Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2015) 23: 17 – 27

doi:10.3906/elk-1209-64

Design and implementation of IR and laser-based electronic ciphering systems

Feyzi AKAR*, **Osman AŞKIN**
Department of Electrical and Electronics Engineering, Naval Academy, İstanbul, Turkey

Received: 13.09.2012 • **Accepted:** 17.10.2012 • **Published Online:** 12.01.2015 • **Printed:** 09.02.2015

Abstract: This paper describes the design and implementation of infrared (IR) and laser-based electronic ciphering systems for use in both indoor and outdoor wireless remote control applications. To communicate between a user and a lock module in a secure way, the proposed systems utilize IR and laser frequencies instead of radio frequencies. Each proposed system has its specific security design. A new communication protocol is also generated, which is compatible for use with IR and laser technologies. The proposed electronic ciphering systems' prototypes are realized together with software and hardware components. They are instrumented using the peripheral interface controller series microcontrollers. All of the designs are made effective in terms of cost and size. Widespread and easy applications of the proposed wireless remote control systems will completely meet the security needs of users in daily life, such as home or office security, immobilizer applications, personal computers, and other personnel electronic equipment.

Key words: Wireless remote control, security, IR, laser, electronic ciphering

1. Introduction

Three different infrared (IR)- and laser-based security solutions for wireless remote control systems (WRCSs), which are well suited for tasks such as door locking purposes of home, office, and automotive applications, are presented in this paper. The first design is mainly based on asynchronous (unidirectional) IR-based communication, where the one-time password (OTP) technique is applied in the production of the password, where the algorithms are defined according to the user's identity. Thus, each registered user has a unique password generation algorithm. In the second design, a laser is used instead of IR, and a perforated plate is designed to overcome the focusing problem. It is also based on the asynchronous communication technique. The last proposed design is based on the synchronous (bidirectional) IR communication technique. The implemented systems include a transceiver module at both the user (the client) and the lock (the server) sides in order to exchange the 32-bit identification (ID) number, which is unique for each user.

Nowadays, WRCSs are commonly used in a wide range of applications in all areas of daily life, including remote start, keyless entry, and security systems (vehicles, garage and parking lots, entrance fees, etc.); office equipment; and a variety of home entertainment electronics. The reliability and safety of the WRCS might not be a critical factor in entertainment or home equipment (e.g., remote controller of a radio, television and DVD player, or air conditioner), while it is an essential and sometimes a vital issue in a security access system [1–3]. Most home entry systems or cars are equipped with various alarm security solutions that notify owners about unauthorized attempts for access through an alarm or informing data [4]. Global position system (GPS) tracking

*Correspondence: feyziakar@dho.edu.tr

devices, passive radio-frequency ID (RFID), touch sensitive alarms, digital cellular technologies, voice-activated command recognition devices, and remote keyless entry systems are some of the common security technologies that are used in such applications [5–7]. However, together with emerging technologies, these security solutions can be easily defeated or become inadequate in a short time. Since passive RFID devices have a fixed ID number, radio frequency (RF) tuning devices can easily be used to attack them. Global system for mobile communications devices and GPS tracking systems can also be used, but they need additional equipment and costly devices to be installed. Therefore, the vulnerability of such devices is very high and they do not provide complete protection. [8]. IR solutions for WRCSs are also used as an alternative to RFID technology. Electronic home appliances, home security systems (home, office, garage door, etc.), and remote control systems are some applications running with IR technology. IR-based WRCSs are able to offer reliable and cost-effective solutions for short ranges. The need for a clear line of sight between the receiver and transmitter in these applications makes it inferior, as interventions from outside of the system are highly possible.

Different authentication techniques, such as fixed password, OTP, and question-answer, are already available to ensure the security of WRCSs. The fixed password technique has a vital drawback since unauthorized people can seize and copy the password and use the password to access the system while the transmission of the password takes place (playback attack) [9]. It can be said that there is a similar security weakness in RFID applications. The descriptive information contained in RFID tags is fixed. For example, in the passive anti-theft security system, developed for the car safety, the user's key has a fixed ID code, and sending this code activates the receiver system [10]. While security technologies evolve, fixed password applications have been replaced by OTP applications. For example, nowadays, Internet banking users are mostly requested to enter an OTP.

