World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:2, No:8, 2008

Fingerprint Identification Keyless Entry System

Chih-Neng Liang, Huang-Bin Huang, and Bo-Chiuan Chen

Open Science Index, Electronics and Communication Engineering Vol:2, No:8, 2008 publications.waset.org/15525/pdf

Abstract—Nowadays, keyless entry systems are widely adopted for vehicle immobilizer systems due to both advantages of security and convenience. Keyless entry systems could overcome brute-force key guessing attack, statistics attack and masquerade attack, however, they can't prevent from thieves stealing behavior. In this paper, we proposed a new architecture try to improve the existent flaws. The integration of the keyless entry system and the fingerprint identification technology is more suitable to implement on the portable transponder to achieve higher security needs. We also adopt and modify AES security protocol for life expectancy and security of the portable transponder. In addition, the identification of a driver's fingerprint makes the service of automatic reinstatement of a driver's preferences become possible. Our design can satisfy not only the three kinds of previous illegal attacks, but also the stealing situation. Furthermore, many practical factors, such as costs, life expectancy and performance, have been well considered in the design of portable transponder.

***Keywords*—Keyless entry-system, fingerprint identification, AES security protocol, vehicle immobilizer system.**

I. Introduction

CURRENTLY there are three ways to enter your car and start the engine, and they are mechanical key-lock system, remote keys system and keyless entry-system [1]. However, either way, the driver has to have a key for the car to recognize. At present, for the security design of car keys, encryption with radio communications is most commonly used to prevent brute-force key guessing attack, statistics attack and masquerade attack [2]. The key that a driver carries may be stolen or picked up by someone after it is lost, creating a security breach for theft prevention. In addition, the verification with a driver's key does not guarantee that the key holder is really the driver. Therefore it is impossible to provide the service of automatic reinstatement of a driver's preferences [1].

Biometric identification provides solutions for the above problems. Biometric identification identifies by using the biological features of a driver as the basis of identification, thus reducing the risks of theft or loss of property due to driver's negligence. In addition, the biometric features of every driver are perfect for driver identification, or even for automatic reinstatement of a driver's preferences in the future as they are unique to the driver him/herself. So far there are many ways of biometric identification, such as fingerprint, face profile, iris, palm print, voice, vein and multi-pattern identification. According to International Biometric Group (IBG) [3], AFIS/Live-Scan accounts for the highest share in biometric identification market in 2007 with 33.6%, followed by fingerprint ID (25.3%), face profile （12.9%), intermediate software (5.4%), iris ID (5.1%), palm print (4.7%), voice (audio) (3.2%), vein patterns (3.0%), multi-pattern ID (2.9%) and other types of identification (4.0%). Among all, AFIS/Live-Scan and fingerprint ID account for 58.9% of all identification methods. It is clear that fingerprint ID has become the mainstream of biometric identification. The reason is that it costs less and requires less calculation compared to other types of biometric identification, thus more acceptable in the market.

In this study, fingerprint identification is integrated in keyless entry-systems. Integrated with fingerprint identification, keyless entry-systems are able to prevent brute-force key guessing attacks, statistics attacks, masquerade attacks and thief stealing attacks. Also, drivers' fingerprints are adopted for driver identification in order to provide the automatic reinstatement of a driver's preferences.

II. Background Information

A. Fingerprint Identification

Fingerprint identification has been widely used in our daily life. The most commonly seen adaptation is on laptop computers, where fingerprint identification has been adapted in place of entering personal password on keyboard. Another adaptation is mobile personal device, such as USB flash drive or cell phone. It is also fairly common to see a security system at a dormitory and residence using fingerprint identification. For the use of fingerprints for identification, the following procedure is introduced [1], as shown in Fig. 1:

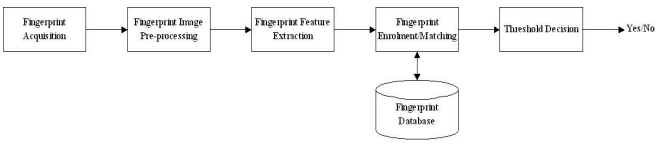


Fig. 1 Functional blocks of a fingerprint identification system

1) **In the fingerprint acquisition phase**, the gray-scale images of fingerprint are obtained from fingerprint sensor. There are several types of fingerprint sensors, for example, optical sensors, capacitance-based silicon sensors, thermal silicon sensors, and ultrasonic sensors. At present, the most popular ones in the market are capacitance based silicon sensors. The capacitance-based silicon sensors use minute electric current signals to

Chih-Neng Liang is with the R&D Division, Automotive Research and Testing Center, Lukang Town, Changhua County, Taiwan (e-mail: cnl@artc.org.tw).

