European Journal of Scientific Research
ISSN 1450-216X Vol.62 No.2 (2011), pp. 164-171

http://www.eurojournals.com/ejsr.htm

A Prototype of a Fingerprint Based Ignition Systems in Vehicles

Omidiora E. O.
Department of Computer Science & Engineering
E-mail:omidiorasayo@yahoo.co.uk

Fakolujo O. A.
Department of Electronic & Electrical Engineering
University of Ibadan, Ibadan, Nigeria

Arulogun O. T.
Department of Computer Science & Engineering

Aborisade D. O.
Department of Electronic & Electrical Engineering
Ladoke Akintola University of Technology, Ogbomoso, Nigeria

Abstract

Biometric systems have overtime served as robust security mechanisms in various domains. Fingerprints are the oldest and most widely used form of biometric identification. A critical step in exploring its advantages is to adopt it for use as a form of security in already existing systems, such as vehicles.

This research work focuses on the use of fingerprints for vehicle ignition, as opposed to the conventional method of using keys. The prototype system could be divided into the following modules: fingerprint analysis software module that accepts fingerprints images; hardware interface module and the ignition system module. The fingerprint recognition software enables fingerprints of valid users of the vehicle to be enrolled in a database. Before any user can ignite the vehicle, his/her fingerprint image is matched against the fingerprints in the database while users with no match in the database are prevented from igniting the vehicle. Control for the ignition system of the vehicle is achieved by sending appropriate signals to the parallel port of the computer and subsequently to the interface control circuit.

The developed prototype serves as an impetus to drive future research, geared towards developing a more robust and embedded real-time fingerprint based ignition systems in vehicles.

Keywords: Fingerprints, Biometrics, Ignition, Interface, Vehicles

1. Introduction

Biometrics refers to the automatic identification of a living person based on physiological or behavioral characteristics for authentication purpose (Omidiora, 2006). Among the existing biometric

technologies are the face recognition, fingerprint recognition, finger-geometry, hand geometry, iris recognition, vein recognition, voice recognition and signature recognition (Graevenitz, 2003).

Biometric method requires the physical presence of the person to be identified. This emphasizes its preference over the traditional method of identifying 'what you have' such as, the use of password, a smartcard etc. Also, it potentially prevents unauthorized admittance to access control systems or fraudulent use of ATMs, Time & Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, vehicles and computer networks. Biometric recognition systems offer greater security and convenience than traditional methods of personal recognition (Yang and Verbauwhede, 2003).

Fingerprint recognition represents the oldest method of biometric identification which is dated back to 2200 BC. The use of fingerprints as a personal code has a long tradition and was already used by the Assyrians, the Babylonians, the Chinese and the Japanese (Graevenitz, 2003).

All human beings have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows/valleys on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending (*http://www.biometricinfo.org/fingerprintrecognition.htm*). Fingerprint images are rarely of perfect quality. They may be degraded and corrupted with elements of noise due to many factors including variations in skin and impression conditions. This degradation can result in a significant number of spurious minutiae being created and genuine minutiae being ignored. Thus, it is necessary to employ image enhancement techniques prior to minutiae extraction to obtain a more reliable estimate of minutiae locations. (Thai, 2003)

The prices of fingerprint recognition systems compared to other biometric systems are quite low and the user acceptance is very high. The strength of fingerprint identification is that it can be deployed in a varied range of environments. Also, it is a proven core technology and, the ability of enrolling multiple fingers can increase the system accuracy and the flexibility dramatically (Graevenitz, 2003).

There is a present demand for robust security systems in vehicles. Therefore, the usefulness of designing and implementing a biometric security system using fingerprint technology, to prevent unauthorized vehicle ignition cannot be overemphasized.

1.1. Fingerprint Basics

All humans have minute raised ridges of skin on the inside surfaces of their hands and fingers and on the bottom surfaces of their feet and toes, known as 'friction ridge skin'. The friction ridges provide a gripping surface in much the same way that the tread pattern of a car tyre does (*http://www.crimtrac.gov.au/fingerprintanalysis.htm*). Friction ridge skin constitutes the only skin on the body without hairs. Fingerprints are patterns of ridges and valleys on the surface of the finger.

