VOL. 20, NO. 1, 2021, 9-14
www.elektrika.utm.my
ISSN 0128-4428

ELEKTRIKA
Journal of Electrical Engineering

Development of a fingerprint lock safe with vibration sensor

Alim Sabur Ajibola* and **Eseyin Theophilus**

Mechanical Engineering Department, Ahmadu Bello University, Zaria,Nigeria.

*Corresponding author: moaj1st@yahoo.com

Abstract: Biometric recognition is the method of using natural human features to identify and recognize people. Biometrics include iris, DNA, face, fingerprint and voice. Numerous algorithms have been developed to interpret these human features for use in identifying human being. This study was aimed at developing a safe which can be accessed using fingerprint in order to address some of the recent cases of theft recorded in the department. This system ensures that only people whose fingerprint has been enrolled (saved on the fingerprint sensor's memory) can access the safe. The system makes use of Arduino UNO microcontroller to control and connect the necessary hardware required for locking and unlocking the safe. The other hardware are LCD screen, 4×4 keypad, fingerprint scanner and buzzer. The enrolment, delete user and vibration sensor tests were conducted on the system. Furthermore, It can be observed that the Admin plays an important role in any fingerprint-based system as s/he is saddled with responsibility of enrolling and deleting user(s) as well as in this case the deactivation of the vibration sensor.

Keywords: Arduino UNO, fingerprint, safe, security.

Article History: received 1 April 2020; accepted 25 March 2021; published 30 April 2021.

1. INTRODUCTION

With Significant technological advancement, there has been a proportionate increase in rate and sophistication of crimes precisely theft. This has necessitated the need to explore newer ways of improving security of lives and properties. Human beings find it challenging to secure to his properties manually as these security measures can either be broken or opened with a master access key. The use of mechanical locks has not had much effect on crime rate as break ins occur consistently. In order to keep our properties safe, there is the need to find alternative methods/ technologies which can provide complete security. As a result of this risk, personal identification technologies that can distinguish between legitimate users and imposters, have minimal error and provide necessary alerts in case of forced entry or otherwise.

Over time, passwords, microchip embedded cards and PIN verification techniques are being used. Passwords can however be hacked, while cards may be lost, stolen or cloned. The use of biometrics such as fingerprint recognition is possibly one of the most secure and sophisticated technique for securing in high profile systems. A fingerprint is distinct to each individual and stays unchanged for a lifetime. It has been observed that even identical twins with same DNA have distinct fingerprints (Kawade & Ubale, 2013). Fingerprint recognition uses the unique and invariant features of human fingerprints for purposes such as verification, identification and recognition. According to the FBI, fingerprints on the ten fingers of an individual differs (Carl, 2015). Among these available biometric trait/features, fingerprint proves to be one of the best, providing good mismatch ratio, high accuracy in terms of security and reliability and relatively cheap to set up. Other biometrics commonly used include face, iris, voice, signature, and hand geometry recognition and verification. Several other approaches are in different stages of development and testing.

The earliest use of fingerprints or handprint patterns was in the examination of the authenticity of prints by experts. As time went by, progress was made in identification process. As advances were made in computing technologies, automation was introduced to the process of capturing and identifying fingerprints.

In 1684, Dr. Nehemiah Grew described the pores, ridges and furrows that can be found in the fingerprints of both the hands and feet of human beings (Lambourne, 1977). Subsequently, Professor Johannesh created a system for identifying and classifying fingerprints. He described nine types of fingerprint patterns and classified each pattern type by a specific name. He was also able to show that each person has unique fingerprints and that the fingerprint on each finger differs (Sharma et al., 2013).

The idea of looking at the use of thumbprint locks is from the backdrop of the recent break-ins in the Department of Mechanical Engineering, ABU, Zaria, where the mechanical locks in use have not been able to deter the thieves from gaining access to the offices of lecturers. This issue of theft was repeated on at least two occasions in which valuable items were stolen from the offices affected. This encouraged the development of this

safe to keep personal items in the office and can be adapted for use at the office doors to replace the mechanical locks.

Sheng et al. (2009) introduced an approach in which they used a consensus matching function and a genetically guided approach to optimize the consensus matching function for simultaneous fingerprint alignment and verification. Experimental results of proposed algorithm show that the consensus function had a substantial improvement in performance while the local matching operation helped to identify promising initial alignment configurations.