Huang-Bin Huang is with the R&D Division, Automotive Research and Testing Center, Lukang Town, Changhua County, Taiwan (e-mail: abin@artc.org.tw).

Bo-Chiuan Chen is with the R&D Division, Automotive Research and Testing Center, Lukang Town, Changhua County, Taiwan (e-mail: blissdom529@artc.org.tw).

Open Science Index, Electronics and Communication Engineering Vol:2, No:8, 2008 publications.waset.org/15525/pdf

simulate the epidermis, and store the changes in electric signals using tightly packed matrices of capacitors all over the surface of sensors. The distance between the skin and the sensor surface differs between ridges, which directly touch the sensor surface, and valleys, which are separated by an air gap from the sensor surface. This difference in distance causes a difference in capacitance, which is measured by the sensor and finally results in an image describing the contours of the fingertip.

2) **In the fingerprint image pre-processing phase,** it is to normalize the data and apply filters to remove the distortion introduced by noise, manufacturing tolerances and environmental conditions.

3) **In the fingerprint feature extraction phase**, fingerprints are converted into feature values, and it has to be ensured that different fingerprints do not generate the same value. The algorithm looks for minutiae in the fingerprints, such as divides, terminations or loops. At the end, the coordinates and feature values of these minutiae are converted into the feature values.

4) **In the fingerprint enrolment or matching phase**, the user's fingerprint features are stored in database, or compared to those stored in database for matching. Matching refers to a process of comparison, in which the user's fingerprint features are compared to those stored in database. At the end, the matching score for fingerprint features in the database will come out.

5) **In the threshold decision phase**, a threshold is given. Qualification is granted when matching score is greater than threshold, while qualification is denied when matching score is less than threshold.

B. Keyless Entry System

A keyless entry system combines a remote control, keyless entry and an immobilizer [4]. The driver's portable transponder communicates via UHF (433,92 MHz) or via LF (125 kHz). The vehicle sends data to the transponder always via LF. To allow for a flat transponder battery, a passive bi-directional communication can be established.

When a drive puts his/her hand on the grip of the car door and tries to open the door, the on-board antenna electronics send out an LF signal (125 kHz) to the driver's portable transponder. When a signal is received, the portable transponder is activated. Any portable transponder within the transmission range will receive the signal, but only one of them will be chosen for security check. After the portable transponder is identified, the antenna electronics will send a signal to open the door, and another to on-board control unit to initiate the automatic reinstatement of a driver's preferences. The control unit will condition the seat and rear view mirror based on the driver's preferences.

The remote control functionality is that the user can access to vehicle locking or unlocking applications from a greater distance. After pressing the button on the portable transponder, the transponder sends out unidirectional UHF sequence, and wakes up the on-board UHF receiver. The UHF receiver demodulates the UHF sequence and sends the bit pattern to the antenna electronics. The antenna electronics validates the code and determines which action is being requested.

The keyless entry system includes the following components:

1) **PORTABLE TRANSPONDE** — the portable transponder consists of hard-wired core logic with interfaces for external components such as the coil, battery, UHF transmitter and push buttons.

2) **LF- ANTENNA** – A wound loop antenna is built into the driver's door mirror.

3) **UHF RECEIVER** – The UHF receiver wakes up when an UHF sequence is received from the portable transponder. The UHF receiver is connected to the control unit. After the UHF sequence passes the identification, the UHF receiver sends out an open door request to control unit.

4) **DOOR HANDLE** – The keyless entry systems use existing vehicle door handle. An additional push button integrated into the door handle activates the lock process after a successful verification.

5) **DOOR MODULE** – The door module combines the antenna electronics and bus connection. The door module is connected to the door handle and the actuators. An interface connects the door module with the CAN bus.