Like everything in the human body, these ridges form through a combination of genetic and environmental factors. The genetic code in DNA gives general orders on the way skin should form in a developing fetus, but the specific way it forms is a result of random events. The exact position of the fetus in the womb at a particular moment and the exact composition and density of surrounding amniotic fluid decides how every individual ridge will form (*http://www.computer.howstuffworks.com/fingerprintscanner.htm*). This development process occurs in such a way that, in the entire course of human history, there is virtually no possibility of the same exact pattern forming twice.

Consequently, fingerprints are a unique marker for every person, even identical twins. No matter how similar two prints may look at a glance, a trained investigator or suitable software can pick out clear, defined differences. This is the basic idea of fingerprint analysis, in both crime investigation and security (*http://www.computer- .howstuffworks.com/fingerprintscanner.htm*).The two fundamental principles underlying the use of fingerprints as a means of identifying individuals are: immutability and individuality or uniqueness.

Immutability: This refers to the permanent and unchanging character of the pattern on each Finger. Several years accumulated fingerprint study and experience has demonstrated that friction ridge patterns do not change naturally during the life of a person. This pattern starts developing in the third month of pregnancy and is fully formed by the fourth month. During a person's lifetime, the pattern remains the same, apart from changing in size or by accident, mutilation or skin disease, until death. In fact, the friction ridge patterns will remain after death until the body decomposes (*http://www.crimtrac.gov.au/fingerprintanalysis.htm*).

Uniqueness: Individuality refers to the uniqueness of ridge details across individuals; the probability that two fingerprints are alike is about 1 in $1.9x10^{15}$ (*http://webfealb.fea.aub.edu.lb/dsa/labs/projectv1.1.pdf*). Friction ridge detail forms in a purely random manner during foetal development in the womb. There is sufficient variability in the arrangement of minutiae to ensure that no two friction ridge patterns are identical, whether they are on different fingers of the same person or on the fingers of different people (*http://www.crimtrac.gov.au/fingerprintanalysis.htm*). Although this is difficult to prove empirically, no two fingerprints have ever been found to be identical in over a century of the use of fingerprinting. Studies have further shown that while identical twins share the same DNA profile markers, they can nevertheless be differentiated by their fingerprints.

1.2. Minutiae Based Approach in Fingerprint Recognition

Most automatic systems for fingerprint comparison are based on minutiae matching Minutiae are local discontinuities in the fingerprint pattern. A total of 150 different minutiae types have been identified. In practice only ridge ending and ridge bifurcation minutiae types are used in fingerprint recognition (*http://webfealb.fea.aub.edu.lb/dsa/labs/projectv1.1.pdf*). Some of the different types of minutiae are shown in figures 1 (a) and 1(b) below:

Figure 1: *(a) Some different types of minutiae*

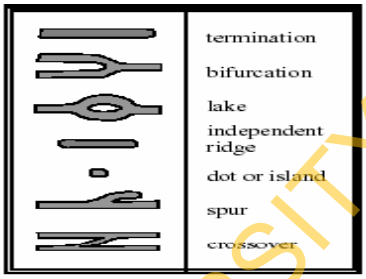
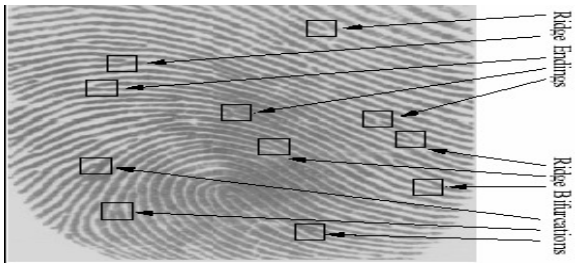


Figure 1: *(b) Ridge bifurcation & ending*



Fingerprint recognition systems based on minutiae consist mainly of three stages: Image acquisition/pre-processing, locating the minutiae, and comparing the minutiae list of both fingerprints, often solved as a constrained graph matching problem. This process has many stumbling blocks. Each of the processing steps requires careful fine-tuning of parameters and handling of ambiguous cases. Thus, the whole process of comparing two fingerprints may become rather time-consuming (Anton, 2002; Koichi et al, 2005).