In this study, IR and laser communication technologies are preferred instead of RF in the proposed WRCSs. For indoor communications (short range), IR and laser radiation offer some important advantages over RF [11] due to the fact that IR light-emitting diodes (LEDs), lasers, and detectors are capable of high-speed operations and are available at a very low cost. Their transmission regions are confined to a room. The IR and laser spectral regions offer unlimited bandwidth and are virtually unregulated worldwide. As a result, their signal confinement makes it easy to secure transmissions against casual eavesdropping by third parties in virtually all short-range indoor applications [12]. Since IR- and laser-based systems require a visible wireless connection between the transmitter and receiver units, directing the IR or laser beam properly may avoid the criminal recording of data while in transit [13].

The rest of the paper is organized as follows. In the next section, the main security threats for WRCSs are presented. Section 3 shortly describes the principles of IR and laser communication. The proposed asynchronous and synchronous WRCSs, together with the new communication protocol and their implementations, are detailed in Section 4, followed by performance comparisons in Section 5. Finally, concluding remarks are given in the last section.

2. Security threats for WRCSs

None of the security systems are totally and genuinely secure for access control applications. For example, if a thief wants to steal a car, he/she can load the car onto a truck and drive away, or to burglarize a home or office, he/she can blow down the doors quickly and take valuable assets. However, these methods are evidently noisy and disruptive, contrary to the fact that all thieves would want to open door locks silently with their own methods.

For a safe access entrance system, a wireless communication system between the lock and user must meet

3 basic requirements [14–19]. First of all, communication must take place only between authorized people, all with a unique ID. All of the proposed WRCSs in this paper have an ID recognition system for user distinction, which is so flexible that authorized ID numbers can be added or removed easily. Unauthorized ID numbers cannot be used to access the system. Second, the communication link must be unreachable by third parties. In order to provide this feature in the proposed WRCSs, the IR band is selected instead of RF due to its advantages; for example, if someone wants to capture the signal he/she must be between the receiver and transceiver, which is nearly impossible because the application is designed for short-range communication. In IR-based systems, there is no electromagnetic wave leakage; therefore, the proposed WRCSs are utterly free from eavesdroppers. In the case of eavesdropping, first, a third party must decipher the custom IR communication protocol and then work out the encryption algorithm. Finally, the integrity of the communication must be provided. This means that the information must not be modified in any way by the third party while in transit. This is also provided by the proposed WRCSs, as intervention or modification is hardly possible due to the properties of the IR band. IR frequencies are functional at a short range. If someone wants to break the integrity of the information signal, he/she must be physically close to the user. The custom IR communication protocol will help to prevent intervention or modification as well.

Security systems play a deterrent role with the implemented security policies. These aforementioned requirements are important and considered in the design of the proposed WRCSs. Manufacturers implementing these products may have to face a tradeoff between the low costs and high security. Security and low power consumption are also important; however, the manufacturing cost is the main factor for WRCS products, as well as versatility, flexibility, and physical size.

3. Principles of IR and laser communications

IR communications systems are cheap and useful ways for the remote controlling of electronic devices. They are based on an exchange of information in the form of a binary array by means of IR signals, where usually one channel is used for serial communication. Various methods and protocols are developed for IR applications. An IR light source transmits with modulation at a particular frequency (i.e. 40 kHz). The IR receiver module is set to the same frequency so that it filters out all other frequencies. A 32–40-kHz modulated square wave signal is used for IR remote control communication. Sending information from different remote control modules relates to the IR protocols. There are basically 3 types of standard IR communication protocols, namely pulse-coded, space-coded, and shift-coded (Figure 1). In pulse-coded protocols, levels '0' and '1' are created by changing the length of a pulse. The Sony protocol is a common example of this type. In space-coded protocols, levels '0' and '1' are obtained by changing the length of the gaps between pulses, which Sharp widely implements in its applications. In shift-coded protocols, the direction of the transitions creates levels '0' and '1', and all of the bits have a fixed time period, which is mostly used in Philips products.

Laser communications systems work similar to fiber optic links, except that the beam is transmitted through free space, requiring line-of-sight conditions. They can be easily deployed, as they are naturally inexpensive, small, and low power. The carrier transmission signal is usually produced by a laser diode, where 2 parallel beams are needed for transmission and reception.