Islam et al. (2010) proposed two new methods for the identification of fingerprints of different people based on 1-D and 2-D discrete wavelet transformations (DWTs). In first method, several fingerprints of an individual were taken in a random manner followed by a 2-D DWT. Four filtered signals were transformed at 9 levels DWT and the approximations are stored in place of the original images. In second method, several fingerprints of an individual were taken in a random manner similar to the previous method (in context of translation and rotation) then an RGB conversion is performed on them. The contrast of the images is improved using canny filter then colour inversion is performed on them.

Jain and Feng (2011) introduced a method of recognizing characters in natural scenes like clutter and placement as well as with different font style and variation in light conditions. The authors implemented two common descriptors namely shape context and wavelet. In the shape context method, the relative positions of pixels at the edge of the image is extracted. For each location, they impose a log-polar grid and bin the pixels in the edge of the image into a histogram. The second Wavelet transform was used for texture representation, image compression and character recognition.

Thaiyalnayaki et al. (2010) used a level 2 daubechies transform and only the second level LL image for the analysis as it contains the most relevant textural information. The daubechies method deals with problems associated with JPEG compression and random additive noise. The authors proposed a combination of three texture descriptors namely Standard Deviation, Kurtosis and Skewness. This approach is very simple compared to minutia point pattern matching algorithm.

2. METHODOLOGY

In this study, proper selection of materials was carefully done. The type of fingerprint scanner to use, the maximum number of fingerprint images that can be save on the memory, the type and size of the microcontroller to use, its RAM and programmable memory were all appropriately selected considering cost, availability and capacity.

2.1 Stages of Fingerprint Lock Safe

2.1.1 Data Capture

This is the first stage of any fingerprint-based system. In order to enrol new users, the fingerprint information of the users are captured by requesting them to place their fingers on the fingerprint sensor. The fingerprint image is stored on the fingerprint scanner database as template. FPD10A optical scanner was used for the capture and verification of fingerprint images.

2.1.2 Feature Extraction

Some selected features are captured in the data capture stage. These features perfectly describe each fingerprint with minimal information size. These features are stored in the database. This is where image enhancement, enhance ridge and the extraction of minutiae are also carried out.

2.1.3 Fingerprint Verification

To access the safe, the user is required to place his/her finger whose data has been captured and stored on the fingerprint scanner for verification. The fingerprint Image is taken and undergoes a process of template matching. This is done by extracting the minutiae features of the scanned image and comparing it with templates on the database of the fingerprint scanner. If the fingerprint matches any template in the database, the ID of the user is retrieved and sent to the microcontroller which then grants the user access (open the safe or enroll other users). Else, the unauthorized user is denied access to the safe (Zhang et al, 2011; Zaeri, 2011).

2.2 Procedure for Design and Implementation of Fingerprint Safe

The procedure followed in the construction and implementation of the fingerprint safe is divided into major steps as presented below.

2.2.1 Step 1: Design of the Box

For demonstration purpose, a model safe was constructed using wood and the dimensions of the box are shown in figure 1.

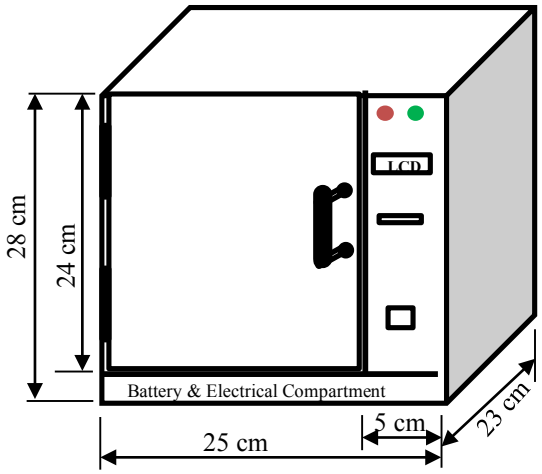


Figure 1. Model Safe

2.2.2 Step 2: Connection of Hardware Equations

This shows the pin definition and how the hardware were connected to the Arduino board. The connections are as in figures 2, 3, 4 and 5, while the pin definition can be seen in tables 1, 2, 3 & 4.

