A Low Cost Computer based Fingerprint Security System for Restricted Access Control Automation using LabVIEW

Jared Maato
Department of Physics
Kenyatta University, PO BOX 43844, Nairobi, Kenya

Elijah Mwangi
School of Engineering
University of Nairobi, PO BOX 30197, Nairobi, Kenya

Patrick M. Karimi
Institute of Energy Studies & Research, PO BOX 30099
Nairobi, Kenya

ABSTRACT
The access to a restricted area is normally done through a manual system of keys and locks. In some places, it has been automated through the use of personal identification number or passwords and smartcard technology. However, such systems are faced with a number of limitations such as losing a smartcard, forgetting a PIN, duplication of keys and impersonation among others. Thus the use of an authentication system such as biometric verification techniques has recently been suggested for security system for instance access control. Unfortunately, biometric systems for access control currently in the market are expensive thus restricting their wide usage. This is because they are available as embedded units made of high-cost sensors and hardware. In this research study, a prototype of a computer based fingerprint door access control is designed and presented. The main components include a low-cost SM630 fingerprint verification module, a personal computer and a relay-operated electromagnetic lock. The system performs training and verification using a LabVIEW program in conjunction with the SM630 fingerprint reader module. The verification result is passed onto the electromagnetic lock to grant physical access to a restricted area. The system has an additional feature of capturing an imposter image. This is an important tool in carrying out security analysis. It has been found through testing that the proposed system can be effectively applied in restricted access control.

Keywords
LabVIEW, access control, SM630, automation.

1. INTRODUCTION
The physical access control is an important security tool. One of the basic security systems in a building is the door access control [1]. It can be noted that most doors are controlled manually through the use of lock and key system [2]. Others are controlled by smartcards and personal identification numbers [3]. However, such devices face authentication problem thus the use of biometric verification solution e.g. the voice, the palm and the fingerprint is being considered for restricted access control [4].

While biometric devices have been designed and are installed within buildings for access control purposes, the high cost has restricted their usage in most premises. With the advancement of computer technologies, interfacing sensors and other peripherals with personal computers have been made possible [5]. In addition, various programming languages are currently available to enable automation of these systems. An example is LabVIEW software which is mostly used for instrumentation, control and automation [6, 7]. In this research paper, we present a low-cost computer-based fingerprint access system which is automated using the LabVIEW programming language.

2. RELATED WORK DONE
Computer-based access control, focusing on biometric solution, has been widely studied and published in literature.

Wahyudi *et al* [1] designed a voice-based door access control system using adaptive-network-based fuzzy inference systems (ANFIS). A low-cost microphone was used to record the voice. The voice-based verification system adopted the Perceptual Linear Prediction (LPC). The verification algorithms were implemented using MATLAB with a decision signal being sent through the parallel port to physically control the door-lock. The experimental results included parameters such as the FRR and FAR. For instance, the overall FAR was found to be smaller than 10%. However, a FAR less than 1% is recommended for high level security applications.

Arulogun *et al* [8] designed an access control system using facial recognition. The face is compared with the ones in the database and if it matches, the program sends a signal through the parallel port to trigger the operation of the mechanical motor to unlock the door. The main program was written on a MATLAB platform. It was driven by a timer function such that it samples the output of the digital camera every three seconds to inform the necessary sub-program. Thus any moment an image is detected in the camera, the face comparison and recognition sub-program is executed.

Ashraf [9] designed a biometric access control system using fingerprint for restricted area. The system was designed to register fingerprints in a database. A personal computer and a Bio Entry Plus Scanner were the main components. A MATLAB code for image filtering and processing; and a C# for matching were used. Thus registration, verification and identification were implemented.

Iwasokun [10] designed a fingerprint matching algorithm using minutiae-singular point's network. The matching algorithms were designed on a MATLAB platform using the Euclidian and spatial relationships to determine matching score for fingerprint images obtained from the FVC2002 Fingerprint Database. The experimental results gave a FAR of 0% with FRR in the range of 7-10%.

