Digital Security System in Automobile

Hemanth Kumar.R[1], Leon Dharmadurai.P[2], Aathimaran.V [3], Ranjith.T [4], Vasanth .S[5]

[1]Hemanth Kumar.R - IV B.E Automobile Engineering , SNS College of Technology.
[2]Leon Dharmadurai.P - Assistant Professor, Dept. of Automobile Engineering, SNS college of Technology, Coimbatore, Tamil Nadu, India.
[3]Aathimaran.V - IV B.E Automobile Engineering, SNS College of Technology.
[4]Ranjith.T - IV B.E Automobile Engineering, SNS College of Technology.
[5]Vasanth.S - IV B.E Automobile Engineering, SNS College of Technology.

---***---

Abstract *: The **RFID , Biometric Security System** is a New **Two factor authentication** in Automobile Security System The RFID (Radio Frequency IDentification) technology is a well-known wireless application for traceability, logistics, and access rol. It became ubiquitous in industry and our daily life (ticketing, payment, passports, car keys, etc.).*

RFID is nowadays a standardized technology; its inherent advantages, which are unitary, identification, wireless communication, and low cost of tags, provide it with decisive practical benefits that drive new developments in terms of concepts and applications. This trend is largely confirmed by the market forecast, but also by its implementation in Automobile. As the Biometric is applied in various Fields for data base purposes ,here it is used in the Automobile to reduce the immobilized Automobile theft.

Keywords: Digital Security in Automobile, Biometric System in Automobile, RFID in Automobile.

1. Introduction

A New two factor authentication by radio frequency distinguishing proof(RFID)& Fingerprint scanner established automobile immobilizer framework comprising of low hacking possibility and at the same time protecting security of the travelers of the captured automobile. The immobilizer employs the active RFID modernization wherever the label is shaped through almost massive character sets. The accepting unit is insightfully included in three command circuits in the automobile, specifically, start circuit, command unit, and programmed gear growing framework, allowing it to put across the automobile velocity down to focus in a protected systematic manner. The offset theft auto safety framework anticipated here was tested under a variety of typical weather state of affairs and possible sign bending conditions to check its reliability.

1.2 The Communication

The communication is established between a dedicated reader and the tag, and the information captured by the reader is generally distributed to a remote database. For instance, the ID for an object, the so-called “Electronic Product Code” (EPC), is constituted of only 96 bits there are two categories of RFID:

1. Near Field, allowing a communication distance of some tens of centimeters,

2. Far Field, which allows typical communication distance of some meters.

The main difference between the two categories is the operating frequency, and therefore, the type of tag and reader antennas. For Near Field case, loop antennas at both reader and tag are used, and the communication is achieved by magnetic coupling between the two loop antennas, which limits the communication distance.

For Far Field case, UHF or microwave antennas are used, which allows longer communication distances up to 25 meters.

2. Biometric Replaces the Immobilizers

The anti-theft system EAS (Electronic Article Surveillance) became the first consumer application based on the backscatter technique.... The modern RFID (Radio Frequency IDentification) was born!

Various forms of biometric sensing are under consideration by the car industry Looking to the future, there is some interest in the possibility of using biometric indicators. This might allow the car to issue an alert to the driver, for instance to Security of the car.

Today, however, the industry’s preferred biometric indicator is the fingerprint. This means an authentication event can be triggered only when the pad is pressed, minimising the risk that the driver might inadvertently authenticate a security, for instance, when resting their hands naturally on the steering wheel.

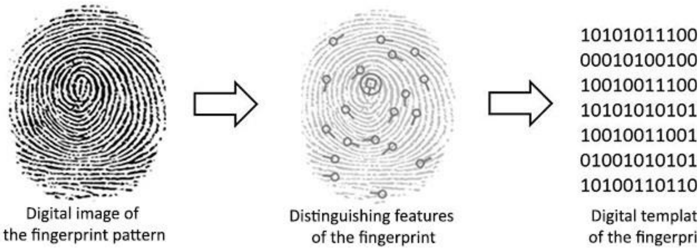
Digital image of the fingerprint pattern
Distinguishing features of the fingerprint
10101011100
00010100100
10010011100
10101010101
10010011001
01001010101
10100110110
Digital templat of the fingerpri

Fig.1. Fingerprint Reader Data Descripition

Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1: N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

Conclusions

Library System sets aside a certain space within Flash for fingerprint template storage, that's fingerprint library. Contents of the library remain at power off. Capacity of the library changes with the capacity of Flash, system will recognize the latter automatically. Fingerprint template's storage in Flash is in sequential order. Assume the fingerprint capacity N, then the serial number of template in library is 0, 1, 2, 3 … N. User can only access library by template number. An RFID reader is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data. An RFID tag is a microchip combined with an antenna in a compact package; the packaging is structured to allow the RFID tag to be attached to an object to be tracked.

Hence the Two Factor Authentication RFID & Biometric System Ensures the Safety in a User Friendly Manner, The Fingerprint & Data Enrollment is very Easy in this Digital Security System.

References

Journals

[1] P.V. Nikitin, L. Theremin, L. Termen, IEEE Antennas Propag. Mag. 54(5) (2012) 252–257.

[2] H. Stockman, Communications by means of reflected power, in: Proc. IRE, 1948, pp.1196–1204.

[3] S. Tedjini, G. Andia Vera, Z. Marcos, R.C.S. Freire, Y. Duroc, Augmented RFID tags, in: Proc. IEEE Radio and Wireless Week, Austin, TX, USA, January 23–27, 2016.

[4] www.businessinsider.com/how-hospitals-are-using-iot-2016-10.

Conference Proceedings

[5] L. Faggion, G. Azzalin, Low-frequency RFID based mobility network for blind people, in: Proc. International Conference on RFID Technologies and Applications, September 2011.

[6] S. Chumkamon, P. Tuvaphanthaphiphat, P. Keeratiwintakorn, A blind navigation system using RFID for indoor environments, in: Proc. International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, May 2008.

[7] S. Willis, S. Helal, RFID information grid for blind navigation and wayfinding, in: Proc. International Symposium on Wearable Computers, October 2005.

[8] B. Ding, H. Yuan, L. Jiang, X. Zang, The research on blind navigation system based on RFID, in: Proc. International Conference on Wireless Communications, Networking and Mobile Computing, September 2007.

[9] Y.P. Lin, P.H. Cheng, Mobile nursing cart service with radio frequency identification technology for use in measuring disabled body temperature, in: Proc. IEEE Region 10 Conference TENCON, November 2011.

[10] O. Postolache, J. Freire, P.S. Girao, J.M. Dias Pereira, Smart sensor architecture for vital signs and motor activity monitoring of wheelchair' users, in: Proc. International Conference on Sensing Technology, December 2012.