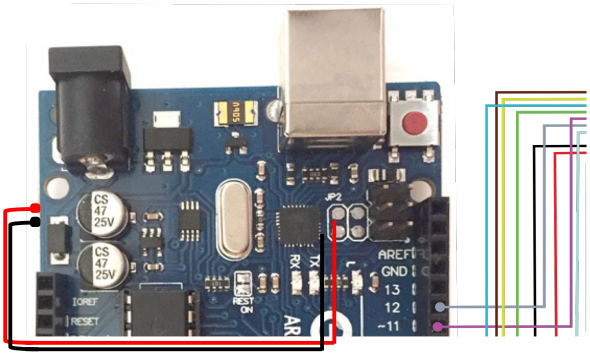


Figure 2. Arduino microcontroller and I2C LCD

Table 1. Pin definition for I2C LCD

Arduino Uno	I2C LCD
5v	VDD, A
GND	VSS, RW, K
V0	Potentiometer
11	EN
12	RS
3, 2, 1, 0	D4, D5, D6, D7

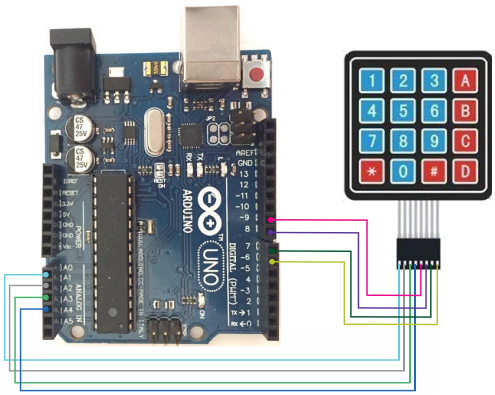


Figure 3. Arduino UNO and 4x4 keypad

Table 2. Pin definition for the 4x4 keypad

Arduino Uno	4x4 Keypad Matrix
A0	ROW 1
A1	ROW 2
A2	ROW 3
A3	ROW 4
9	COL 1
8	COL 2
7	COL 3
6	COL 4

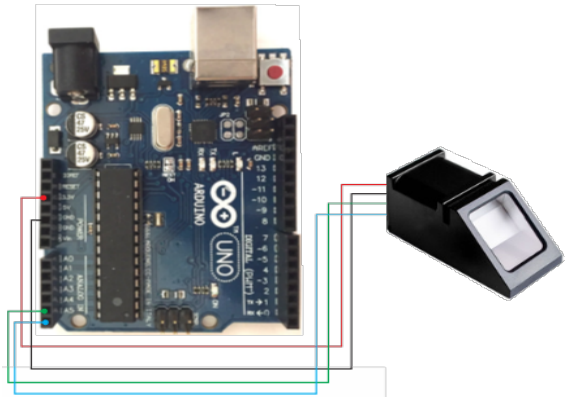


Figure 4. Circuit diagram for FPM10A Fingerprint Scanner

Table 3. Pin definition for FPM10A

Arduino Uno	FPM10A Module
3.3V	VCC
GND	GND
A4	RX
A5	TX

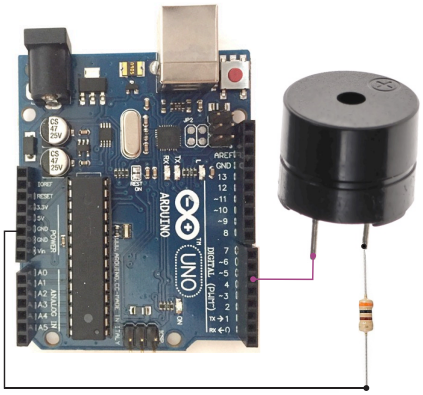


Figure 5. Circuit diagram for buzzer (vibration censor)

Table 4. pin definition for the buzzer (vibration censor)

Arduino Uno	Buzzer
GND	- Terminal
5	+ Terminal

All Components (LCD, Fingerprint Sensor, Keypad, Solenoid Lock, Lock Sensor and Vibration Sensor) and their pin definitions can be seen in figures 2-5 and tables 1-4. They were connected and attached to the safe using bolts and adhesive where necessary. A cut to the size transparent glass was used to cover the LCD, it acts as a screen to protect the LCD from direct touch. All the wires were neatly clipped together and passes down to the electrical compartment which is located at the bottom of the safe. The charging cable was run through a hole at the back of the electrical compartment to the transformer

which is used to charge the battery that powers the microcontroller. The On/Off switch is connected at the front of the safe.

