A NOVEL KEYLESS ENTRY SYSTEM USING VISIBLE LIGHT COMMUNICATION

Kuniyoshi Okuda, Hideaki Shirai, Tomoo Nakamura and Wataru Uemura

Department of Electronics and Informatics, Ryukoku University, Shiga, Japan

ABSTRACT

A major conventional car key is the mechanical key. When users inserted the key into a cylinder mechanical key and turn, users can unlock. The mechanical key may be able to be worn away for physical contact. And it may be impossible to use. Further the mechanical key may be damaged or destroyed by mischief. So a keyless entry system has been developed. The keyless entry system locks and unlocks using the infrared ray and radio waves communication. The keyless entry system does not require physical contacts. Therefore, the possibilities of damage due to mischief and be worn away are fell. However, the transmission ranges of infrared ray and radio waves communication are not clear. Submitting data might be tapped to the malicious people. If the information is tapped, then you have theft of the car and the risk of car break.

We propose a keyless entry system using visible light communication in order to solve this problem. Visible light communication transmits signal using blinking light. Thus the transmission range is clear. The user can transmit the information only to the aimed place. Therefore, the usability is improved. We measure the durations of "take out the remote control", "put the aim" and "takes to unlock key" in order to evaluate the usability in the experiment. We also compared with the infrared ray communication and examined the superiority. Usability is improved in the experimental results, and usability is better than conventional keyless entry system.

KEYWORDS

Keyless entry system, Infrared ray communication, Visible light communication

1. INTRODUCTION

Recently many car manufacturers are adopting the keyless entry system. A keyless entry system unlocks doors without the key inserted into the keyhole. In the traditional mechanical key (Figure 1), keyholes and keys are worn away. Therefore the mechanical key will be difficult to unlock or lock. And people with malicious might to unlock forcibly or destroy the keyhole by malicious mischief. The keyless entry system solves these problems.

There are some types of authentication methods. In the case of two-way communication, there are the zero-knowledge proof and challenge-response. In the challenge response, at first the transmitter sends an authentication request. After the receiver gets it, the receiver sends back a random number sequence. It is called a challenge. The transmitter receives the challenge, and combined with the password and challenge. It is called response. The transmitter sends the response. In the same way, the receiver makes response. It receives transmitter's challenge and checks.

The Zero-knowledge proof is a proof method to check the remainder of the quotient. The receiver

DOI : 10.5121/ijasuc.2014.5501

sends the divisor to the transmitter. The transmitter divides by the received divisor password. The transmitter calculates the remainder, and sends it to the receiver. In the same way, the receiver calculates the remainder. It receives transmitter's remainder and check. The transmitter and the receiver repeat these steps several times.

Figure 1: mechanical key and keyless entry module

2. SOME PROBLEMS OF THE CONVENTIONAL KEY

The mechanical key is used long time on many occasions even now. There are several types of mechanical key. Most major keys are a cylinder type. A cylinder type has some cylinders in the keyhole. The cylinders of different lengths move up and down. When the user inserts into the key hole, the lock cylinder are arranged in a row. The key is unlocked when the cylinders are in a line. Mechanical keys have some weak points. One is that it is damaged or destroyed the keyhole [1-4]. When the key is broken there is a possibility of theft.

Therefore the keyless entry system does not require a mechanical lock and has become widespread. The keyless entry system locks and unlocks using the remote control. The keyless entry system uses infrared ray and radio waves communication for unlocking. The system does not require physical contact. Therefore, the possibility of wear of the keyhole and the key is less. The possibility of mischief and theft is also low. Users can unlock using the mechanical key in an emergency.

However humans can not know the propagation area of the infrared ray and radio waves, because humans are not able to view the infrared ray and radio waves. Therefore we cannot know a reach emitted signal from the remote control. However, people with malicious may intercept the contents of communication using the listening device [5].

