Design of a Fingerprint Biometric Access Control System with GSM Functionality

Terene Govender and Patrice Umenne

Electrical and Mining Engineering
University of South Africa
Johannesburg, South Africa
59467525@mylife.unisa.ac.za,   umennpo@unisa.ac.za

Abstract—**We live in a world with ever-increasing digital technology, hence the need for enhanced security systems is vital. In the past a simple PIN or password would have been sufficient to maintain the integrity of security systems, however with the advancements in technology, these are slowly becoming a secondary method of access control. Biometrics provide an enhanced level of security since they make use of unique characteristics or features of a person making them increasingly popular in security systems. This paper describes a project in which the fingerprint biometrics together with the Arduino Uno are used to provide access to a home security gate. A GSM module is appended to the system and used to provide an alert when unauthorized access occurs via a cellphone.**

Keywords—Arduino Uno, Access Control, Biometrics, Fingerprint, GSM.

I. INTRODUCTION

The current and continuous advancements in the use of technology, create the need for enhanced security. Traditional methods of securing a system such as pins, passwords and access cards can be cloned or replicated. These methods have previously been the cause of security breaches resulting in major data losses and the exposure of sensitive information. Residential security home access systems are often built with a simple key or keypad and an alarm system that uses a password. This is prone to methods of bypassing.

Safety is a concern as housebreaking [1] incidents are on the rise. Therefore, good security is one of the main measures that can be used to prevent housebreaking. Whilst biometric based security cannot alleviate the problem of security completely, it can at least add an enhanced level of security to any system. Unlike keys or passwords, biometric characteristics are unique to every individual and cannot be easily replicated.

Biometric technology [2-4] has become popular in recent years and a tried and trusted method in security access. These include methods such as fingerprints, retina, iris and voice recognition for access. Fingerprint technology incorporated with the Arduino Uno is described in this paper.

The current rise in crime statistics in South Africa, creates a demand for advancements in the technology used in home security systems. The introductions of biometrics to security enables the fabrication of more advanced home security systems that can create a safer living environment. Biometrics use unique human characteristics which add an extra layer of security to home security systems. Basic security systems with access codes or keypads can be easily breached. This paper describes a low-cost solution for a fingerprint based biometric access control system with GSM functionality.

II. LITERATURE REVIEW

Fingerprint biometric technology was used in a classroom attendance management system in [5]. This work involved the enrolment of each students fingerprints via the fingerprint module. If a match occurred a door was unlocked to the classroom. The door was then automatically closed after 5 secs. If a match does not occur an alarm is set off. The alarm has to be manually switched off. The tracking and storage of the fingerprints was done via an SQL server or database. In addition, all the timing information for the lecture such as the start and stop time, course codes and faculty details are stored in the database. There is a time period for the recording of the fingerprint, the fingerprint must be captured 5 mins before and 5 mins after the lecture time has started. If the fingerprint is not captured in the allocated time-frame, the fingerprint will be deemed invalid. Some false rejections occurred with users that were registered. This was due to wrong positioning of the fingerprint on the scanner.

A fingerprint-based security system for vehicles was implemented in [6]. There fingerprint control is used to put the vehicle into motion. A fingerprint will have to be enrolled and registered in the system for a person who is allowed to use the vehicle. Prior to using the vehicle, the fingerprint scanned needs to correspond to the fingerprint recorded in the database. Once a fingerprint match occurs a valve attached to the fuel tank is opened. If the fingerprint is authentication fails, the valve is closed. The fingerprint prototype is low-cost to the engineer; however, a valve has to be inserted into the fuel tank and such an addition to the vehicle could be costly and in general is done on special request.

A fingerprint sensor and GSM module are used to access an Automatic Teller Machine (ATM) in [7]. In this application, a fingerprint was registered and stored in the database. The cellular phone number of the customer is also stored in the database. When the customer makes use of the ATM, the fingerprint is initially scanned. If accepted, a one-time pin is sent to the user as in [4] via an SMS. The SMS is sent using the GSM module. The user then types in the received code and carries on with the transaction.