4. The proposed WRCSs and specific communication protocol

In this section, the proposed asynchronous and synchronous WRCSs, based on IR and laser communication technologies, together with the new communication protocol and their implementations, are detailed.

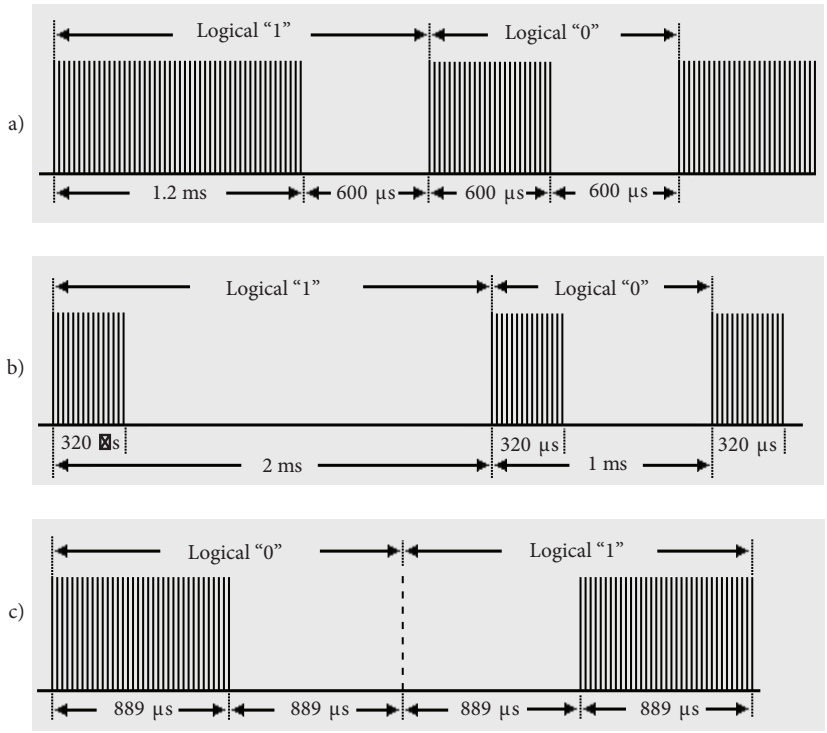

Figure 1. Basic IR communication protocols: a) pulse-coded, b) space-coded, and c) shift-coded.

4.1. IR-based asynchronous communication system

The OTP encryption technique is used in the proposed asynchronous (unidirectional) IR communication system design. In this technique, the password is generated by a special algorithm for each authorized user, and the validity of the password is limited to a single usage. In this case, having been used once, a password losses its validity and is sent to the trash. Basically, the receiver and transmitter modules use the same encryption algorithm to produce the password. A new and different password is sent to the receiver by pressing a button located on the transmitter each time. Here, in this proposed WRCS, users do not enter the password using a keypad; rather, an autogenerated password is transmitted to the receiver with a single keystroke. Thus, the possibility of copying the password decreases. In addition, if an unauthorized copying of the password is performed, it is not considered a security vulnerability since the validity of the password (OTP) is over. Figure 2 presents the flow chart of the proposed WRCS transmitter part of the operations, and the prototype is depicted in Figure 3.

The transmitter creates a 24-bit password divided into 3 main parts, each with 8 bits. When the button is pressed, the transmitter sends the produced password to the receiver with an 8-bit command and 4-bit address. After sending the password, using the encryption algorithm, the transmitter generates 3 new 8-bit password sources and writes them to the electrically erasable programmable read-only memory (EEPROM). Thus, the password, which is already sent to the receiver, is deleted. To be different every time, the number of 24-bit passwords that can be produced is 2^{24}, meaning that the possibility of unauthorized access for a third party at first trial (assuming that the first layer of security of the IR communication protocol is passed) is 5.96×10^{-8}. The produced password is sent in 3 parts due to the special communication protocol designed, where, on average, 22.8 ms is necessary to send each part. This means that sending a 24-bit password takes 68.4 ms Trying

all of the possible passwords incessantly continues for 318.77 h (approximately 13 days), where the receiver's responding time for each password is not included.