3. SYSTEM TESTING RESULTS

Test were conducted on the fingerprint lock safe and the results were used to analyze and compare with the expected output. Table 5 shows the results of the enrolment test, while table 6 shows the delete user fingerprint test.

Table 5. Enrolment test

Test	LCD Display	Expected Outcome	Success ✓ / Failure X
Ask for Admin fingerprint before enrolling	Admin finger on the Sensor	Waiting for the Admin to place his/her finger on the sensor to verify	✓
Enter the name of the user whose print wants to be enrolled	Enroll name	If user's name is less than 5 characters, LCD shows error: Name cannot be less than 5 character	✓
Check if fingerprint exist	Place finger on sensor to verify	If the fingerprint has been enrolled before, the LCD shows Finger exist and gives maximum of 4 retries of same finger.	✓
Enroll proper	1. Same finger on the Sensor pls. 2. Place same Finger again.	During verification, the user is required to place the same finger twice and if it does not match, the enrolment process is cancelled with an error message.	✓
ID number	The ID number for the captured print is generated automatically after the previously saved ID.	Appropriate error message must be shown in the LCD	✓

In any system that is dedicated for identification and recognition, such a system must have an admin(s) who would manage the system, be able to enroll (add) new user(s), delete (remove) user(s) and perform other tasks as desired by the designer. it is essential to test a system such as this fingerprint lock safe to ensure that in the process of programming the microcontroller, all the necessary information are not omitted. These information include the desired responses when there is a success or failure in any of the stages.

Table 5 shows the enrollment test, where 5 tests were conducted on the system. The table has four columns which include the expected outcome and the success/failure of tests. It would be observed that all the tests were a success as the tests had been factored into the design while programing the microcontroller. Similarly, table 6 shows the delete user/fingerprint test. It would be observed that the Admin has control over both the enrolment and deleting of new users. This is the desired state of such a fingerprint-controlled system. In a similar study by Abdullateef et al. (2018), they presented their tests for the enrollment and deleting of users in form of sub-routines. The sub-routines of their fingerprint attendance management system with automatic excel computation were presented in form of flowcharts.

Table 6. Delete user/fingerprint test

Test	LCD Display	Expected Outcome	Success ✓ / Failure X
Ask for Admin fingerprint before deleting	Admin Finger on the Sensor	Waiting for the Admin to place his/her finger on the sensor to verify	✓
Enter ID to be deleted	Enter the ID of the print to delete	If 0 or 1 is entered, the process is cancelled because the Admin Fingerprint is saved with ID 1 and 0 is not allocated in the memory	✓
ID not Found	Fingerprint with ID not Found.	Process is cancelled	✓
ID Found	Deleting user: (Shows name of user).	The systems require the Admin to press 1 to proceed with the delete or 0 to cancel	✓

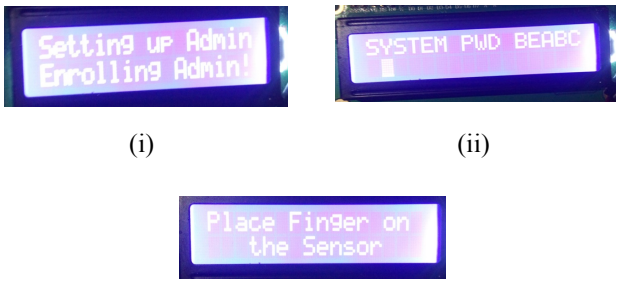
In table 7, the tests for the vibration sensor were conducted. Most importantly is the fact that switching off the system does not switch off the vibration sensor and that any sudden shake of the safe also triggers the vibration sensor and switches into alarm mode. Most thieves in the academic environment use the cover of the night and absolute silence to commit their dastardly act. With the introduction of the vibration sensor and alarm into the system, would reduce their activity and increase the chances of them getting caught.