3. THEORETICAL BACKGROUND

3.1 Fingerprint recognition

Fingerprint recognition is an automated method of confirming the identity of an individual based on the comparison of two fingerprints. It is one of the most well known biometrics and is so far the most used solution for authentication in access control, attendance systems and electronic voting system (EVM). The fingerprint recognition has been researched for the long period of time and it has shown the most promising future in the real world application [11]. It is popular due to ease of acquisition, established use and acceptance when compared to other biometrics [12].

A fingerprint sensor is used to capture a digital image of a fingerprint pattern or a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted minute points) which is stored and used for matching.

Matching algorithms are used to compare previously stored fingerprint templates against the subject's for authentication purposes. This is done through either the original image being directly compared with that of the candidate or minutiae features of the same being used in the comparison. This analysis is very important since no two fingerprints of the same type from different subjects have been shown to be identical [13]. There are two types of matching algorithms commonly used namely; minutiae and pattern based. The minutiae algorithm is the most widely used technique. It relies on recognition of the minutiae points. The pattern matching, on the other hand, compares the basic fingerprint patterns such as an arch, whorl and loop between a previously stored template and a subject's fingerprint. The two images must be aligned in the same orientation. This is done by the algorithm finding a central point in the fingerprint images. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match and a score is generated [14].

3.2 LabVIEW basics

The term LabVIEW stands for Laboratory Virtual Instrument Engineering Workbench. It is a graphical programming language developed and distributed by National Instruments (NI). A LabVIEW Program is created using graphical notations unlike in text based programming languages. It enables a programmer to easily develop powerful applications.

A LabVIEW program is made up two main parts: a front panel and a block diagram. The front panel is the interactive user interface of a Virtual Instrument (VI). It contains controls (which are user inputs) and indicators (which are program outputs). Examples of controls are knobs, push buttons, toggle switch; and indicators are graphs, LEDs, numeric and many more. The block diagram is the LabVIEW program's source code constructed by drawing wires to connect the appropriate objects (graphical icons) together in order to define data. Thus this is the actual executable program. Front panel objects have corresponding terminals on the block diagram hence data can pass to and from the user to the program.

Data transfer between the objects is done through wires. Each wire has a single data source but it can transfer data to multiple functions and VIs. They are of different colors, styles and thickness depending on the data type. Thus connecting a wire between a source and destination of different data types will indicate an error thus making debugging easier.

Structures are graphical representation of loops and case statements in text-based programming environment. They include: for loop, while loop, sequence structure, case structure, formulae node, timed loop and stacked sequence structure.

4. THE PROPOSED SYSTEM

The proposed computer-based access system comprises of fingerprint sensor module, relay driver and electro-mechanical lock system. It is expected to provide an alternative and low-cost access control to restricted areas. It is made up of two parts namely the hardware units and the software.

4.1 The hardware

In the proposed system, the hardware constitutes of the fingerprint sensor module (SM630), the USB to UART converter (UC00A), a relay driver and an electromagnetic lock unit. A block diagram of the proposed system is shown in figure 1 and a corresponding photograph in figure 10.

Since the SM630 uses UART interface standard, a USB to UART bridge is required in order to connect it to the computer. The Tx pin of SM630 is connected to Rx of UC00A. Similarly, the Rx of SM630 is connected to Tx of UC00A. When the UC00A is plugged into the computer, a virtual serial port (COM) is created. The first step is to install the virtual COM port drivers (VCP) downloadable at the Future Technology Device International (FTDI) website [15]. This is done once. After this installation, the device manager is able to recognize the virtual COM port. In order for a LabVIEW program to access the virtual COM port resource, the National Instrument Measurement and Automation Explorer (NI MAX) is used to configure it.

A relay is required to energize the electromagnetic lock. It is driven by a simple transistor circuit shown in the figure 2. When the decision signal is in HIGH state, the transistor is driven to saturation thus energizing the relay which subsequently opens the lock. On the other hand, when the signal falls to a LOW state, the transistor switches to cut-off thus the spring-latched lock closes. Since most of the recent computers use the USB interface for connecting peripheral devices, a USB to parallel interface can be used for relay control. An example is the FT245R USB to parallel interface [17]