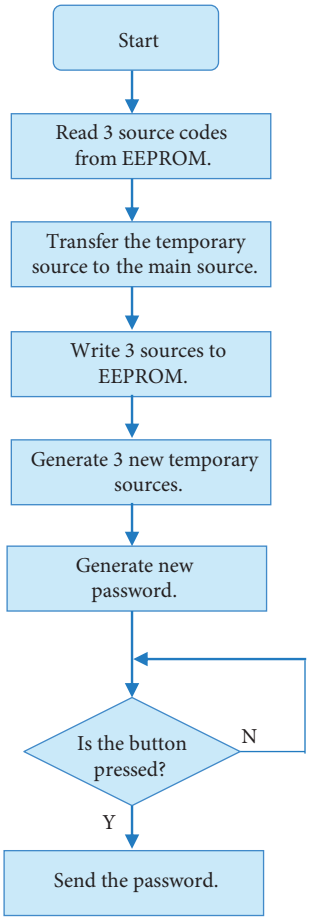

Figure 2. IR-based asynchronous system transmitter part flow chart.

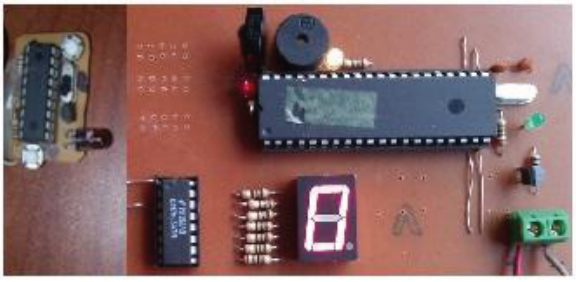

Figure 3. Hardware design of the IR-based asynchronous system receiver and transmitter.

On the receiver side, 10 source codes, each of them having 24 bits, are generated using the same algorithm and written to the EEPROM. If the transmitter button is pressed several times at a point away from the receiver, the password changes and the synchronization between the transmitter and receiver is lost; generating 10 source codes on the receiver side prevents this situation. Briefly, after the transmitter button is pressed 9 times at a certain point away from the receiver (undetectable by the receiver or in a different environment from the receiver), and then if the button is pressed a tenth time in the receiver's coverage area, the generated password will be accepted by the receiver.

Figure 4 shows the flow chart of the operations at the receiver side. After generating 10 source codes, the receiver waits for the transmitter signal. The receiver takes and resolves the signal to deduce the 3 $\times$ 8-bit passwords. After reading the password, the receiver compares it with the self-produced source codes. If the password does not comply with the 10 self-produced source codes, the receiver does not unlock the system and waits for the new signal. Otherwise, the receiver unlocks the system and the preceding passwords are deleted. In a case where the source codes are used at a certain point away from the receiver, they are no longer valid. The passwords that are wasted by pressing the button are not allowed to be used again considering the possibility of

being copied. New passwords are generated and written to the EEPROM as the number of deleted passwords continues. Unused source codes are not wasted because they move up to the top of the codes. If sorting is disrupted, the synchronization between the transmitter and receiver disappears, resulting in different password production at both sides. The receiver waits for the transmitter signal again after generating 10 new codes.