6) **CONTROL UNIT** – The control unit is connected to the CAN bus. The control unit provides the controls of automatic reinstatement of a driver's preferences, such as positions the driver's seat, mirror, etc. The control unit controls the actuators for global locking or unlocking.

C. AES Security Protocol

The keyless entry-system comprises a portable transponder to be held by the driver and a set of radio transceiver devices located in the car. Operation commands are represented by the wireless signal transmitted between the portable transponder and the radio transceiver. Because the wireless signal is transmitted in proximity of open area, the remote keyless system has the possibility of exposing the key secret commands to a car thief. In the newly designed AES security protocol (ASP) [2], the portable transponder and radio device will be engaged in the protocol interrogation after the portable transponder initiates a connection. A fixed key is used for the encryption of handshake message and a pseudo random number (PRN). This PRN is proposed by portable transponder, and will serve as the variable key. This method can effectively defeat today's common attack tricks such as brute-force key guess attack, statistics attack, and masquerade attack.

The ASP sequence is illustrated in Fig.2. Firstly, the portable transponder sends a handshake request to the car transceiver. Equation c1 = E(KEY, Car _ ID) means cipher text c1 is the result of encryption calculation performed on the car ID with the original fixed key (KEY). Equation m1 = D(KEY, c1) means plain message m1 is the function of the decryption

Open Science Index, Electronics and Communication Engineering Vol:2, No:8, 2008 publications.waset.org/15525/pdf

calculation performed on c1 with the key (KEY). Obviously m1 is the car ID. After the car ID is authenticated, the car transceiver sends a positive acknowledgement to the portable transponder. All the acknowledgement messages are in plaintext form. Equation c2 = E(KEY, PRN) means the portable transponder creates a 128-bit-length pseudo random number (PRN) and encrypts it with the key (KEY). Equation m2 = D(KEY, c2) means plain message m2 is the function of the decryption calculation performed on c2 with the key (KEY). m2 is the PRN. If the car transceiver correctly receives and decrypts c2, it sends out an acknowledgement packet. When the portable transponder receives this acknowledgement, PRN working as the variable key in both the car transceiver and the portable transponder will be synchronized and into an operation iteration. Equation c3 = E(PRN, OPERATION) means the operation is encrypted by the variable key (PRN). Equation m3 = D(KEY, c3) means plain message m3 is the function of the decryption calculation performed on c3 with the key (PRN). m3 is the OPERATION. The number of operations is optional, but a specified timeout counter is set for counting time elapse from the point of the last operation. The portable transponder will issue a disconnection command after the timeout counter is expired.

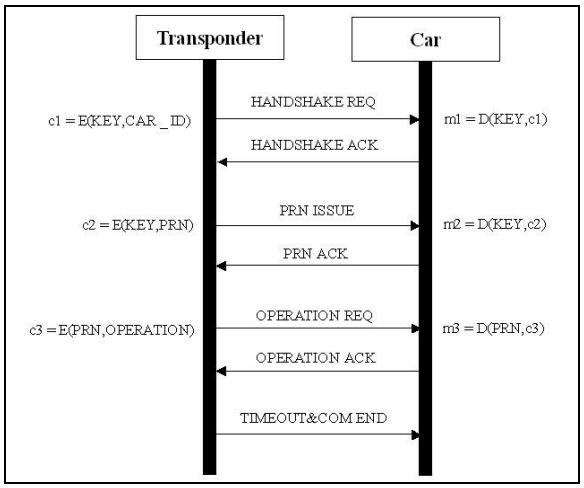


Fig. 2 AES Security Protocol

III. System Architecture

A. Architecture of fingerprint identification keyless entry-system

The architecture of fingerprint identification keyless entry-system is shown in Fig. 3. A fingerprint identification keyless entry-system consists of **PORTABLE TRANSPONDER, ANTENNA MODULE, DOOR HANDLE, DOOR MODULE and CAR PC.** Not one can use the portable transponder without passing fingerprint identification. After the driver passes the fingerprint identification, a passive bi-directional communication of the portable transponder is activated. When the driver pulls the door handle, the on-board antenna module send out an LF signal (125 kHz) to the driver's portable transponder. On the signal, the portable transponder is initiated and starts the security check. After the portable transponder passes the security check, the door module sends a signal to open the door and another to on-board control unit to activate the automatic reinstatement of a driver's preferences. The potable transponder identifies the current driver by fingerprints and sends out the driver's ID through wireless communication module for the CAR PC to call out the current driver's preferences.