A smart entry system has been developed now. The smart entry system is an extension to keyless entry system. The smart entry system transmits and receives using radio waves. This system does not require the manipulation of the remote controller to lock and unlock. Users with a remote control can unlock by approaching the car. And users with the remote control can start the engine without the mechanical key, because the remote control communicates with the car.

However the starting of the engine and unlocking can be even a person with malicious intent, when it is in the vicinity of the car remote control of regular. Also, if the user forgets the key, it is impossible to start the engine on the go.

For preventing eavesdropping, the transmitter sends data to only a specific location. However the communication areas of infrared ray and radio waves are unclear, because we cannot see the infrared ray and radio waves. That is, it is impossible for the users to understand the transmission range of the transmitted data. It is a benefit to a people with malicious. Therefore, with the use of visible light communication [6-8], it is possible to lower the potential to provide the password to the people with malicious. Visible light communication is different from the conventional communication method. Visible light communication sends information by blinking light. We can understand intuitively the communication range that is characteristic of visible light communication. Its transmission range is lit by light. The user can understand intuitively transmission range. We can use the lighting infrastructure as transmitters of visible light communication. Recently, The LED is used as a lighting equipment. The LED is long life and high brightness, and further it is expected success.

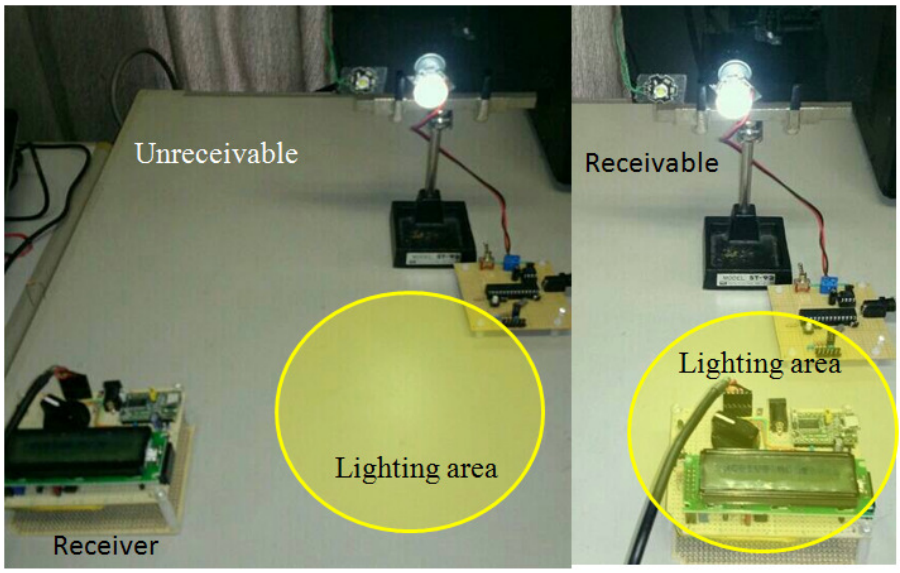


Figure 2: Visible light communication

3. A NOVEL KEYLESS ENTRY SYSTEM USING VISIBLE LIGHT COMMUNICATION

We propose a keyless entry system using visible light communication. The conventional keyless entry system uses radio waves or infrared rays. Therefore the transmission range is unknown. Our proposed system uses visible light communication for keyless entry system. Therefore the transmission range is clear. We show the proposed system in Figure 3.