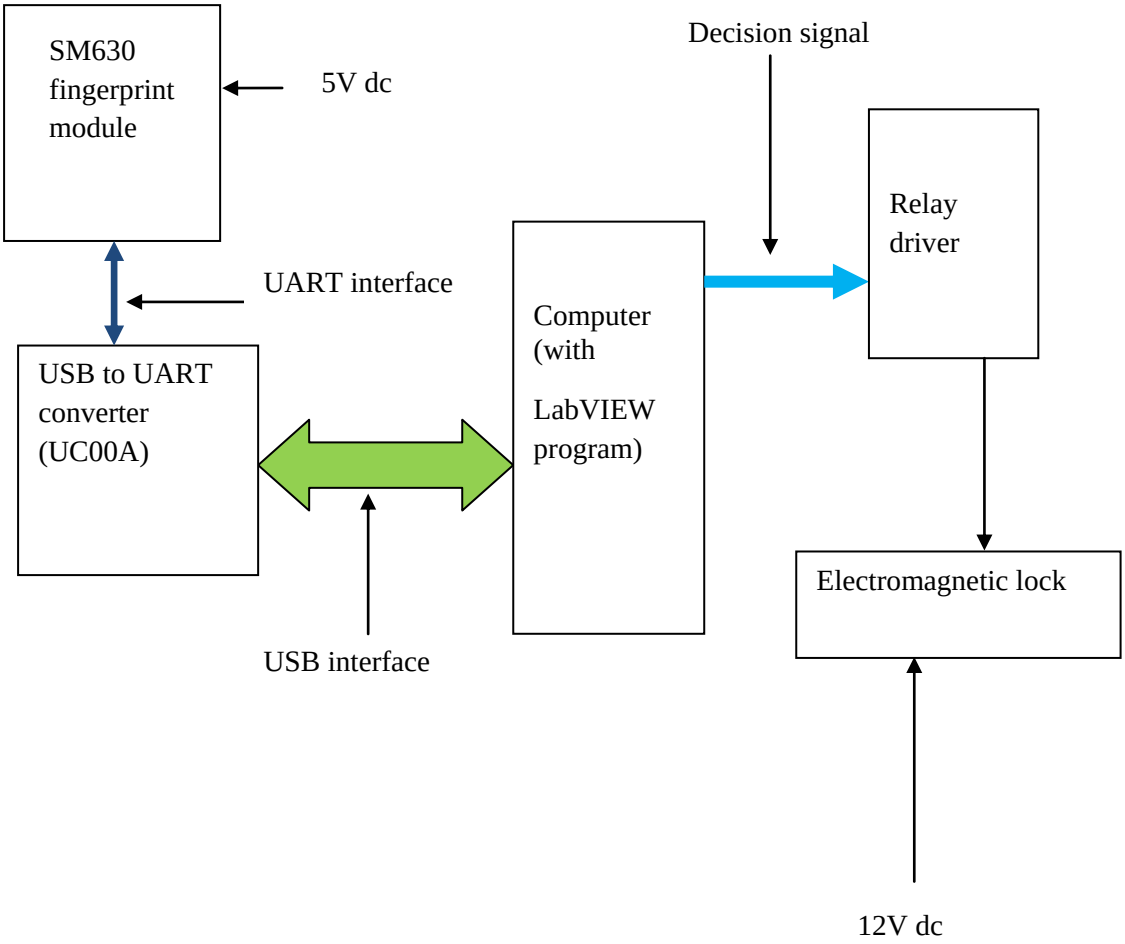

Figure 1: A block diagram showing the system hardware

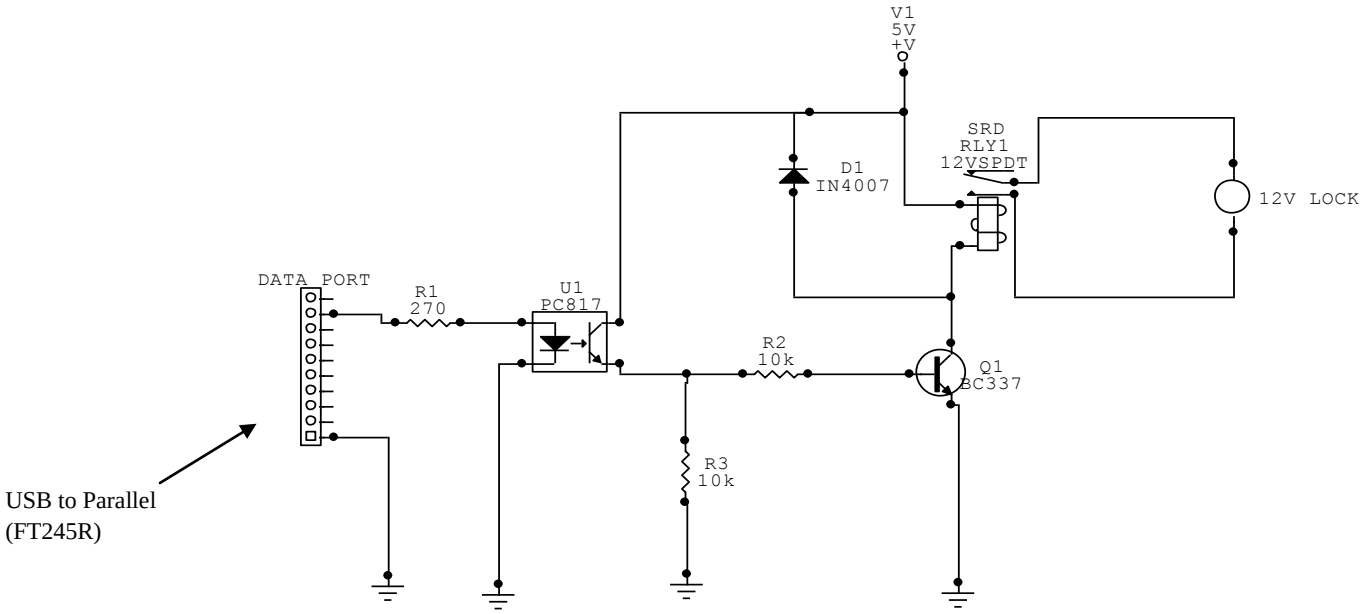

Figure 2: Schematic diagram showing the switching circuit

4.2 The software design

The software has been designed using LabVIEW programming language. Its main functions are to send commands to and from the SM630, triggering a camera to capture an image and sending a decision signal to control the lock unit. To accomplish these functions, the software has been designed to include program segments or SUB VIs . The

main program is designed to execute in the following steps as shown in the flow chart in figure 3:

(i) Checks whether a thumbprint is placed on the sensor window.

(ii) If the thumb is present, it moves to the next step otherwise it loops.

(iii) The program then checks whether the thumbprint matches with any in the template library and makes appropriate decision as discussed in section 5.2.