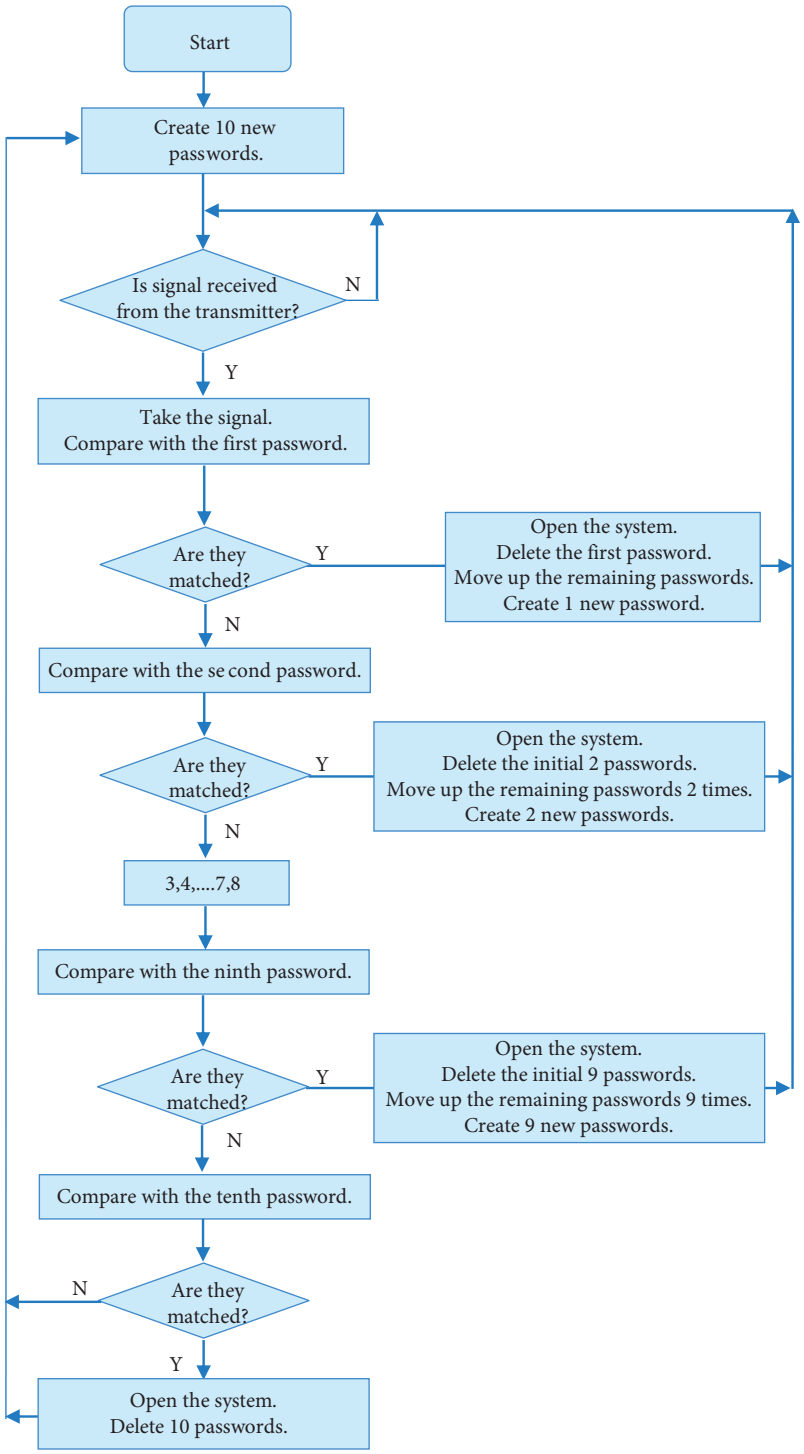

Figure 4. IR-based asynchronous system receiver part flow chart.

4.2. Laser-based asynchronous communication system

At the transmitter side of the proposed laser-based asynchronous communication system, a green laser pointer is preferred instead of an IR transmitter LED, differing from the previous WRCS. This WRCS also employs the same hardware and software as the previous one at the transmitter side, except for the IR transmitter LED replaced with a laser pointer.

At the receiver side of the laser-based asynchronous communication system, as in all applications utilizing this technology, focusing problems arise due to the small surface area of the receiver phototransistor (approximately 1 cm^2). It gets more difficult to stabilize the laser beam on the sensor as the distance increases. To eliminate this problem, different solutions were introduced in the literature, for example, using lens or multiplexing sensors [20,21]. In this study, a perforated plate is developed with the benefit of scattering the light, as seen in Figure 5. Incoming laser beams scatter from the edges of the holes of the plate and fall over the receiving sensor. The distance between the plate and sensor is 15 cm, and the dimensions of the perforated plate are 17 cm $\times$ 17 cm.

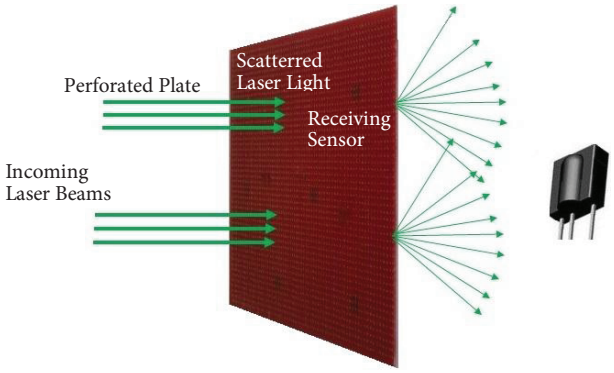

Figure 5. Scattering of the laser beam on the perforated plate.