Typical fingerprint recognition methods employ feature-based matching, where minutiae mostly ridge ending and ridge bifurcation are extracted from the registered fingerprint image and the input fingerprint image, and the number of corresponding minutiae pairs between the two images is used to recognize a valid fingerprint image. Minutiae-based matching is highly robust against nonlinear fingerprint distortion, but shows only limited capability for recognizing poor-quality fingerprint images due to unexpected fingertip conditions (e.g., dry fingertips, rough fingertips, allergic-skin fingertips) as well as weak impression of fingerprints.

2. Interfacing through the PC Parallel Port

External devices (hardware) can be controlled through the PC parallel port. This is known as hardware interfacing. It enables communication between a designed hardware and a digital computer. The modes of communication and the system operation are controlled by a program or codes that are resident on the digital computer.

The parallel port is a simple and inexpensive tool for building computer controlled devices and projects. It is often used in computer controlled robots, Atmel/PIC programmers, home automation etc. The primary use of a parallel port is to connect printers to computers but many other types of hardware for that port is available today. Thus it is often called the printer port or centronics port (after a popular printer manufacturing company 'centronics' who devised some standards for the parallel port) (AlphaSigmaura Team, 2005) .The parallel port connector is located in the rear panel of a PC. It is a 25 pin D-shaped (DB25) female connector to which the printer or other devices may be connected. Not all 25 pins are needed always. Usually only 8 output pins (data lines) and signal ground are used. The parallel port data pins are TTL outputs, that can both sink and source current. In ordinary parallel port implementations the data outputs are 74LS374 IC totem-pole TTL outputs which can source 2.6mA and sink 24mA (Engdahl, 2005). On almost all PC's only one parallel port is present, but more can be added by buying and inserting ISA/PCI parallel ports cards. When a PC sends data to a printer or other device using a parallel port, it sends 8 bits (1 byte) of data at a time. These 8 bits are transmitted parallel to each other; as opposed to the same 8 bits being transmitted serially through a serial a serial port. The standard parallel port is capable of sending 50 to 100 kilobytes of data per second (AlphaSigmaura Team, 2005).

The lines that connect to the DB25 connector are divided into three groups: data lines (pins 2-9), control lines (pin 1, pin 14-16) and status lines (pins 10-13, pin 17). As their names depict data is transferred over data lines, control lines are used to control peripheral devices and the peripheral returns status signals back computer through status lines. These lines are connected internally to the Data, Control and Status registers internally. By manipulating these registers in program, the parallel port can easily be read to or written from with programming languages like Delphi, Visual basic, C, C++ and BASIC. The word connection does not mean that there is some physical connection between data/control/status lines. The registers are virtually connected to the corresponding lines such that whatever is written to these registers appear in corresponding lines as voltages, which can be measured with a voltmeter. Whatever is given to the parallel port as voltages can be read from these registers. For instance, if a '1' is written to the data register, the data line D0 will be driven to +5v. In the same way, the data lines and the control lines can be programmatically turned on and off.

In most PC's, the aforementioned registers are input/output mapped and will therefore have unique addresses. These addresses work with the parallel port. For a typical PC, the base address of the printer port LPT1 is 0x378 and LPT2 is 0x278. The data register resides at this base address, status register at base address + 1 and the control register at base address + 2.With the base address, the address of each address of each register can be calculated.

2.1. Parallel Port Programming

Programming languages like Visual Basic, Visual C, Visual C++, C#, Delphi etc are fast and easy tools for developing user friendly applications. They however lack important functionalities like direct access to the parallel port. Writing programs that communicate with the parallel port is easier with operating systems such as DOS (Desktop Operating System) and Windows 95/98 through the use of functions such as *inporb* and *outporb* or *_inp()* or *_outp()* in program codes. However newer operating systems such as Windows 2000, XP, NT etc do not allow this simplicity. This is as a result of the security privileges and restrictions they assign to different types of programs running on them. They classify all programs into two categories, namely: *User mode* and *Kernel mode*. User mode programs run in ring 3 mode and kernel mode programs run in ring0 mode (AlphaSigmaura Team, 2005).

