Finger Print Based Automotive Security Lock System

Lennox M. Mwaringa and Theophilus Biketi

***Abstract*—** The vehicle anti-theft system presented in this paper consists of double layers of protection with one complementing the other, rather than the conventional anti-theft system where only one particular system is used. The first layer of protection in the system is a fingerprint recognition, from which the doors and drive implements are opened. The fingerprint matching is done by utilizing the minutiae based fingerprint recognition scheme. The second layer consists of a Dual Tone Multi Frequency (DTMF) module which uses mobile phone to effect control over a long distance, just in case thieves break the glass and get access to the vehicle. The vehicle can be turned on by a start button upon verification by the system. No mechanical keys are used in this system. When finger ID entered is not correct, or a wrong DTMF password is entered will result in vehicle getting immobilized by keeping the door door locked, cutting the fuel supply and switching off the ignition power, an alarm will turned on to alert people in the vicinity of the vehicle. The different layers of protection defined are controlled by an AVR based controller acting as the central node. The whole system was tested using a test set up by mimicking the vehicle door, whereas fingerprint and DTMF data was received from the system. Output signals from the microcontroller proved that the functionality of the anti-theft system in good working condition.

***Keywords*—** AVR, DTMF, Fingerprint recognition.

I. Introduction

THE rapid rate at which vehicle thefts has been increasing across the world has called for increasing thrust in the field of vehicle locking systems. This particularly assumes significance for expensive vehicles and those who go behind even more expensive cosmetic modifications. The vehicle locking system typically performs two functions (1) detecting vehicle unauthorized entry and preventing false alarms (2) alerting the owner. The main focus while developing the vehicle locking system was to integrate the above features equally. The most important feature is the vehicle security from theft and it has been ensured by providing two layers of anti-theft protection. First the entry to the vehicle is restricted only to the authorized persons with the help of a fingerprint recognizer. The Fingerprint of the owner and other authorized persons are stored into the database beforehand and at the time of entry to the vehicle, scanned fingerprints are crosschecked with the database. The biometric scheme is used as the primary layer of protection since the chances of it being duplicated are very minimal. Also additional DTMF module is integrated to the system to allow both short and long distance wireless remote operation of the vehicle. This paper had few assumptions made during the design process of this system; the authorized users will have no injuries that will damage their finger print; no two authenticated users can have the same finger print; there will be no network delays or failures during remote operation using DTMF over a long distance. This vehicle locking security system showed several advantages over other previous locking mechanisms and had few limitations. The advantages are; firstly, the operation of this lock is keyless; hence no inconvenience carrying and losing keys; secondly, high security as no two persons can have similar finger print; thirdly, the use of master keys and other crude means to open the vehicle door are made impossible by this locking system; fourthly, the system has long distance wireless remote operation using cell phone DTMF which makes it more convenient and finally, the system has a separate power supply battery hence not affected when the vehicle battery dies or gets damaged. However the limitations are firstly, authenticated users can get injuries that will damage their finger prints; secondly, network failures or delays can occur during long distance remote operation with DTMF, thirdly the system requires the owner of the vehicle to be computer literate The current vehicle door key locking system has a major weakness, as keys can be duplicated or forged to open the door easily; also it experiences memory loss when the car battery is removed. Thieves have taken it as an advantage steal peoples vehicles.

This challenge motivated me to design a finger print based security lock, whose operation will be keyless and of high reliability. The lock will also have wireless DTMF operation to enable long distance access.

II. Related Work

The Vehicle locking Systems has been an area of interest for many researchers. A lot of work done on the area focused on cutting down the vehicle to functions should there be an attempt to steal the vehicle. Fingerprint based authentication most advanced and accepted biometrics technologies [5], [6], [7], [8]. Gonzalez *et al* the fingerprint scanner and DTMF module denies access to all unauthorized persons. These are generally referred to as Vehicle keyless entry Systems and are useful in controlling and immobilizing stolen vehicles [1].

Antonelli *et al* introduced an auto tamper detection

L. M. Mwaringa, Department of Electrical and Electronic Engineering, Technical university of Mombasa (phone: +254788886644; fax: +254 41 2495632; e-mail: lmmwaringa@tum.ac.ke).

B. Theophilus, Department of Electrical and Electronic Engineering, Technical University of Mombasa (e-mail: obiketi@gmail.com).

technology which disables the vehicle in case of tampering in the car security system. The vehicle immobilization scheme is the next biggest security feature that has been added in the recent years [3]. Fernandez *et al* implemented a security system based on the keyless entry and which immobilizes the vehicle in case of tempering with the vehicle [2]. Washington *et al* invented a system to be used in an automobile, the system has a reader which reads the fingerprint or the retina, the information from the reader is compared with the stored data to determine whether the driver is allowed to drive the vehicle [9]. Bonder *et al* invented an intelligent key that has a scanning chip on the surface that could distinguish between fingerprints. The lock had electrical contacts which come into with the electrical contacts of the intelligent key when the key is inserted. Upon inserting the intelligent key, power is provided to the intelligent key through the electrical contacts to the key lock controller which controls the ignition system of the vehicle [10]. A fingerprint and DTMF scheme is used in this work instead of other biometric techniques such as face recognition, since it is both cost effective and efficient.