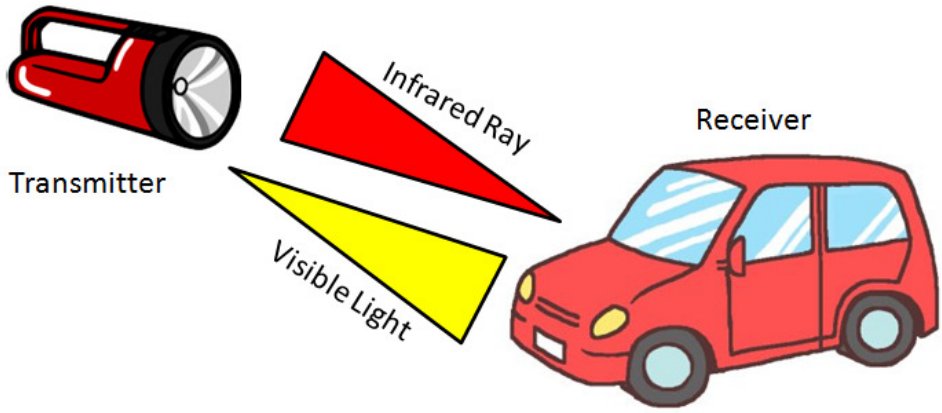


Figure 3: keyless entry system using visible light communication

The remote control includes the LED. The remote control sends the password by using visible light communication. The car has a receiver.

The transmission range of infrared ray and radio waves communication used by conventional keyless entry system is not clear. However our proposed system is different. We can see the transmission range of visible light communication. Thus the user does not send the information to unnecessary place. Therefore information is less likely to be tapping. The user easily can transmit information in an aimed location. It improves the usability.

Our proposed system uses bidirectional communication. An outward path is visible light communication and a return path is infrared ray communication. Our proposed system authenticates a bidirectional communication. We assume that the authentication method is the zero-knowledge proof or challenge-response. Infrared ray communication might be tapping. However, important information is not sent in return path. And modulation system is required to be constant transmission energy by the code.

4. EXPERIMENT

We show fabricated transmitter and receiver in Figure 4 and 5.

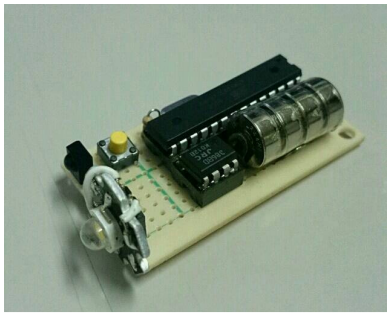


Figure 4: the transmitter

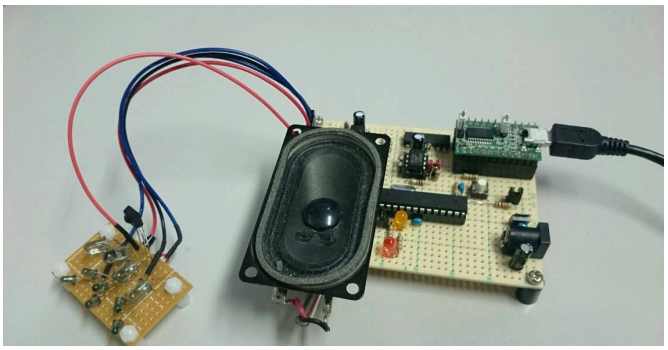


Figure 5: the receiver

The transmitter can perform infrared ray communication or visible light communication by replacing the LED. We use the PPM (pulse position modulation) to the modulation scheme. Brightness is not changed by the data in PPM. The receiver can perform infrared ray communication or visible light communication programmatically, because the receiver has elements of visible light and infrared ray for receiver module. And we use the PPM (pulse position modulation) as a modulation scheme [9-10]. We prevent flicker by using the PPM.

We evaluate the usability of a proposed keyless entry system. The usability means ease of use and convenience. We measure N/E (novice expert ratio method) ratio in the experiment. N/E ratio represents the ratio of the operating time of the designer and the operating time of the general user. That is the operating time of the designer N/E ratio is low, there is no difference in the operation time of the general user. It is judged to have a high usability. We compare the conventional keyless entry system using infrared ray communication and proposed system. The measurement items are time to take out the remote control, time to put the aim and the time it takes to unlock the key. General users and designers measure them. In addition, we calculate the N / E ratio of at that time. We show the results of the experiment in the Figure 6 and 7.