The paper in [8] details the design of a door access system which makes use of the iris biometric technique. The system makes use of an Arduino Uno and an iris scanner. The programming was done in C language. The iris of a user is initially enrolled and stored. When a user seeks entry their iris is scanned, the module searches for the registered irises in the

system and if a match is found access is granted. An LCD is used to display relevant messages.

An authentication device for examination purposes using fingerprint biometrics was designed in [9]. The demand for this project arose as a result of the fact that cheating was occurring during examinations in the form of people getting other people to write their examinations for them. In this system fingerprint authentication is done when a student enters an exam venue in order to identify the student partaking in the examination. In a sample study some students where registered with their fingerprints and some where not registered on the system. The students then scanned their fingerprints for verification on entry to an exam. The

unregistered students where not verified and where denied access to the examination.

III. METHODOLOGY

A. Technical Specifications and Circuit Design

The system consists of the Arduino Uno, R307 fingerprint scanner, a servomotor to open a gate or give access, a GSM module for communicating the status of access to cellphone, two LED's, LCD screen and limiting resistors. A relay is also used to drive the servomotor. The complete circuit diagram can be seen in Fig.1 below.
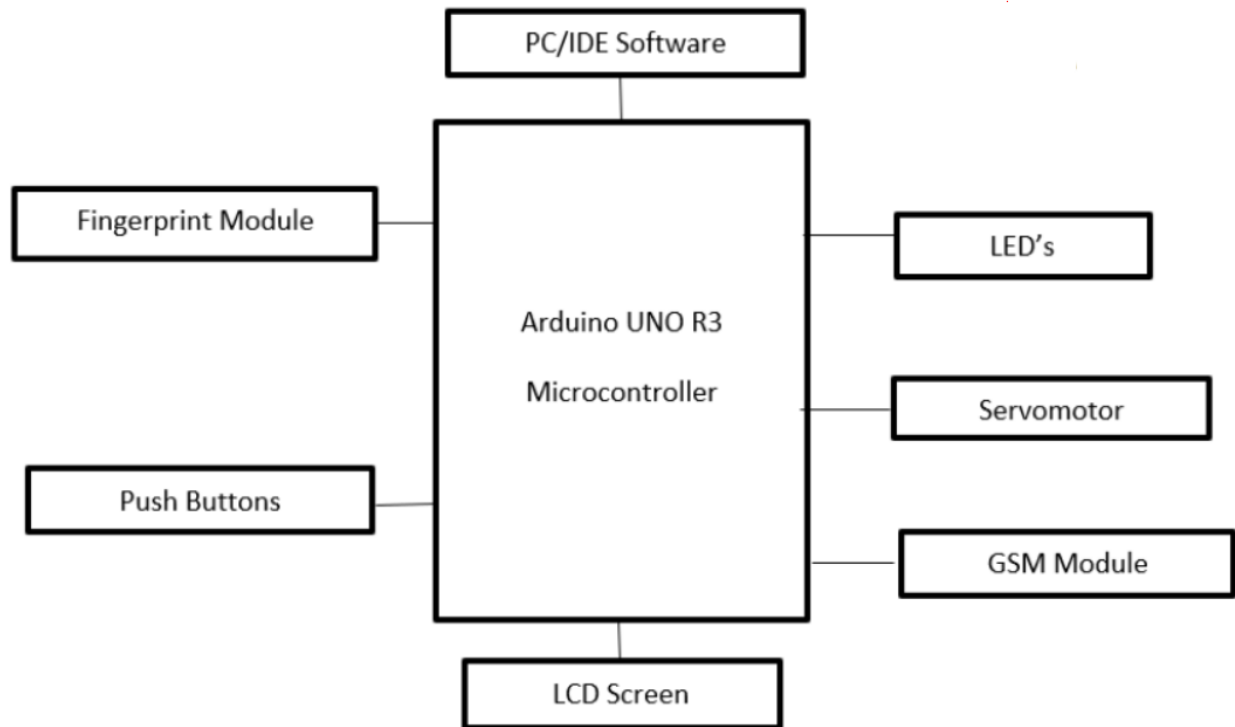

Fig. 1 Block diagram of Fingerprint Biometric Access Control.