III. Design Approach

A. System Design

A model of the fingerprint based automotive security lock system has hereby been constructed. The design of the locking system has been done with the aim of making efficient and advanced modules that are being employed. Also care has been taken to make sure that the functioning of one module does not affect the performance of another. The design of the system adopted two design approaches: modularization and top down approach. Modularization involves dividing the entire design work into activity groups or modules. It consists of three phases namely; conception phase, design phase and integration phase. In conception phase the problem is defined in a manner leading to the real solution, the factors to be considered are clearly outlined, and also the grouping or partitioning of activities into sub activities or modules normally occurs here. Design phase deals with establishing the main algorithm for the entire program i.e. constructing a hierarchy chart that shows the relationship between different modules in the entire system. Lastly in integration phase all the modules are put together through appropriate module interface and software to become a system that satisfies the requirements define in the first phase. On the other hand top down approach involves design of complex modules first, after which other simple or less involving modules will follow.

B. System Operation

The finger print based automotive security lock system, is a locking mechanism designed to replace the available vehicle key/remote key door locking system. It uses finger print ID or DTMF password as a means of authentication before access. The system has a finger print scanner which is used to scan the finger print images, processing and storage in the data base. An embedded C program loaded into an Atmel microcontroller used to coordinate the issuing of commands to the finger print scanner during finger enrollment and verification. Additional computer software is needed to enhance the enrollment process.

Users are required to enroll finger print images and store them in the data base after processing. During verification the user puts the finger on the scanner and the image taken is used to match with those stored in the data successful matching an acknowledgement signal is send to the process microcontroller 1 from the scanner CPU. The process microcontroller1 then sends a control command to system process microcontroller 2 to activate the actuators. Else a failure signal is sent to process microcontroller1 which terminates the process.

The DTMF module is connected to system processor microcontroller 2 and provides a second means of opening the door by typing in the password on the phone's keypad. The module decodes the audible tones from the phones key pad and converts them into an equivalent binary number

The system process microcontroller 2 converts these binary numbers into decimals and displays on the LCD display; it also compares the number displayed to the password stored memory. If the binary number is equal to the password, then access is granted and actuators are activated. The DTMF provides both short range and long range remote operation as it has a cell phone with automatic call answering permanently connected to the system.

Actuators used in the system include: solenoid lock for the door locking mechanism, solenoid valve used to control fuel inlet to the engine and a relay for switching on the ignition power. The main source of power to this system is a separate 12v 7AH battery which is recharged from the vehicle's alternator DC supply.

C. Analysis of Distinctive Fingerprint Features

A fingerprint is composed of a pattern of interleaved ridges and valleys. They smoothly flow in parallel and sometimes terminate or bifurcate. At a global level, this pattern sometimes exhibits a number of particular shapes called singularities, which can be classified into three types: loop, delta and whorl, as shown in Fig. 1. At a local level, the ridges and valleys pattern can exhibit a particular shape called minutia. There are several types of minutiae, but for practical reasons, only two types of minutiae are considered: ridge ending and ridge bifurcation. Singularities at the global level are commonly used for fingerprint classification, which simplifies search and retrieval across a large database of fingerprint images.

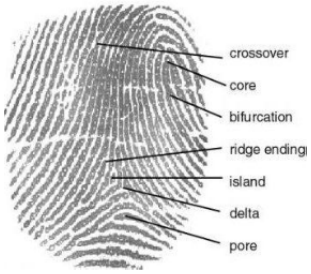

Fig 1. Finger Print Image

D. Fingerprint Image Processing by Minutiae Technique

At first, finger print images are taken with the help of input device. After taking the images, the proposed methodology finds the ridge pattern in different portions of finger print. , the methodology follows the steps shown in Fig. 2.

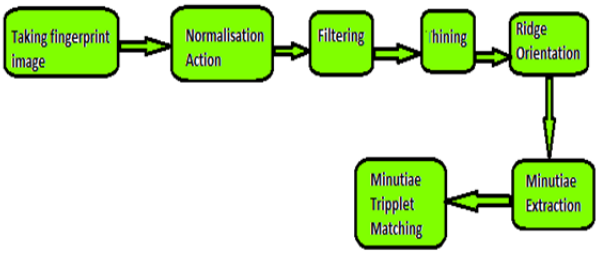

Fig 2. Fingerprint Image Processing by Minutiae Technique

The first step involves is taking image with the help of input devices like camera, sensors, etc.; the second step involves is normalization. This process includes gray scale conversion of the image of the fingerprint. The third step involves filtering. The sensor from which the image is taken may be old or pore with dust. At old age, a person's fingerprint may not be clear at all; because the, because the ridges of his/her fingerprints become into broken parts. So, for better calculation this fingerprints need to be redrawn and filtered for getting approximate full ridge print. The fourth is thinning. After normalizing and filtering the images they are thinned for removing noises and make the ridges thinned. This is done for getting the proper ridge orientation and minutiae features. Fifth is Ridge Orientation. The image is first converted into binary format. Here, RBG color is checked. If RBG is (0, 0, 0) then it is black. For this reason one pixel is put color match.