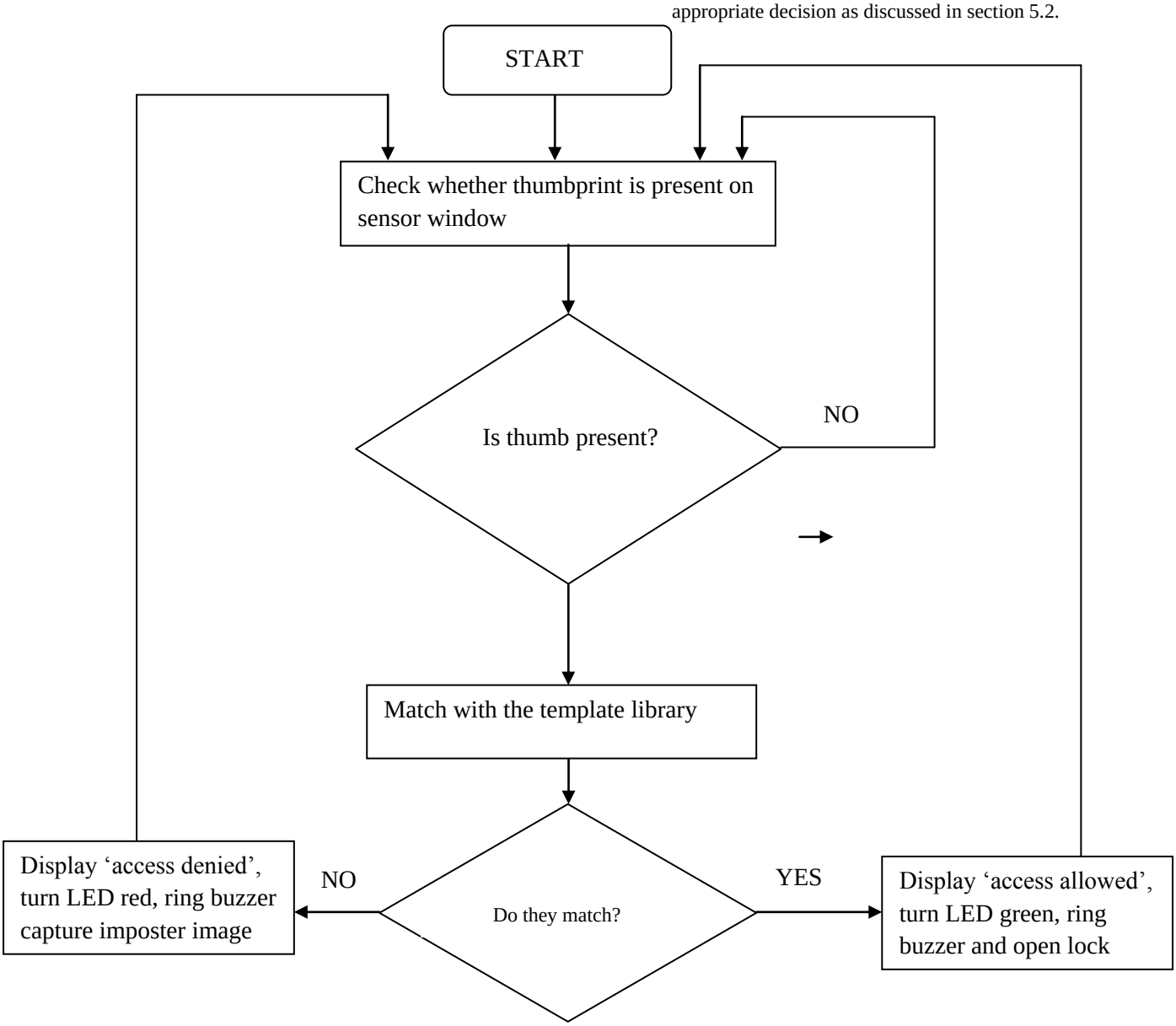

Figure 3: Flow chart for the system software

5. RESULTS AND DISCUSSIONS

5.1 Training performance of the system

During training, the subject places and aligns the thumb on the sensor window. Normally, a thumb or an index finger is preferred because the fingerprint surface is large and its quality better [16]. The system response is displayed on the front panel in two ways: '*thumbprint successfully processed and stored in the system library'* or '*processing failure'*. The possible cause of the latter is either the thumbprint quality being poor or not well aligned with sensor window. In the proposed system, a number of varying thumbprint conditions has been used and the test results presented as shown in table 1.

Table 1: Training performance of the designed system

Subject fingerprint condition	**System response**
Subject 1: dry and clean fingerprint	Training successful; fingerprint added to system memory
Subject 2: wet fingerprint (water)	Training successful; fingerprint added to system memory

Subject 3: dusty with chalk	Training successful; fingerprint added to system memory
Subject 4: dusty with dry soil	Training successful; fingerprint added to system memory
Subject 5: dusty with mud	Fingerprint quality is poor (process failure)
Subject 6: fingerprint with transparent cello tape	Training successful; fingerprint added to system memory
Subject 7: oily and scratched fingerprint with used engine oil	Fingerprint quality is poor (process failure)
Subject 8: fingerprint with ink drops	Training successful; fingerprint added to system memory
Fingerprint on paper (by ink)	Thumb not detected!

As shown in table 1, a wide range of fingerprint conditions have been successfully processed during training. This is because; the SM630 fingerprint module is designed with a self-adaptive parameter adjustment mechanism which improves imaging quality for both dry and wet fingers [16]. Thus training simply requires fairly clean fingerprints in addition to correct alignment on the sensor window.

5.2 Verification performance of the system

In the verification phase, the program '*verify.vi*' is opened to run in a continuous mode. The verification process then automatically executes as follows (summarized by the timing diagram in figure 6):

(i) The front panel first displays the message; '*welcome*'.