B. Fingerprint Module

There are two steps followed when using a fingerprint scanner namely; the fingerprint enrolment step and the fingerprint verification step. In order to enroll a fingerprint, a fingerprint scanner is utilized. The optical component of the scanner passes light across the surface of the finger and creates a digital image. The fingerprint is scanned, a digital image is extracted and analyzed. The image is then stored in an encrypted form in a secure database, in this case the memory of the Arduino Uno. Following storage, the verification step then takes place. During verification step again the fingerprint is placed on the scanner. Once the scanning is completed, the digital image of the fingerprint is compared against the stored fingerprint images in the database. If a match occurs access is granted.

C. Arduino Uno

The Arduino Uno is the microcontroller used in this design to control the operation of all the peripheral components connected to it to give access control as seen in Fig.1. The Arduino Uno can be programmed and re-programmed to perform a specific function. It is an open source platform used for programming devices. The programming is done via the IDE software.

D. GSM Module

The GSM module in this design is used to communicate the status of the access control to a cellular phone that is "Access granted" or "Access denied". The GSM model used is the SIM900. The GSM module is connected to the Arduino Uno and a SIM card is inserted into the module. The GSM module is connected to two PWM enabled pins on the Arduino Uno.

The complete circuit diagram or prototype can be seen in Fig. 2 below. Incorporating the Arduino Uno, Servomotor, GSM module with sim card compatibility, fingerprint scanner, potentiometer for controlling the backend lighting of the LCD, the LCD, relay and the LED lights for indicating the status of access.
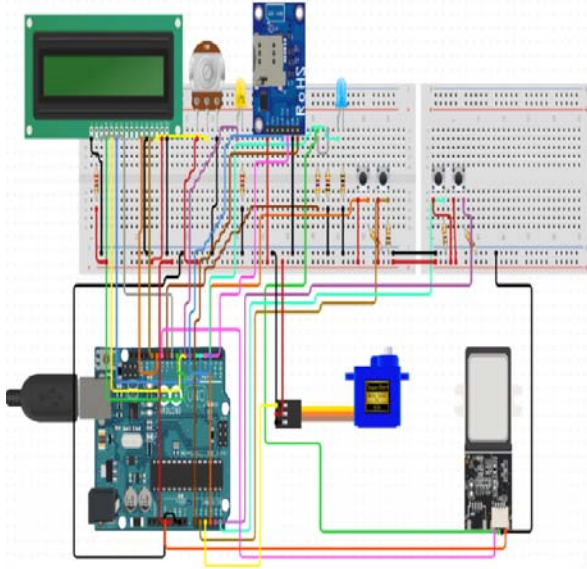

Fig. 2 Circuit diagram of the Fingerprint biometric access control

IV. EXPERIMENTS AND RESULTS

A fingerprint biometric access control system with GSM functionality was successfully designed and built. The solution can contribute to enhanced security for a gate access control in a home security system. The GSM module provides an added level of security since it communicates the status of the access to your cellular phone.