User programs/software falls into the user mode category and is restricted in the use of certain instructions such as IN and OUT to read or write to the parallel port. When they attempt executing such instructions, the operating system halts and displays an error message. Kernel mode programs are however not restricted in executing these instructions. Since device drivers are capable of running in the kernel mode, the workaround for problem stated above is to write a kernel mode device driver capable of reading and writing to the parallel port. The user mode program is then made to communicate with the written device driver. Some of these kernel mode drivers are already written and available as share ware and they include hwintaface.dll, io.dll, IOPORT.ocx, Porttalk.dll, NTportLibrary, Vitport, Inpout32.dll, and so on.

2.2. Ignition Systems of Vehicles

The ignition system of an internal-combustion engine is an important part of the overall engine system that provides for the timely burning of the fuel mixture within the engine. All conventional petrol (gasoline) engines require an ignition system. The ignition system is usually switched on/off through a lock switch, operated with a key or code patch.The ignition system works in perfect concert with the rest of the engine of a vehicle. The goal is to ignite the fuel at exactly the right time so that the expanding gases can do the maximum amount of work that in line with the processes to make the vehicle move. If the ignition system fires at the wrong time, power will fall and gas consumption and emissions can increase (*http://auto.howstuffworks.com/ignitionsystem.htm*).

The part of the ignition system that first initiates the process of moving a vehicle is the key system in conjunction with the kick starter. A wire from the battery in the vehicle connects to the kick starter and other wires connect the kick starter to the key system. When the car key in the ignition system is turned once, two wires coming from the kick starter to the key system are bridged. This causes the engine and some other parts of the vehicle to be put in a READY or ON state. Turning the key again makes a third wire to temporarily join the already bridged wires, causing voltage to flow from the battery to the necessary parts vehicle so as to enable the vehicle move.

3. Fingerprint Based Ignition System Design

The program codes driving the fingerprint recognition software for ignition system control was written in visual basic 6.0 Enterprise Edition and ran on a PC. It uses a set of fingerprint images stored in an image folder in its directory. The test images can be enrolled into its database after it has gone through the stages of image enhancement, minutiae extraction and image post-processing (eliminates false minutiae). An image to be recognized is loaded into the image area and its extracted minutiae is compared with all the images in the database in the case of a 1 to many match, and with just a particular image in the case of a 1 to 1 match. A sufficient number of similar minutiae points between the two images compared, indicates that the input fingerprint image has a match which exists in the database. An insufficient number of similar minutiae points between the two images compared imply that the input fingerprint image has no match which exists in the database.

The results from the matching process are communicated to a section of the recognition software which manipulates two data pins of the parallel port. A fingerprint match causes the data pins to be in a high logic level and ideally output about 5volts while a fingerprint mismatch makes the data pins to be in a low logic level and ideally output 0volts.

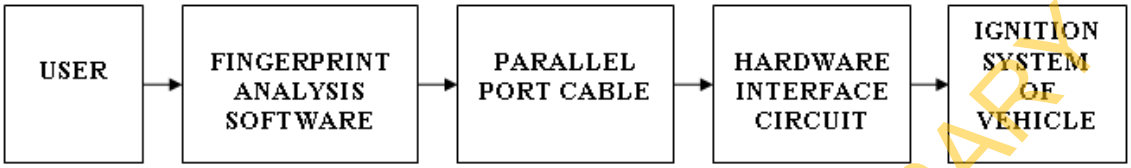
An interface control circuit was constructed to link the PC parallel port to the ignition system of a vehicle. This circuit provides a high degree of electrical isolation between the PC and the ignition system which operate at different voltage levels, through the use of components called optocouplers. The circuit also provides capabilities for the controlling the ignition system via the interconnection of electronic components such as relays, bipolar junction transistors, resistors and diodes.