(ii) Shortly after, it displays '*press your thumb and wait*'.

(iii) If the thumb is pressed, it displays '*thumb detected*' followed by '*processing'*.

(iv) If the thumb is not pressed, it displays '*thumb not detected*' and then loops to (i).

(v) If the thumbprint is of an authorized subject, the system then grants access by displaying '*access allowed*', turning LED green as shown in figure 4 (b), ringing the buzzer and unlocking the spring latch. After 4 seconds, the system loops to (i).

(vi) If the thumbprint is of an imposter subject, the system then denies access by displaying '*access denied*', turning LED red as shown 4 (a), ringing the buzzer, leaving the spring latch locked and capturing the image of an imposter. After 4 seconds, the system loops to (i).

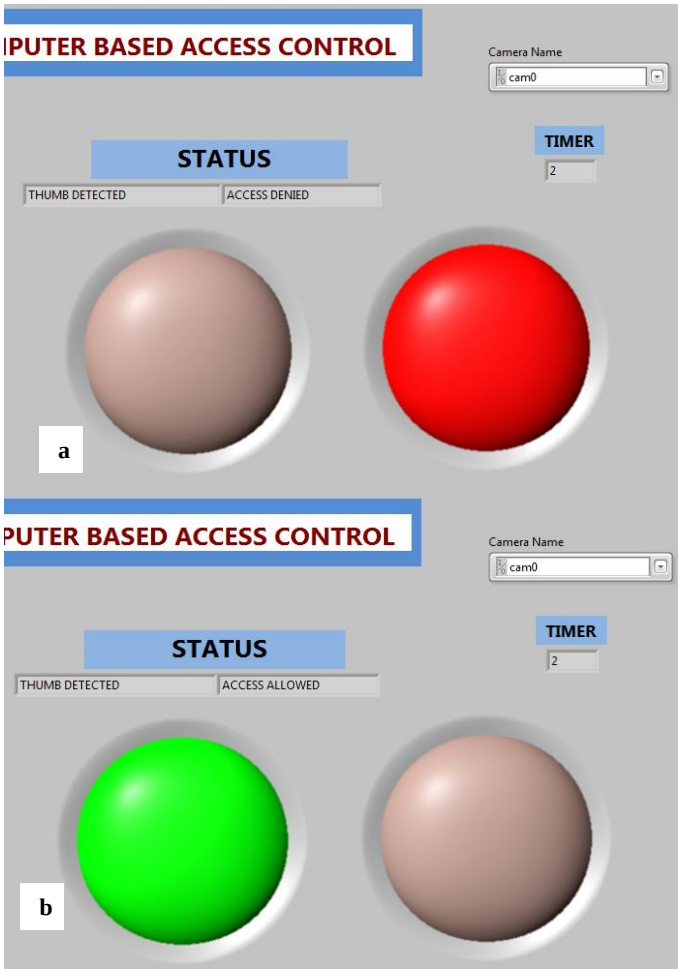

Figure 4: **The front panel response at the end of verification, with (a) access denied and (b) showing access allowed**

In order to evaluate the effectiveness of the designed system in access control applications, false rejection rate (FRR) and false acceptance rate (FAR) are computed. To compute the FRR, 100 subjects are enrolled in the system library. On the verification phase, the system is tested on the same number of authorized subjects. The numbers of rejects (false rejects) are recorded as shown in table 2. Similarly, the same procedure is done on the imposter subjects and the number of false acceptance attempts also recorded.

Table 2: Verification performance of the designed system

	Authorized subject		**Imposter subject**	
SN	**Access allowed**	**Access denied**	**Access allowed**	**Access denied**
1	YES	NO	NO	YES
2	YES	NO	NO	YES
3	YES	NO	NO	YES
4	YES	NO	NO	YES
5	YES	NO	NO	YES
6	YES	NO	NO	YES

7	YES	NO	NO	YES
8	YES	NO	NO	YES
9 ⋮	YES	NO	NO	YES
100	YES	NO	NO	YES

From table 2, it is observed that NFR = 0 and NFA = 0

Using this information, the FRR is determined as [1]:

FRR= (NFR/NAA) ×100%

Where NAA is the number of attempts by authorized users and is given as 100.