Table 7. Vibration sensor test

Test	LCD Display	Expected Outcome	Success ✓ / Failure X
Sensor Active State	The vibration Sensor becomes active when the system is on the default page i.e LCD showing Waiting for a Valid Finger	The vibration sensor need not be active when the locker door is open and also on the Admin page.	✓
Hitting the Locker box with a push	This activate the sensor and the system enter the Alarm mode	LCD displays Admin Print to disable Alarm.	✓
Turn off the system	The buzzer continues with the alarm even if the system is turn off	Switching off the system does not turn off the alarm	✓
Turn Off Alarm	Admin Fingerprint is the only means to turn of the Alarm	Admin required to turn off alarm	✓

3.1 Enrolment and setting up of Admin Fingerprint

Further test were carried out on the setting up of the lock system and also on changing of the system password and also the wipe out all data on the system i.e to reset to factory mode.



(i) (ii)

(iii)

Figure 6. Setting up Admin

When there are no fingerprints enrolled on the sensor, the system will start in factory mode i.e enrolling the Admin fingerprint and setting up the system password as in figure 6 above.

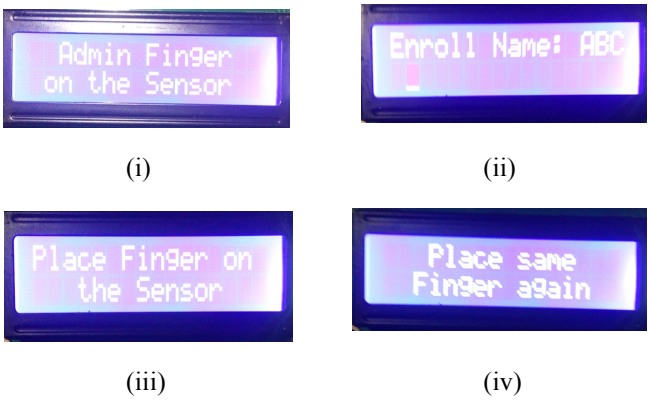
3.2 Admin Screen

(i) (ii)

Figure 7. Default display after admin setup

If the admin's finger is placed on the sensor, the admin page is open where the admin is required to either enter 1 for enrollment or 2 to delete fingerprints as in figure 7.

3.3 Admin Screen – Enroll New Finger



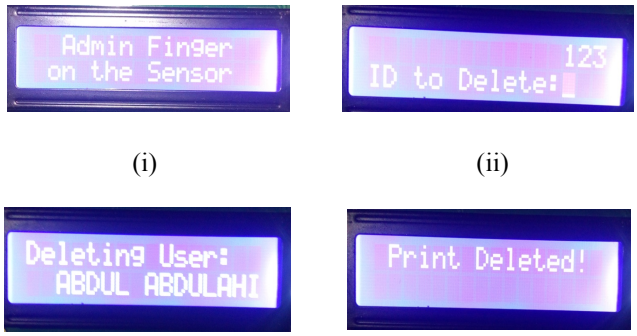
(i) (ii)

(iii) (iv)

Figure 8. Enrolling New Fingerprint

Enrolling of new fingerprint required that the admin first place his finger for verification then the name to save the fingerprint is required, after which the user is then required to place his/her finger on the scanner for enrollment as can be seen in figure 8.

3.4 Admin Screen – Delete Fingerprint



(i) (ii)

(iii) (iv)

Figure 9. Deleting Fingerprints

While on the admin page, if the admin presses 2 on the keypad, the delete fingerprint menu will require the admin to place his/her finger on the sensor for verification. The admin is required to enter the ID of the fingerprint to be deleted and the name of the user who owns the print is displayed as in figure 9 above and then the print is deleted.

3.5 Hidden Admin Screen

When the Admin presses 0 on the keypad, this hidden admin menu shows up. The hidden Admin menu is used to change the system password and also the set the system to default factory mode i.e. by deleting every data saved on the database. The saved data are all saved fingerprints, all saved fingerprint name, system password. and admin fingerprint.