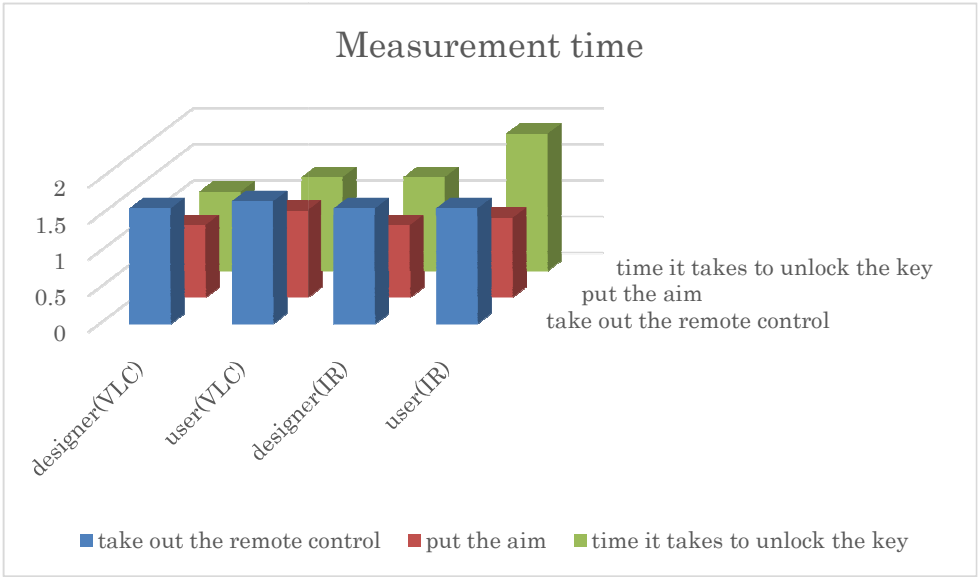


Figure 6: measurement time

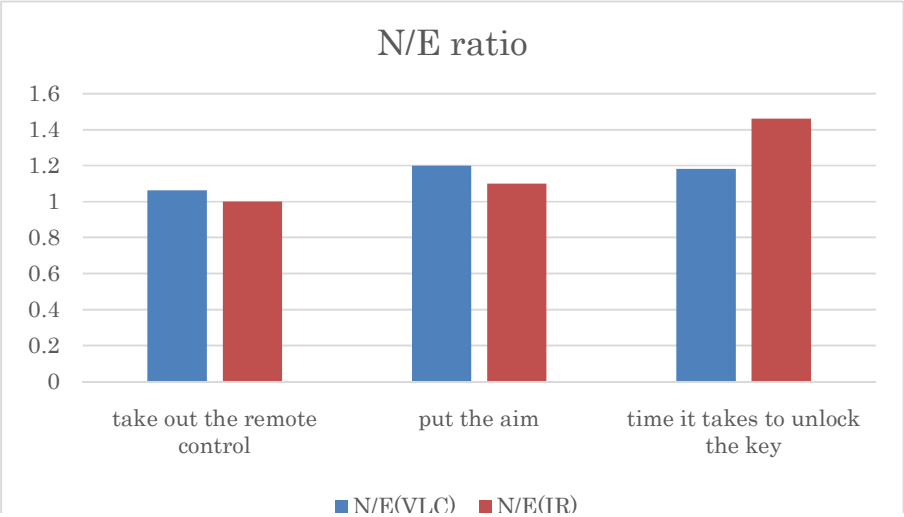


Figure 7: N/E ratio

Remote control parts are common except for the LED. Therefore, there was no difference in time to time other than "time it takes to unlock the key". We think that the cause is clear communication range. Human can understand intuitively transmission range of visible light communication. Therefore, if the user can aim to the wrong place, they can to correct aim immediately. However, infrared ray communication is different. We cannot see the transmission range of the infrared ray communication. Then, the user cannot understand intuitively transmission range. Thus correcting the aim is not easy for the user. Long time, designers are working with a remote control. So designers are familiar with the operation. Therefore, they understand to some extent sighting. General users are unfamiliar with the operation. Therefore, the result is different.

