludag, U., Pankanti S., Prabhakar S. and A.K. Jain (2004). Biometric cryptosystems: issues and challenges, *Proceedings of the IEEE*, vol. 92(6) pp. 948-960.

[17] Welzl, M. (2004, June 25). Transmission Control Protocol (TCP) Corruption Notification options. Retrieved from *http://www.welzl.at/research/publications*