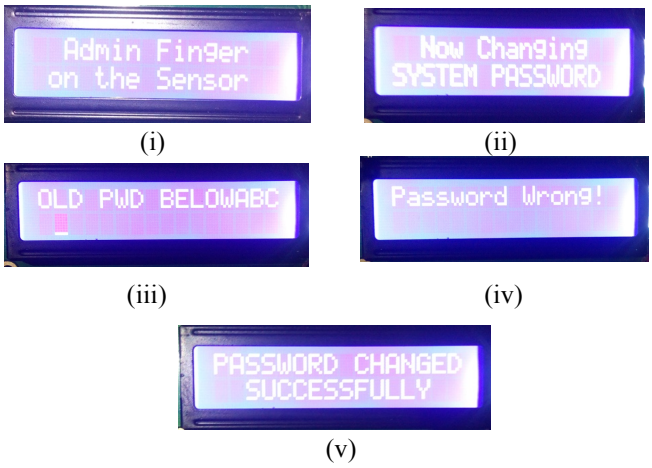


Figure 10. Change system password

If 1 is pressed from the hidden menu, the system requires that the admin revalidates his/her fingerprint, see figure 10 (i) above, then the system request for the old password as seen in figure 10 (ii) in which if wrong password is entered, the system displays a message to the admin that a wrong password was inserted then close as seen in figure 10 (iii) but if the password is right, the system password will change and the LCD alert the admin that the password is changed successfully.

Figure 11. Factory reset

On the other hand, if 2 is pressed from the hidden menu, the reset menu is activated, this resets the system back to the factory settings. The admin is required to place his/her finger on the sensor figure 11 (i). If successful, the system password is required figure 11 (iii). If it went through, the system is reset back to the factory settings figure 11 (iv) i.e all data, fingerprints are deleted.

Every test discussed above was performed several times to ensure the same results were achieved in order to avoid problem or unforeseen error. All output pins on the Arduino UNO was used to maximize cost, else Arduino mega would have been used as it has more output pins (54 digital pins) and 16 analog pins. The Vibration sensor which was procured for used was burnt, as such, a vibration sensor was designed locally to serve similar function. The locally fabricated vibration sensor responded well to minimal touch on the safe which makes it more effective in this study than the purchased vibration sensor. Finally, the circuits and system design process was successful and the safe worked well without any error or fault.

4. CONCLUSION

With the success in implementing this fingerprint lock system, this idea can be translated into some similar or more complex systems such as door access for offices and laboratories as well as personal safe for home and office applications. It can be observed that the Admin plays an important role in any fingerprint-based system as s/he is saddled with responsibility of enrolling and deleting user(s) as well as in this case the deactivation of the vibration sensor. The enrolment and delete user tests show that the system successfully passed the basic expectations for adding and removing user(s). This system can be improved to providing image capture of users who actually access the safe.

REFERENCES

[1] Kawade S. P., & Ubale V.S. (2013). Fingerprint Recognition for High Security Systems Authentication. International Journal of Electronics, Communication & Instrumentation in Engineering Research and Development, Vol. 3, Issue 1.

[2] Carl E. (2015). Fingerprints change over the course of a person's life. Retrieved 11/09/2018, from http://blogs.discovermagazine.com/d-brief/2015/06/29/fingerprints-change-over-the-course-of-a-persons-life/

[3] Lambourne G. T. C. (1977). A Brief History of Fingerprints. Journal of the Forensic Science Society, 17(2–3), (95-98).

[4] Sharma, R., Mishra, N., & Yadav, S. K. (2013). Fingerprint recognition system and techniques: A survey. International Journal of Scientific & Engineering Research, 4(6), 1670.

[5] Sheng W., Howells G., Fairhurst M. C., Deravi F., & Harmer K. (2009). Consensus fingerprint matching with genetically optimised approach. pattern recognition, 42(7), 1399-1407.

[6] Islam M. I., Begum N., Alam M., & Amin M. R. (2010). Fingerprint Detection Using Canny Filter and DWT, a New Approach. JIPS, 6(4), 511-520.

[7] Jain A. K., & Feng J. (2011). Latent fingerprint matching. IEEE Transactions on pattern analysis and machine intelligence, 33(1), 88-100.

[8] Thaiyalnayaki K., Karim S. S. A., & Parmar P. V. (2010). Finger print recognition using discrete wavelet transform. International Journal of Computer Applications, 1(24), 96-100.

[9] Zhang D., Liu F., Zhao Q., Lu G., & Luo N. (2011). Selecting a reference high resolution for fingerprint recognition using minutiae and pore, IEEE Transaction on Instrumentation and Measurement, 60(3), 863-871.

[10] Zaeri N. (2011). Minutiae-based fingerprint extraction and recognition, Biometrics, Jucheng Yang, IntechOpen.

[11] Abdullateef A. I., Ekwemuka B. C., Itopa V., Makinwa T. B. & Alim S. A. (2018). Fingerprint based student attendance management system with automatic excel computation, LAUTECH Journal of Engineering and Technology, 12(2), 123-135