5. CONCLUSION

We proposed a keyless entry system using visible light communication in this paper. The conventional keyless entry system uses an infrared ray or radio waves. The user sends information to unnecessary place, because we cannot see the transmission area of infrared ray and radio waves communication. Therefore, it is possible that people with malice eavesdropping information. So we attempt to solve the problem by using visible light communication. Visible light communication is a communication that is visible to the eye. One of characteristic of visible light communication is to visible transmission range. Therefore, the user does not send the information to unnecessary place. In addition, the transmission range of visible light communication is clear. Therefore, users can operate intuitively. So we propose a keyless entry system using visible light communication. Our proposal can be put on the aim intuitively as compared with the keyless entry system of conventional. Therefore, usability is good.

We have measured N/E ratio to evaluate the usability in experiments. N/E ratio is a comparison of the operation time of the general user and operation time of the designer. If this value is low, usability is good. The measurement item is "take out the remote control", "put the aim" and "takes to unlock key". We compared by infrared ray communication with visible light communication the three items.

The results of the experiment, took time to unlock up to the general user compared to the designer in the infrared ray communication. There was no much difference between them in visible light

communication. We think that the cause is easy to aim. The transmission range of infrared ray communication is not clear. However, visible light communication is different. The users can correct aim easily, because they can understand intuition transmission range.

From the experimental results, we show that our usability of proposed system is better than conventional keyless entry system.

REFERENCES

[1] Eli Biham, Orr Dunkelman, “How to Steal Cars -A Practical Attack on KeeLoq”, pp.3 (2007)

[2] Nicolas T. Courtois, Gregory V. Bard, and David Wagner, “Algebraic and Slide Attacks on KeeLoq, (2007)

[3] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani hysical, “Cryptanalysis of KeeLoq Code Hopping Applications”, (May 8, 2008)

[4] Nathan Keller, Orr Dunkelman, Eli Biham, and Bart Preneel, “A Practical Attack on KeeLoq”, pp.4,5(2008)

[5] Saleh Almowuena, “AN EFFICIENT KEY AGREEMENT SCHEME FOR WIRELESS SENSOR NETWORKS USING THIRD PARTIES”, IJASUC Vol.4, No.4, 2013

[6] S.Haruyama,"Visible light communication", Journal of IEICE, 94(12), D, pp. 1055-1059, 2011

[7] Rajan Sagotra, "Visible Light Communication", International Journal of Computer Trends and Technology (IJCTT) volume4 Issue4, pp. 906-910, 2013

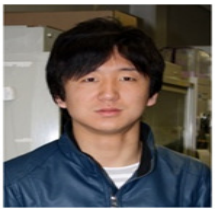
[8] Dominic C. O'Brien, "Visible Light Communications: challenges and possibilities", PIMRC 2008. IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, pp.15-18, 2008

[9] T. Saito, "A Study for flicker on Visible Light Communication", Technical Report of IEICE CS, vol. 106, No. 450, pp. 31-35, 2007.

[10] I.Shouichi, "Reduction of Flicker by Coding and Modulation for Visible-Light Communication" Technical Report of IEICE OCS, vol. 108, No. 39, pp. 1-4, 2008.

AUTHORS

Kuniyoshi Okuda (b.1986) is a student of Ryukoku University in Japan. After studying Electronics and Informatics at Ryukoku University, he completed his Master of Engineering at Osaka City University. Now he is a doctor course student at Ryukoku University.



Hideaki Shirai received B.E, M.E. and D.E. degrees from Ryukoku University, in 2010 and 2012, respectively.

Tomoo Nakamura was born in 1948, and received B.E, M.E. and D.E. degrees from Kyoto University, in 1970, 1972, and 1988. He is a professor of Ryukoku University in Shiga, Japan.

Wataru Uemura was born in 1977, and received B.E, M.E. and D.E. degrees from Osaka City University, in 2000, 2002, and 2005. He is an associate professor of the Department of Electronics and Informatics, Faculty of Engineering Science, Ryukoku University in Shiga, Japan. He is a member of IEEE, RoboCup and others.