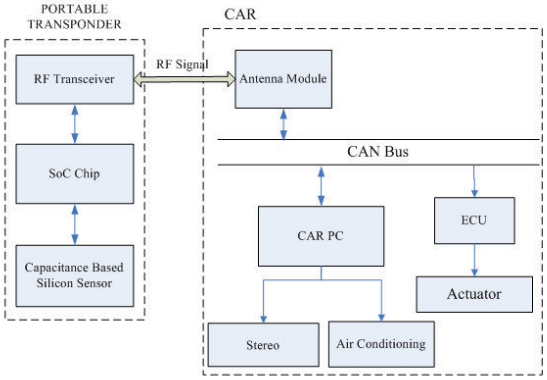


Fig. 3 Architecture of fingerprint identification keyless entry-system

The fingerprint identification keyless entry system consists of the following:

1) **PORTABLE TRANSPONDER** — The portable transponder consists of a SoC chip with interfaces for external components such as the capacitance-based silicon sensors**,** the coil, battery, UHF transmitter and push buttons.
2) **ANTENNA MODULE** – The antenna module consists of the antenna electronics, UHF receiver, bus connection, and a wound loop antenna. The wound loop antenna is built into the driver's door mirror.
3) **DOOR HANDLE** – The keyless entry systems use existing vehicle door handle. An additional push button integrated into the door handle activates the lock process after a successful verification.
4) **DOOR MODULE** – The door module is connected to the door handle and the actuators for global locking or unlocking. An interface connects the door module with the CAN bus.
5) **CAR PC** – The CAR PC is connected to the CAN bus. The CAR PC provides the control of automatic reinstatement of a driver's preferences, such as seat, rear view mirror, stereo and air conditioning.

B. The Design of The Portable Transponder

In a keyless entry-system, the portable transponder is the most important component for identification to open the door

Open Science Index, Electronics and Communication Engineering Vol:2, No:8, 2008 publications.waset.org/15525/pdf

and start engine. In this study, a fingerprint identification system is integrated into the portable transponder. Therefore, no one can open the car door or start the engine even with the portable transponder in case that the transponder is stolen or lost and picked up by any one but the driver. Shown in Fig. 4 is the structure of portable transponder used in the design of this study. The SoC Chip gets the gray-scale images of driver's fingerprints from capacitance-based silicon sensor, and finds the minutiae in the fingerprint images. The coordinates and features of minutiae are then converted into the feature values of the specific driver. The SoC Chip is responsible for the comparison and management of fingerprint features. It matches the features of driver's fingerprints with those saved in the memory and calculates the matching scores between all the fingerprint features in database with the driver's fingerprints. Then, the threshold, which was set in the system at the beginning, is used to decide whether it passes or not. After the driver is identified by his/her fingerprints, the portable transponder turns on the LED that indicates the identification, and the driver now can add new fingerprints or delete old ones with the buttons. Once the portable transponder's car key function is activated, the transponder will receive the data transmitted from the car through LF receiver, and the LF receiver will relay the data to the SoC Chip, which in turn responds to the car through UHF transmitter based on the data transmitted from the car. The SoC Chip executes the entire process of wireless communication and the transmitted data is encrypted using AES algorithm.