Substituting;

FRR= (0/100) × 100%

FRR=0%

Similarly, the FAR is determined as:

FAR= (0/100) ×100%

FAR=0%

The ideal FRR and FAR for the SM630 is less than 0.01% and 0.0001% respectively [16]. The experimental results thus confirm the same. It can be noted that the system may reject an authorized subject. This could be due to wrong alignment or fingerprint quality being poor. However, the system does not grant access to an imposter under any condition thus making the system ideal for highly restricted access control applications.

6. CONCLUSION

A computer based security system for restricted access control has been designed, implemented and tested. The main components of the system are fingerprint sensor module (SM630) and a LabVIEW program. The system has been successfully tested for training and verification performance. Quantities such as FRR and FAR have been determined. The proposed system can be an alternative access control to a restricted area in premises.

The proposed system can be enhanced by using a combination of biometric attributes for instance, the face and fingerprint. In the face recognition, the image processing algorithms can be developed using LabVIEW platform in conjunction with the IMAQ vision toolbox. The image can be captured using a USB camera. The SM630 is supposed to be off when not in use so as to improve its lifespan. Thus incorporating motion sensors at the entrance will assist in automatic powering of the system. Finally, a fingerprint sensor utilizing ultrasound technology should be used. This because ultrasound sensors do not reject dirty or poor quality fingerprints.

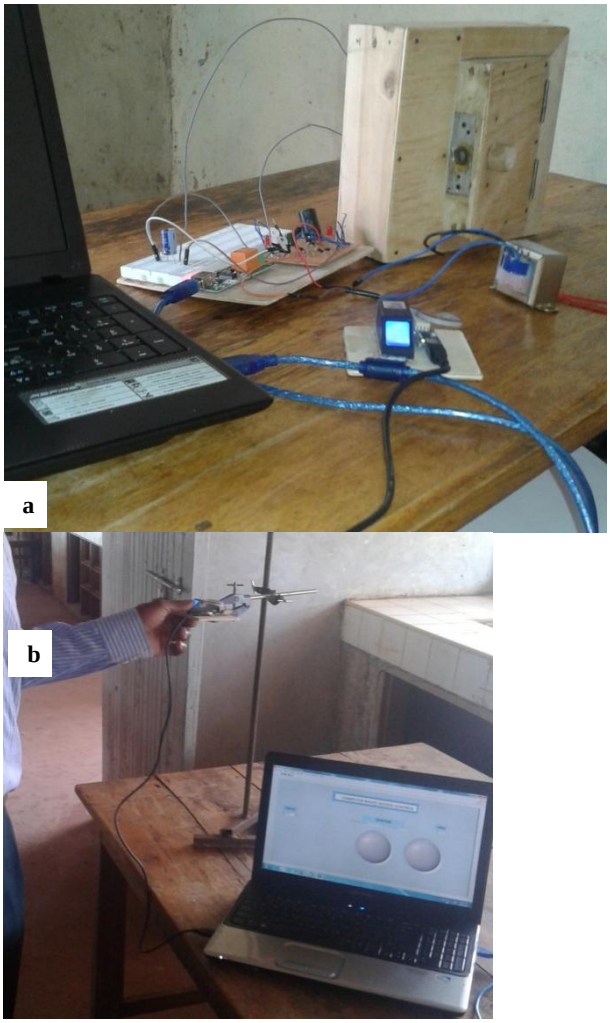

Figure 5: Photograph showing a prototype of the proposed system in (a) and testing in (b)

