UDC 004.352

O. Polshakova, Y. Malchenko

REVIEW OF THE «SMART» CAR BIOMETRIC ACCESS CONTROL SYSTEM USING THE FINGERPRINT SCAN

Abstract: This work describes the features and benefits of developing a biometric vehicle access control system that allows the use of a fingerprint scanner built into the smartphone to start the car engine. The widespread car protection methods are analyzed, the disadvantages are concluded and the ways of their overcoming are considered. This makes it possible to create a reliable, user-friendly and affordable system.

Key words: Biometric identification, access control system, Fingerprint, mobile application, microcontroller, BLE-module.

Introduction

Currently, Physical Access Control systems (PACS) often use biometric parameters for identification, which provides a higher level of security than when using keys or passwords.

However, using separate fingerprint scanners greatly increases both the complexity of the system and its overall cost. In this regard, the issue of improving the biometric PACS functionality by abandoning individual scanners in favor of more affordable and compact – embedded in modern smartphones is urgent.

The purpose of this article is to describe a smart car access control system by fingerprint scanning using a smartphone scanner and a dedicated mobile application.

Formulation of the problem.

In order to take the necessary steps for the operation of the biometric system of physical access to “smart” car, it is necessary to present a system that must satisfy the following conditions: be reliable, easy to use, affordable and energy efficient. So it is required to provide a structure diagram showing the main elements, optimally selected for a system, and principles of their operation. The main objective of the system is to protect against unauthorized access to the control of the car. A convenient, reliable and accessible user interface for system access is also required.

Description of existing solutions.

Physical Access Control system, PACS - a set of hardware and software security tools, aimed at limiting and registering the entrance-exit of objects (people, transport) in a given territory through the "checkpoints": doors, gates, etc [1].

This article examines access control systems for car applications. The main way to protect the car is traditionally considered car alarm. However, the alarm is not quite reliable, since in the case of theft of the key chain with the key, the thief immediately gets the opportunity to open and start the car. Another popular solution is engine immobilizer. An immobilizer is a device designed to immobilize a car. Turning the immobilizer off and on must only be accessible to the car owner. Typically, a non-contact electronic key, manual key, or hidden key is used for this purpose. The principle behind this device is to lock the main circuits and systems of the car.

However, in general, the immobilizer also has its drawbacks. The presence of an immobilizer does not in itself protect the car from penetration. In addition, if the immobilizer is controlled by a separate keychain, the problem of maintaining the keychain itself again arises. In the case of using a hidden button in the car, an attacker, knowing the scheme of the system, can easily overcome this protection.

Thus, the most reliable remedy will be the use of biometric data [2]. But installing an extra scanner on a car is, firstly, quite expensive, and secondly, it will still not be reliable enough, since the location of such a scanner causes many factors outside, such as weather conditions that make the scanner unstable. By installing such a scanner inside, we come back to the idea of an immobilizer, which, although it will protect the car from theft, but does not protect against penetration.

One solution is to install a fingerprint scanner connected to a controller that can control the starting of the engine and other vehicle systems [3]. The implementation of such a system is quite simple and is used on some models of modern "smart cars". However, such a system, firstly, is quite expensive due to the need to install a quality scanner, which is independent of weather conditions, and secondly, still does not protect against entry into the interior of the car, leaving this function separately installed traditional alarm system.

The solution to the need to install a separate expensive fingerprint scanner has been implemented in some versions of "smart" door locks [4]. Using an owner's smartphone with a fingerprint scanner can significantly reduce the cost of the system. However, there is another problem - the connection of the lock controller to the smartphone is only possible with the receiver's scanning mode permanently turned on. In the case of a fixed lock, electricity is taken directly from the home's mains electricity supply or from a separate battery that consumes power solely for the controller and receiver, ensuring a long uninterrupted operation of the device. However, in the case of a car, installing a separate battery for the system will overload the system and make it cumbersome and inconvenient.

A relative solution to this problem is offered by some separately installed car security systems, which use an automatic short-term start of the engine when a certain low battery level is reached [5]. However, after a while, the car runs the risk of being left with too low a fuel level, which we think is unacceptable.

Therefore, the most reliable solution will be a comprehensive system of protection, which should both prevent the penetration of a third party in the interior of the car, and make it impossible to start the car without biometric data of the owner. Such a system should be versatile and relatively easy to use in order for its installation to be possible on a car of different designs. By building on the examples of previous implementation attempts reviewed, it is possible to create a system that combines the best elements of the solutions considered.

Problem solving

This can be solved by using a mobile application that uses a fingerprint scanner built into the smartphone, and in the event of a coincidence with the recorded fingerprints, allows the controller to unlock the car, start the engine and use other controls depending on the equipment of the car itself.