Three wires from the ignition system of a vehicle are required to be connected to the interface circuit. When the parallel port data pins which form part of the connection to the interface circuit are in

a HIGH logic level, the interface circuit is triggered to ignite the vehicle. On the other hand, the vehicle is not ignited when the circuit is in a LOW logic level.

The principal components of the prototype system are the fingerprint recognition software and the interface control circuit which are to form a continuous connection with a vehicles ignition system. The block diagram of the system architecture is shown below (figure 2):

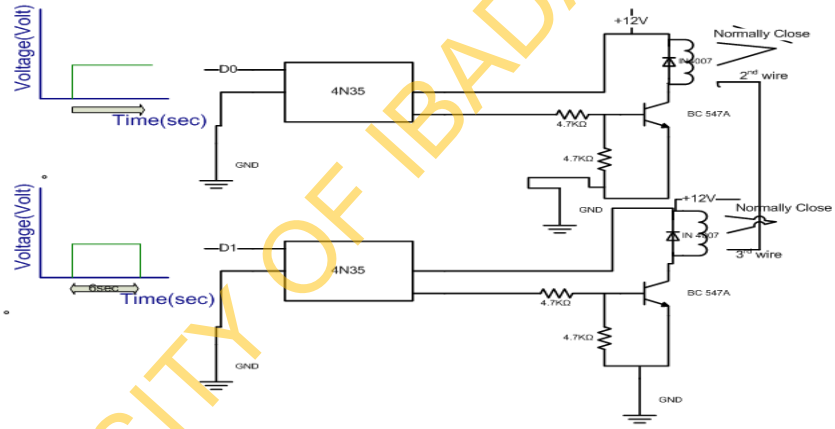
Figure 2: Block diagram Prototype Fingerprint based Ignition System



3.1. The Parallel Port Interface Control Circuit

The circuit was constructed using two optocouplers, two relays, four resistors, two diode, two NPN transistors, and jumper wires. They components were connected together on a circuit board according to the arrangement shown in the diagram below (Figure 3):

Figure 3: Circuit Diagram of Interface Control Circuit



3.2. Controlling the Ignition System

The mechanism of the ignition system comprise amongst other things, three wires that are connected to the key system and used with the keys to ignite the vehicle. Two of these wires are bridged when the key is turned first, causing current to flow from the car batteries to all parts of the car requiring some form of electricity for operation. When the key is turned again, the third wire bridges momentarily with the two wires already connected. This causes the cranking of the engine, which ignites the vehicle.

For the purpose of this research work, the three wires were disconnected from the key system. The first two wires were connected to the first relay, and the third wire was connected to the second relay. This was done to simulate the action of bridging two of the wires together when the first relay is activated. Activating the second relay for a short time causes a temporary connection between the two relays. This connects all three wires together, thus igniting the vehicle. The relays were activated or deactivated by sending appropriate control signals from the fingerprint recognition software, via the parallel port to the interface circuit.

A correctly identified or verified image causes the parallel port control codes in the fingerprint recognition software to send about 5volts to pin 2 of the parallel port. This voltage passes on to the interface control circuit and subsequently activates the first relay. After five seconds, about 5volts is sent again to the pin 3 of the parallel port for three seconds. This activates the second relay for five

seconds and deactivates it. The continuous activation of the first relay and the momentary activation of the second relay cause the vehicle to be ignited.

Conversely, an incorrectly identified image causes the parallel port control codes in the fingerprint recognition software to send about 0volts to pin 2 and pin 3 of the parallel port. Thus, no voltage passes on to the interface control circuit and the two relays remain deactivated. This prevents the vehicle from being ignited.

4. Results and Discussion

The prototype of the fingerprint based ignition system developed was tested with some vehicles. About twenty test images were utilized. Some of them were enrolled in the database. The recognition software correctly identified all the test images used with it and reported whether a match existed or not. A match implied the fingerprint was found in the database and consequently, logic 1 was sent to the relevant data pins of the parallel port. This logic 1 had a value of 4.8volts which closed the interface control circuit connected to the ignition system, and caused the proper ignition and moving of the vehicle. On the other hand, a fingerprint mismatch caused logic 0 with a value of 0volts to be sent to the data pins of the parallel port. The interface circuit thus remained open and this prevented the vehicle from being ignited. The recognition software was also able to stop the vehicle after it had been ignited. After identification, the time taken to ignite the vehicle was about eight (8) seconds given that the engine and batteries were in proper working condition. The interface control circuit also offered the required protection and isolation needed between the ignition system and the computer system.