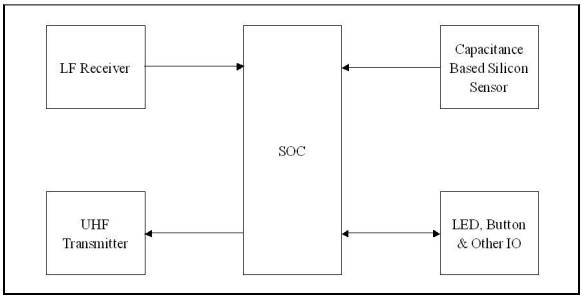


Fig. 4 Structure of the portable transponder

In terms of control unit design, the portable transponder adapts System-on-Chip. That is, the fingerprint identification system, which requires massive calculation resource, and the control system of transponder in a single chip. Therefore, the signals that were supposed to be transmitted externally are now signals transmitted inside the chip. Not only the transmission distance is much shorter, but also the signal transmission bandwidth and speed are increased dramatically, resulting in considerable improvement of performance. The number of system components drops significantly and the size is much smaller as well. This is much better for compact portable transponders. The power consumption for transmitting external signals between IC components is much less, which helps prolong the life of transponder battery. In the selection of fingerprint sensor, capacitance-based silicon sensors are introduced in the portable transponder. The capacitance-based silicon sensors are low in costs, compact and resistant to chemical reactions, suitable for integration with portable transponders [5].

C. The System Communication Sequence

In keyless entry-system, the communication sequence between the portable transponder and car is important for security. In this study, we modify AES security protocol (ASP) [2] for implementation. The communication sequence is illustrated in Fig.5. Firstly, the transponder requests the driver to authenticate, and then the driver inputs his fingerprint to the transponder. After the fingerprint is authenticated, the transponder returns a Yes/No acknowledgement to the driver. After the fingerprint is passed, the transponder starts the key function.

As soon as the user pulls the door handle, the car sends a handshake request to the transponder, and then the transponder returns a c1 acknowledgement to car. Equation c1 = E(KEY, CAR _ ID) means cipher text c1 is the result of encryption calculation performed on the car ID (CAR_ID) with the original fixed key (KEY). Equation m1 = D(KEY, c1) means plain message m1 is the function of the decryption calculation performed on c1 with the key (KEY). Obviously m1 is the car ID. After the car ID is passed, the transponder requests the car for PRN, and then the car sends a PRN to the transponder. The car then creates a 128-bit-length pseudo random number (PRN) and encrypts it with the original fixed key (KEY). This process is denoted by the equation c2 = E(KEY, PRN). Equation c2 = E(KEY, PRN) means cipher text c2 is the result of encryption calculation performed on the PRN with the original fixed key (KEY). Equation m2 = D(KEY, c2) means plain message m2 is the function of the decryption calculation performed on c2 with the key (KEY). Obviously m2 is the PRN. When the transponder receives this PRN, PRN working as the variable key in both the car and the transponder will be synchronized. Thereafter the sequence steps into an operation iteration. The operation commands contain user ID for automatic reinstatement of a driver's preferences. Equation c3 = E(PRN, OPERATION) means the operation is encrypted by the variable key (PRN). Equation m3 = D(KEY, c3) means plain message m3 is the function of the decryption calculation performed on c3 with the key (PRN). Obviously m3 is the OPERATION. The number of operations is optional, but a specified timeout counter is set for counting time elapse from the point of the last operation. The transponder will issue a disconnection command after the timeout counter is expired. Not all messages must be encrypted, but only confidential ones need to be well protected during the wireless communication period. Because the more messages are encrypted, the more power is consumed.

Pseudo random number is used for PRN in ASP. Pseudo random numbers are random numbers generated by software

Open Science Index, Electronics and Communication Engineering Vol:2, No:8, 2008 publications.waset.org/15525/pdf

simulation, which requires large consumption of calculation capacity and power. Therefore in system design, the PRN is provided by the car to save the transponder's power. In addition, the AES encryption algorithm used in ASP requires massive calculation capacity. As a result, the SoC Chip adopted in the system provides hardware AES encryption and decryption for faster calculations and less power consumption.