In general, the mode of operation is described as follows; there is a list of authorized users as in [10] that are permitted to access the system. The fingerprints are registered using the fingerprint scanner and the Arduino Uno [11-17] program stored in it. The LCD screen is initially programmed to display "Please scan finger" when the system is in its idle state. When a user scans their fingerprint on the fingerprint module, the algorithm programmed into the Arduino Uno [18-20] searches through its database to determine if the fingerprint matches any digital image of fingerprints in the system. If it detects a match, the servo motor will switch on and operate a gate to give access. The LCD screen at this point displays a message titled "Access granted" as displayed in Fig 3a. A yellow LED also lights up to verify access is permitted. If the fingerprint is not found on the database, meaning it's an unauthorized fingerprint, the relay does not switch on the servomotor and the access gate is not opened. The LCD in this case displays "Access denied" as can be seen in Fig.3b. In this event the RED LED lights up.
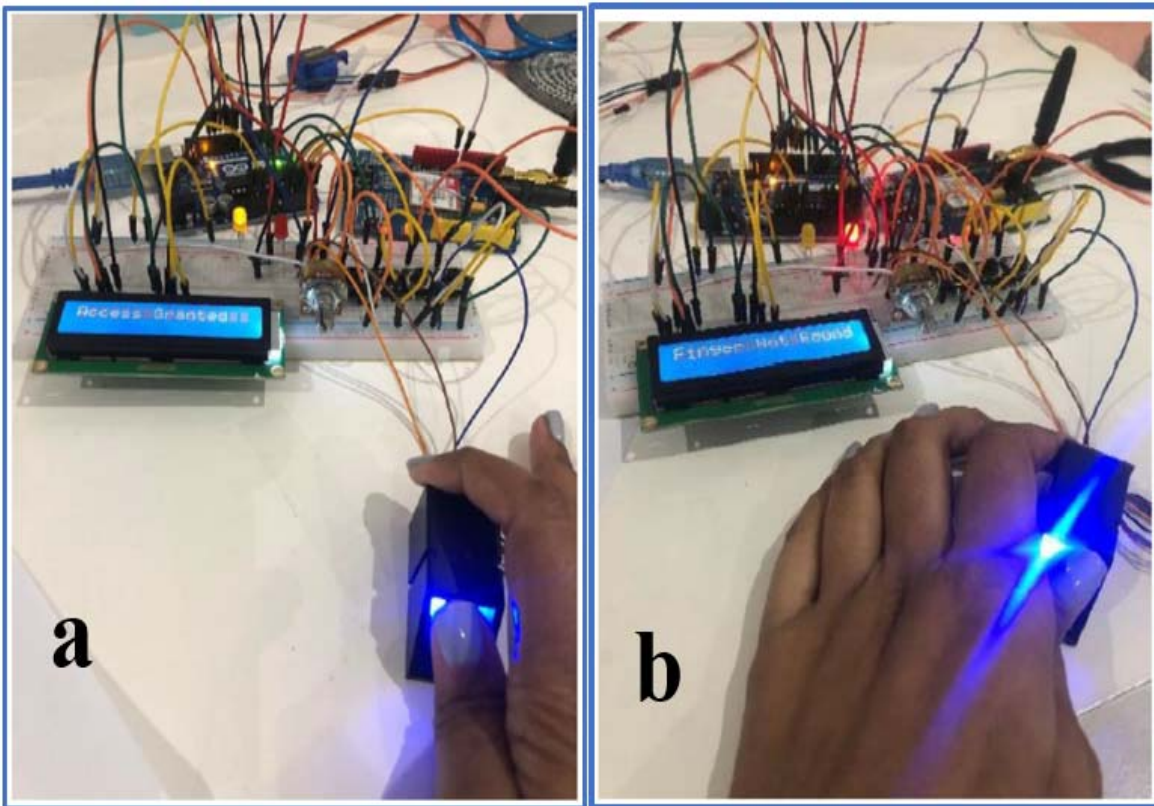

Fig. 3a. Fingerprint biometric access control system when Access is granted and 3b. Access is denied.

When access is not granted the GSM, module sends an SMS to the cellphone of the home occupant indicating that there has been an attempt to breach the home. This SMS basically states that there has been an "Unauthorized user attempt to gain access" as can be seen in Fig. 4 below.
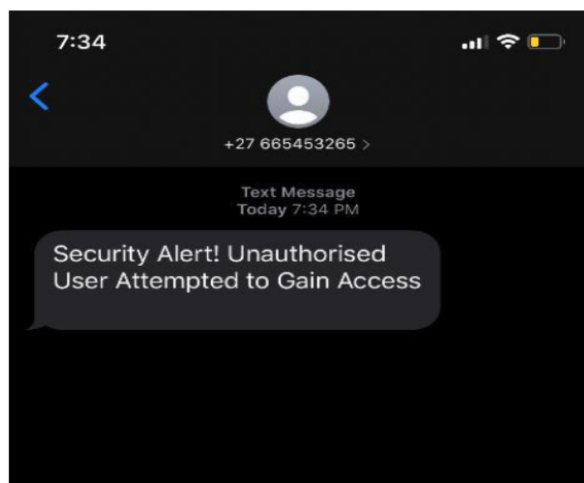

Fig. 4 SMS Notification of gate Access

Improvements can be made to the biometric access control system such that it can send an SMS for both authorized and unauthorized access attempts to the occupants cellphone. The project is intended for low cost small-scale home utilization and implementation.