If RBG is (255, 255, 255) then it is white point. Nothing is needed to do for it. The direction-field of ridges is taken for getting the angle of minutiae in the fingerprint. Joining of points on ridges, which are created at time of filtering and thinning give the directional field for ridges. This also helps to find out the minutiae points.

E. Dual Tone Multi Frequency Module

Use DTMF is a common communication term for touch tone phones. The tones formed when dialing on the keypad (DTMF digits or DTMF number) on the phone can be used to characterize the digits, and some different tone is used for each digit. DTMF signaling is mainly used in DTMF phones, telephone switching system.

F. Working of DTMF Decoder Circuit

DTMF keypads are employed in almost all landline and mobile handsets. Thus this technology is used in the telephone switching centers to identify the number dialed by the caller. The decoder distinguishes the DTMF tones and produces the binary sequence equivalent to key pressed in a DTMF keypad. The circuit uses MT8870 DTMF decoder IC which decodes tone generated by the keypad of cell phone. DTMF signals can be tapped directly from the microphone pin of cell phone device.

G. System Module Integration

Module integration is the act of joining different functional modules together to work as one coordinated system. Following the modularization design approach this was its last phase in system design. Since five functional modules were involved, a control C program was written and loaded into system process microcontroller 2 to coordinate the operation of all modules.

IV. TESTING

The testing of the locking system was done using a specially made test set up. The fingerprint scanner was tested for finger print enrollment and verification, while DTMF module was tested for short and long distance wireless operation.

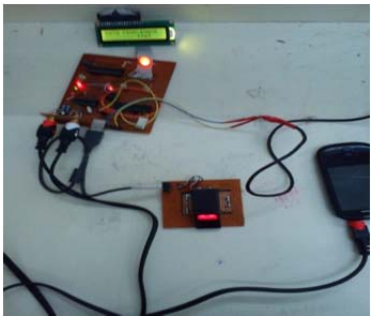

Fig 3. Fingerprint security lock system

V. CONCLUSION

The design and implementation of the finger print based automotive security lock was achieved, when all the system modules designed separately were integrated to function together as a system It was possible to create a finger print image data base using the microcontroller loaded with an embedded C program, the enrollment and verification of finger print images to and from the data base was successful using commands.

REFERENCES

[1] G. AGonzalez-Rodriguez.2004, Fingerprint Minutiae Format for Data Interchange. [e-book] American National Standard pp. 205–212, http: //www.eecs.ucf.edu/[Accessed 10 10 2014].

[2] Alonso-Fernandez, Ortega-Garcia, 2007: A comparative study of fingerprint image quality estimation methods. [e-book] IEEE Trans. on Information Forensics Security pp. 153–186, www.blog.oscarlang.net. [Accessed 20 1 2015].

[3] Antonelli, A., Capelli, R., Maio, D., Maltoni, D 2006. Fake finger detection by skin distortion analysis. [e-book] IEEE Trans. on Information Forensics and Security 1"http://www.dca.gov.uk/elections/e-voting/pdf/e-summary.pdf." [Accessed 20 1 2015]

[4] Bazen, Gerez, 2002. *Systematic methods for the computation of the directional fields and Singular points of fingerprints*. [e-book] Proc. Workshop on Biometrics pp. 200–212 http://www.enterstageright. Com [Accessed 20 2 2015]

[5] Racha N. K et al (2003)., *Secure Data hyding in wavelet Compressed Fingerprint Images*. ACM Multimedia workshop Marina Del Rey CA USA.

[6] Nagar et al (2009)., A hybrid biometric crypto system for securing fingerprint mutiaetemplates: Pattern recognition Lett. 2009 doi10.1016/j patre .20090.09.003.

[7] Farina A et al. (1998)., Fingerprint minutiae xtraction from skeletonized binary images. Journal of the pattern recognition society, Bologna Italy (1998)

[8] Jain K. A (2000)., *Filter bank based fingerprint matching*. IEEE transactions in Image processing Vol 9 No. 5. (2000)

[9] Washington et al (1997)., *Vehicle security system including fingerprint and eyeball part identification*. United states patent no. 5686765. Nov 11, 1997.

[10] Bonder and fisher