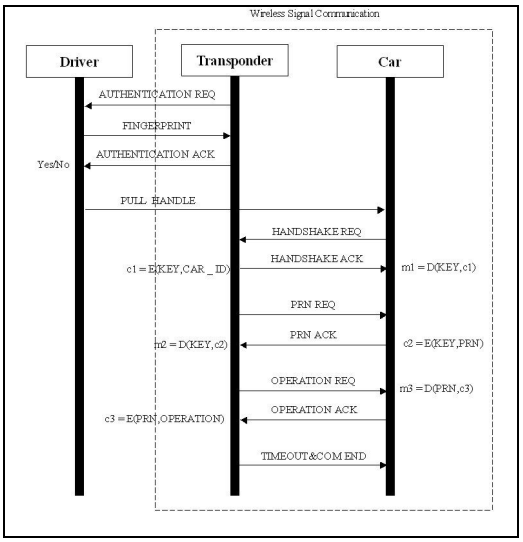


Fig. 5 Communication Sequence

IV. Solutions, Open Issues and Limitations

A. Thief Stealing Attack

The thief stealing attack refers to the stealing of transponders by thieves pretending to be a valet, mechanic technician or others, as to steal the car. In this study, the transponder of keyless entry-system requires the identification of driver's fingerprints for access to the car. A thief cannot do that even with a valid transponder in hand. Therefore the thief stealing attack has no effect to the keyless entry-system in this study, unless he/she has the driver's fingerprint, which, however, is highly unlikely.

B. Brute-Force Key Guessing Attack

ASP is introduced in the keyless entry-system in this study. The ASP uses AES cryptographic algorithm with a 128-bitlength fixed key. The 128-bitlength key offers 2^{128} possible combinations of key. It could take years to break the combinations. Therefore brute-force key guessing attack is out of the picture.

C. Statistics Attack

Statistics attack is the action to guess the possible key combinations from known information and part of the encryption. ASP uses key for the encryption of car ID in the keyless entry-system. The car ID and key of the keyless entry system mentioned in this study are provided by car supplier and exclusive to the drivers. Therefore, statistics attacks are only fruitless attempts.

D. Masquerade Attack

The masquerade attack is the action that a car thief intercepts the wireless signal transmitted from the portable transponder. Once intercepted, the signal provides a means to the car thief to disguise as the car owner for the auto theft. The ASP uses variable keys to prevent masquerade attacks. The value of a key is only valid for this identification process, and the next time, it will be completely different.

E. Security and Convenience

The keyless entry-system proposed in this study has the fingerprint identification system integrated in the portable transponder for prevention of thief stealing. However in practical uses, the portable transponder does not work until the fingerprint identification process approves in advance. Yet, it will cause the drivers a lot of troubles if fingerprint identification is required every time. Compared to the transponder of other keyless entry-systems, the portable transponders in the system proposed in this study consumes more power with the additional function of fingerprint identification, although the energy saving issue is addressed in the design of transponder. For the use and design in the future, it is necessary to configure the time of use for the transponder based on the way the drivers use it. For example, the identification stays valid for an hour, so no further identification is required when the driver just leaves the car for a moment. Less identification means less power consumption. However, longer time of use increases the risks of thief stealing. It is necessary to conduct further analyses to the way the drivers use the transponder and how thieves may steal in order to provide a convenient and safe system for drivers.

V. Conclusion

This paper suggests that a keyless entry-system integrated with fingerprint identification prevents brute-force key guessing attacks, statistics attacks, masquerade attack and thief stealing attacks. A design of keyless entry system integrated with fingerprint identification and the identification process through wireless communications are proposed. Finally, the security of the entire system is discussed. Based on the design proposed, the fingerprint identification keyless entry-system is able to provide a safer keyless entry-system for the protection of car and identify different drivers for automatic reinstatement of the driver's preferences through fingerprint identification. In the design of portable transponder, there are many practical factors to be considered, such as costs, life expectancy and performance. Therefore, it is highly possible to see a car equipped with fingerprint identification keyless entry-system for better and more convenient protection.

References

[1] Lichtermann, J., Pettit, R. "Automotive Application of Biometric Systems and Fingerprint," SAE World Congress, March 2000.
[2] Xiao Ni, Weiren Shi, V. F. S. Fook, "AES Security Protocol Implementation for Automobile Remote Keyless System," IEEE 65th Vehicular Technology Conference, Spring 2007.

[3] International Biometric Group, available at http://www.biometricgroup.com/
[4] S. Schmitz, C. Roser, "A New State-Of-The-Art Keyless Entry System," SAE International Congress and Exposition, February 1998.
[5] Mohamed K. Shahin, A. M. Badawi, M. S. kamel, "On-Line, Low-Cost and Pc-Based Fingerprint Verification System Based on Solid-State Capacitance Sensor", In Proceedings of IEEE, International Conference on Industrial Electronics, Technology and Automation IETA, December 2001.

Open Science Index, Electronics and Communication Engineering Vol:2, No:8, 2008 publications.waset.org/15525/pdf