A. Testing the system for Authorized and UnAuthorized Entry

The fingerprint biometric access control was tested for its performance when authorized and unauthorized fingerprints where scanned. In the first instance a fingerprint that had been stored in the system for authorized access was scanned several times to determine how many times it will grant access and how many times it will reject access even though authorized. The results show an accuracy of 71% as can be seen in Table I below. Basically 71% of the time when the authorized fingerprint is scanned it grants access.

TABLE I TESTING AUTHORIZED FINGERPRINT

Test Number	Fingerprint Accepted (Y/N) and access granted
1	Yes
2	Yes
3	No
4	Yes
5	Yes
6	No
7	Yes

In the next test an unauthorized fingerprint or a fingerprint not registered for access was tested. The results show in Table II below, 100% accuracy. Basically, the same unauthorized finger was scanned for access several times. 100% of the time the fingerprint was not accepted for access.

TABLE II TESTING UNAUTHORIZED FINGERPRINT

Test Number	Result Fingerprint accepted or rejected access
1	Rejected Access
2	Rejected Access
3	Rejected Access
4	Rejected Access
5	Rejected Access
6	Rejected Access
7	Rejected Access

In the last test the GSM module functionality to communicate with the aid of an SMS the status of unauthorized entry was tested. Based on Table III below, its shows that this test was 89% accurate. Basically 89% of the time an SMS is sent the cellular phone of the occupant warning him/her that unauthorized entry has occurred accurately.

TABLE III ACCURACY OF SENDING SMS IN THE EVENT OF UNAUTHORIZED ACCESS

Test Number	SMS Sent (Y/N)
1	N
2	Y
3	Y
4	Y
5	Y
6	Y
7	Y
8	Y
9	Y

V. Conclusion

In this paper we designed a fingerprint based biometric access control system for a home security system where the access point is via a gate. The fingerprint biometric access control makes use of the Arduino Uno, servomotor, LCD screen, relay and a GSM module as the main components. In this project a GSM module is used to inform or communicate to the home occupant when unauthorized entry occurs via an SMS message to a cellular phone. Initially a fingerprint which constitutes authorized entry is stored in the database by scanning and registering the fingerprint into storage. Subsequently on entry the fingerprint is scanned again and since its authorized access is granted. The system is then tested. First the system is tested for authorized entry, and the system is found to be 71% accurate. Meaning that when an authorized fingerprint is scanned it gives access 71% of the time. For the test of unauthorized entry, the system is 100% accurate. Preventing access 100% of the time. Lastly when the GSM messaging functionality is tested, during unauthorized entry, the system is 89% accurate. The system sends a message to the home occupant indicating unauthorized entry 89% of the time.

VI FUTURE WORK

In this project the future work would include adapting the fingerprint biometric system to be able to send an SMS via the GSM module to the occupant both for the scenario in which there is unauthorized entry as well as the scenario in which there is authorized entry to inform the occupant.

REFERENCES

[1] L. A. Hamid and W. Z. M. Yusof, "Experiential Approach as a Design Innovation Solution to Prevent House Breaking Crime", *Procedia – Social and Behavioral Sciences*, Vol. 107, pp. 145-152, 11th December 2013, Available online: https://doi.org/10.1016/j.sbspro.2014.02.293.

[2] A. K. Jain, "Biometric Recognition:Overview and Recent Advances", *Iberoamerican congress on Pattern Recognition (CIARP 207): Progress in Pattern Recognition, Image Analysis and Applications*, pp 13-19, doi: 10.1007/978-3-540-76725-1_2.

[3] M. F. Zanuy, "Biometric security technology", *IEEE Aerospace and Electronic Systems Magazine*, vol. 21, no. 6, June 2006, ISSN 0885-8985, doi: 10.1109/MAES.2006.1662038.