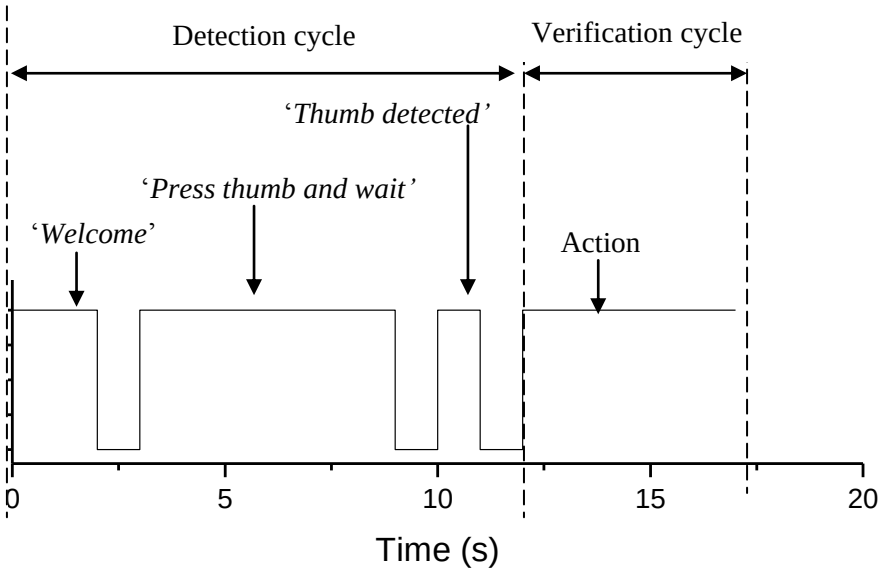

Figure 6: **The system response timing diagram**

7. REFERENCES

[1] Wahyudi, W.A and Mohamed, S. (2007). Intelligent Voice-Based Door Access control System Using Adaptive-Network Fuzzy Inference System (ANFIS) for Building Security. *Journal of computer Science 3(5)*: 274-280

[2] Oke, A.O., Olaniyi, O.M., Arulogun, O.T. and Oloniyani, O.M. (2009). Development of a Microcontroller-Controlled Security Door System. *The Pacific Journal of Science and Technology* 10, 398-403

[3] Osadciw, L., Varshney, P. and Veeramachaneni, K. (2002). Improving Personal Identification Accuracy Using Multisensor Fusion for Building Acess Control Application. *In Proceedings of the Fifth International Conference of Information Fusion*: 1176-1183

[4] Kung, S.Y., Mak, M.W. and Lin, S.H. (2004). Biometric Authentication: Machine Learning Approach. *Prentice Hall*.

[5] Chaudhry, K. and Nakra, P. (2004). Instrumentation, Measurement and Analysis. *Tata McGraw-Hill, New Delphi*.

[6] Ketui,D.K., Karimi,P.M., and Merenga, A.S. (2012). Design and Fabrication of a Computer Based Firefighting System Automated Using Labview. *International Journal of Current Research*. 4 (3): 258-263

[7] Agumba, J.O., Katana, G.G. and Karimi, P.M. (2011). Towards virtual laboratories: a survey of LabVIEW-based conduction of science experiments via the internet with an illustrative consideration of remote control of an oscilloscope. *International Journal of Current Research.* 33 (6): 123-127

[8] Arulogun, O.T., Omidiora, E.O., Olaniyi, O.M, and. Ipadeola, A. (2008). Development of Security System using Facial Recognition. *The Pacific Journal of Science and Technology* 9: 377-385

[9] Ashraf, E.S. (2011). Design and Implementation Biometrics control system Using Fingerprint for restricted area Based on Gabor Filter. *The International Arab Journal of Information technology* 8: 355-363

[10] Iwasokun, G.B (2015). Fingerprint Matching Using Minutiae-Singular Points Network. *International Journal of Signal Processing, Image and Pattern Recognition* 8: 375-388

[11] Kumar D. and Ummal S. (2013). A Comparative Study on Fingerprint Matching Algorithms for EVM. *Journal of Computer Sciences and Applications* 1(4) :55-60

[12] Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S. (2003). Handbook of Fingerprint Recognition. *Springer Verlag, New York*.

[13] Mazumdar, S. and Venkata, D. (2013). Biometric Security Using Fingerprint Recognition. *University of California, San Diego*

[14] Jain, A.K., Jianjiang, F. and Karthink, N. (2010). Fingerprint Matching. *IEEE Computer Society*, 36-44

[15] http://www.ftdichip.com/Drivers/VCP.htm accessed February 2017

[16] Miaxis Biometrics (2008). SM630 Fingerprint Verification Module User Manual. http:// www.miaxis.com

[17] http://www.ftdichip.com/products/ICs/FT245R.htm (2016). About FT245R