Fingerprint authentication is used by many popular applications as a more convenient and secure method of access control. Many modern applications also use this method to provide customers with a more secure and user-friendly system speed. Application design has a number of distinctive elements that can be played. The system of biometric control and access control presented by us should consist of the following structural elements. First, it's the controller to control the system and the user's smartphone to transmit the unlock signal to the controller. Smartphone and controller communication is possible through the Bluetooth module. Finally, the system is controlled by a load converter that will allow the controller to be connected to the car's electrical circuit, allowing it to control the start and shutdown of the engine and obtain power from the car's battery. The primary firmware of the controller requires the necessary sketch from the PC via the controller's USB port before direct assembly of the system. The block diagram of the described system is presented in Fig. 1.

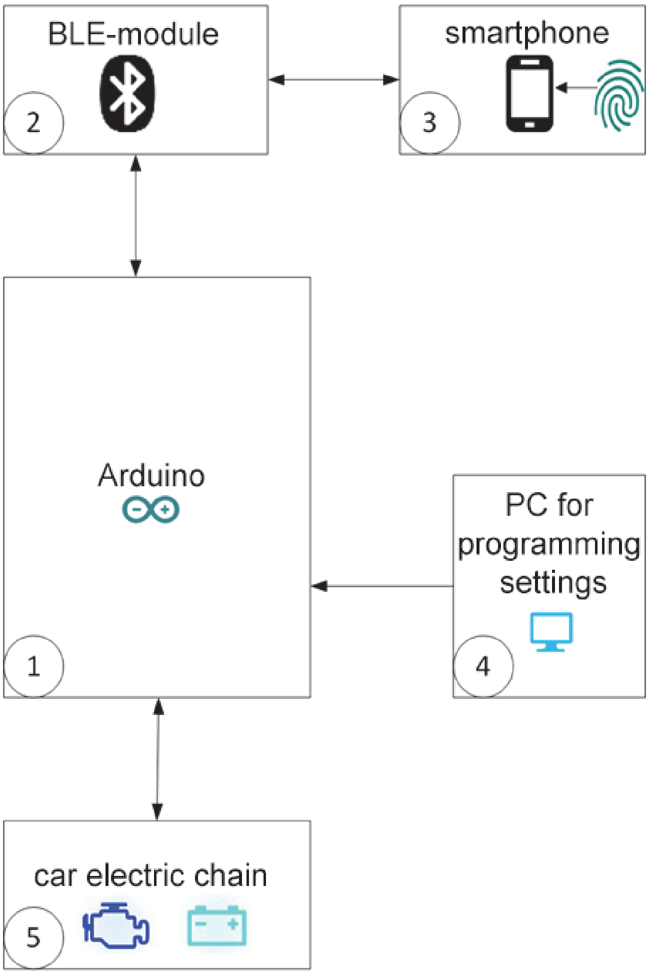

Figure 1. Structural diagram of the biometric system of physical access control to «smart» car using fingerprint scan

Before starting the system, the controller must be initially set up. To do this, you need to download the required libraries and custom sketches to work with all connected devices via the controller's USB port. If this part is done correctly, no further connection of the board to the computer is required. After that it is necessary to collect the scheme from the controller, BLE-module and to plug the system into the car's electrical network, so that starting of the car becomes impossible without passing authorization through the system. After performing the above steps, the system is ready for use.

The use of the system begins with the imprint of the user in the memory of the system. To do this, you need to install an application for communication with the controller via the BLE module (Bluetooth low energy, energy-saving communication protocol) on the smartphone. The prints scanned using the smartphone scanner must be entered into the system database using the application. In the future, to unlock, the user must scan one of the fingers entered into the database. When the signal is received, the system sends a signal to unlock the car's electrical circuit, thereby allowing the engine and other electrical systems to be started. If desired, using the backup code, the system can be completely switched off, allowing the car to be started with a standard ignition.

Conclusion

Using a hidden locking system for the car's main electrolinks connected with BLE module to the smartphone and the fingerprint scanner application we can provide a relatively simple, reliable and user-friendly car access control system. The memory of the prints is stored on the smartphone, there is a comparison, and then when the coincidence signal to unlock is transmitted to the controller. The controller switches on the electric circuit of the car and the engine starts. This creates a reliable, easy-to-use and affordable car access control system that integrates the best elements of existing solutions and eliminates their disadvantages.

REFERENCES

1. Physical access control systems [Електронний ресурс] // https://www.sibis.com.ua/ ua/services/intelligent–engineering–solutions/security–and–access–control–systems/ 2016. Дата доступу: 23.10.19

2. Vorona V. Biometric identification technologies in physical access control systems. Computational nanotechnology 2016 № 3

3. Biometric car lock [Електронний ресурс] // https://volt–index.ru/high–tech/arduino/ohrannoe–ustroystvo–avtomobilya–po–otpechatku–paltsa–svoimi–rukami.html 2017. Дата доступу: 06.11.19

4. Door lock with fingerprint scanner [Електронний ресурс] http://dom–automation.ru/umnyj–dom/articles/dvernoj–zamok–ola–imeet–skaner–otpechatkov–paltsev.html . 2018. Дата

5. Autostart settings on the alarm: [Електронний ресурс] // https://alarmspec.ru/signalizacii/pandora/avtozapusk–pandora.html. 2017. Дата доступу: 17.10.19