[4] R. Malathi and R. Jeberson, "An Integrated Approach of Physical Biometric Authentication System", *Procedia Computer Science*, vol. 85, pp. 820-826, 2016. Available Online: https://doi.org/10.1016/j.procs.2016.05.271

[5] Y. Mittal, A. Varshney, P. Aggarwal, K. Matani and V.K. Mittal, "Fingerprint biometric based Access Control and Classroom Attendance Management System", *Annual IEEE India Conference (INDICON)*, 17 – 20th December, 2015, New Delhi, India, ISBN 978-1-4673-7399-9, doi: 10.1109/INDICON.2015.7443699

[6] S. Namboodiri and P. Arun, "Fingerprint based security for vehicles", *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 4, no. 4, 2018, Availble online: www.ijariit.com.

[7] A. J. Bamidele and J. R. Gbenga, "Secure Automated Teller Machine (ATM) Using fingerprint Authentication and Short-code Message in a cashless society", *University of Ilorin*, Ilorin, Nigeria.

[8] Etinosa Noma-Osaghae, Robert Okonigene, Chinonso Okereke and Olatunji J. Okesola, "Design and Implementation of an Iris Biometric Door Access Control System", Covenant University, Nigeria, 2017.

[9] E.P. Ogherohwo and E.O. Ezeoba, "Design and Construction of a Biometric Examination Authentication Device", International Journal of Advanced Research in Physical Science (IJARPS), vol. 3 no. 5, pp. 29-39, 2016, ISSN 2349-7874.

[10] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, "Sacalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, January 2013, ISSN 1045-9219, doi: 10.1109/TPDS.2012.97

[11] T. W. Schubert, A. D'Ausilio and R. Canto, "Using Arduino microcontroller boards to measure response latencies", *Behavior Research Methods*, vol. **45**, pp. 1332-1346, 2013, doi: 10.3758/s13428-013-0336-z

[12] A. D'Ausilio, "Arduino: A low-cost multipurpose lab equipment", *Behavior Research Methods*, vol. 44, pp. 305-313, 2012, doi: 10.3758/s13428-011-0163-z.

[13] I. Kotseva, M. Gaydarova, K. Angelov and F. Hoxha, "Physics experiments and demonstrations based on Arduino", *AIP Conference Proceedings*, vol. 2075, pp. 180020, 2019, Available online: https://doi.org/10.1063/1.5091417

[14] R. Saha, S. Biswas, S. Sarmah, S. Karmakar and P. Das, "A Working Prototype Using DS18B20 Temperature Sensor and Arduino for Health Monitoring", *SN Computer Science*, vol. 2, Article Number 33, 2021, Available Online: https://doi.org/10.1007/s42979-020-00434-2

[15] K. K. Kumar, E. Ramaraj and P. Geetha, "IoT Based Trash Collection Bin Using Arduino", *Journal of Critical Reviews*, vol. 7, no. 4, 2020, ISSN: 2394-5125.

[16] P. W. Digarse and S. L. Patil, "Arduino UNO and GSM based wireless health monitoring sytem for patients", *International Conference on Intelligent Computing and Control Systems (ICICCS)*, 15-16th June 2017, Madurai, India, ISBN: 978-1-5386-2745-7, doi: 10.1109/ICCONS.2017.8250529

[17] S. Chaouch, M. Hasni, A. Boutaghane, B. Babes, M. Mezaache, S. Slimane and M. Djenaihi, "DC-Motor Control using Arduino-Uno Board for Wire-Feed System", *International conference on Electrical Sciences and Technologies in Maghreb*, 28-31 October, 2018, Algiers, Algeria, ISBN: 978-1-5386-4988-6, doi: 10.1109/CISTEM.2018.8613492

[18] L. Chen, J. Zhang and Y. Wang, "Wireless Car contol System Based in ARDUINO UNO R3", *2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, 25-27th May 2018, Xi'an, China, ISBN: 978-1-5386-1803-5, doi: 10.1109/IMCEC.2018.8469286

[19] P. Madan, L. Dhama, R. Dahiya and R. Doda, "A Review Paper on Arduino Research Papers", *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 7, no 3, 2019, ISSN: 2321-9653.

[20] A. M. Chaudry, "Using Arduino Uno Microcontroller to Create Interest in Physics", *The Physics Teacher*, vol. 58, pp. 418, 2020, Available Online: https://doi.org/10.1119/10.0001841