The robustness of the system developed was easily demonstrated using manually imputed fingerprint images. Some of these test images were downloaded from the internet while others were manually acquired from some individuals. The recognition software was able to classify the test images as one of high, medium or low quality after the extraction of the template of minutiae. This classification was based on the number of minutiae that could be extracted from the image being analyzed. Some fifty (50) minutiae make up a regular fingerprint image and at least thirteen (13) of them were needed to assure a successful enrollment and identification or verification. An image was labeled a bad quality image if only about 13 to 20 minutiae could be extracted from it. If about 20 to 30 minutiae could be extracted then the image was labeled a medium quality image while about 30 to 50 extracted minutiae points characterized a high quality image. The bad quality images were amongst those manually acquired and were found not to be properly imprinted on paper.

5. Conclusion

The prototype of a fingerprint based ignition system developed has a specific sequence that must be followed before it can be used to ignite a vehicle. Basically, the fingerprint recognition software must be first initialized before fingerprint images can be loaded from a file of sample images. The last acquired fingerprint image is then analyzed and its minutiae identified, extracted and stored as a template. The next step involves either enrolling the template or matching the template with other templates. The enrollment process button saves the last extracted template into the database. The identity number of the enrolled template is displayed in the log window. The identification process compares the query template against reference templates in a database. For verification, the identity number of the reference template to be matched with the query template must be supplied.

In the results, it can be deduced that the use of biometric security systems offers a much better and foolproof means of restricting the ignition of vehicles by unauthorized users. Furthermore, it can be logically derived from the findings of this research work that fingerprint images can be used for motor vehicle ignition system control. Parallel port control codes used with fingerprint analysis codes can provide capabilities for allowing only authorized users, authenticated through their fingerprint images to ignite a vehicle.

Acknowledgement: The authors acknowledge the devotion and involvement of Miss. Omocho H. G. C. and Mr. Soetan S. A. for their immense contributions to this research work.

References

[1] AlphaSigmaura Team (2005) "Computer Interfacing and control", Paper presented at the workshop on Computer Interfacing and Control, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

[2] Anton S. (2002) "Sorting it out: Machine learning and fingerprints", Paper presented at the seminar on Telematik fingerprint, Siemens Corporate Technology, Munich, Germany.

[3] Engdahl T. (2005) "Parallel port interfacing made easy", http://www.epanorama.net

[4] Graevenitz G.A. (2003) "Introduction to fingerprint technology", A&S International, Vol. 53, pp. 84 – 86.

[5] http://auto.howstuffworks.com/ignitionsystem.htm, "How Automobile Ignition Systems Work "

[6] http://www.biometricinfo.org/fingerprintrecognition.htm,"Biometrics Information Resource"

[7] http://www.crimtrac.gov.au/fingerprintanalysis.htm, "Fingerprint Analysis – The Basics"

[8] Koichi I., Ayumi M., Takafumi A., Hiroshi N., Koji Kobayashi, and Tatsuo H. (2005) "A Fingerprint Recognition Algorithm Combining Phase-Based Image Matching and Feature-Based Matching", http://www.aoki.ecei.tohoku.ac.jp/~ito/cr2114.pdf -00

[9] Omidiora E. O. (2006), A Prototype of Knowledge-Based System for Black Face Recognition using Principal Component Analysis and Fisher Discriminant Algorithms, Unpublished Ph. D Thesis, Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

[10] Thai R. (2003) "Fingerprint Image Enhancement and Minutiae Extraction", Unpublished B.Sc Thesis, School of Computer Science and Software Engineering, The University of Western Australia, Australia

[11] Yang S. and Verbauwhede I. (2003) "A Secure Fingerprint Matching Technique", http://www.emsec.ee.ucla.edu./pdf/2003acm.pdf