A modulated laser beam is sent to the plate from up to a 30 m distance. The receiver gets the signal with great accuracy, as the perforated plate presents more angular independency due to its large surface area (289 cm^2). On the other hand, a lens with a radius of 5 cm has only a $\pi r^2 = \pi \times 5^2 \approx 80$ cm^2 surface area. An angular comparison between the sensor, lens, and the plate is shown in Table 1. In addition to its superiority in signal accuracy, the perforated plate is also relatively cheap and easy to use in applications (Figure 6).

Table 1. Angular value comparison.

	1 m	3 m	5 m	10 m	20 m	30 m
Only sensor	0.57°	0.19°	0.11°	0.05°	0.03°	0.02°
Lens	5.71°	1.90°	1.14°	0.57°	0.28°	0.19°
Perforated plate	9.64°	3.24°	1.94°	0.97°	0.48°	0.32°

4.3. IR-based synchronous communication system

Design of the proposed IR-based synchronous (bidirectional) communication system relies on client-server architecture (Figure 7). More than one client can be defined in this WRCS, and the server uses a different encryption algorithm for each client. Here, there is a mutual exchange of data between the client and server. For this reason, both the client and the server have a transceiver module.

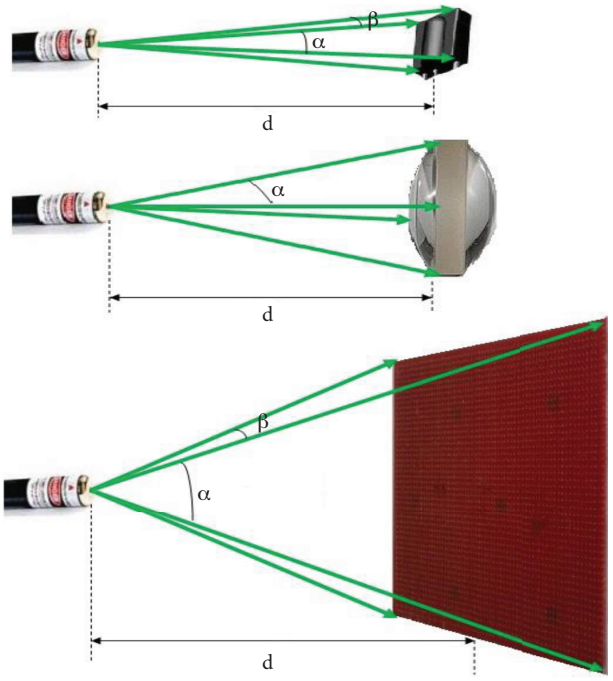

Figure 6. Angular advantage of the perforated plate.

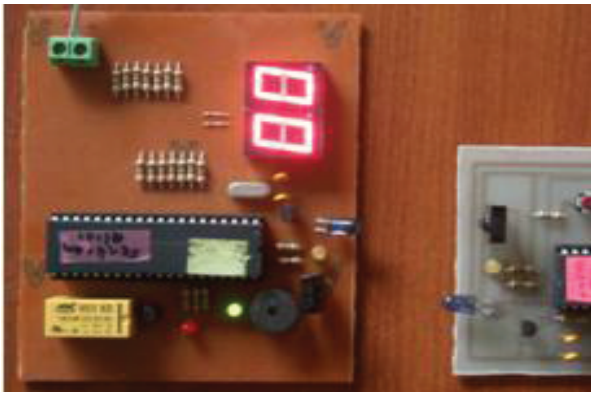

Figure 7. Hardware design of the IR-based synchronous server and client system.

Figures 8 and 9 show the flow charts of the operations performed on the client and server sides, respectively. An authentication technique similar to the 'challenge-response technique' is utilized in the proposed WRCSs. First, each client is given a 32-bit ID, which is generated using a special protocol. When a user requests access to a system via pressing the button on the keypad, the client ID is relayed to the server. After receiving the ID number, the server generates a random password, encrypts it using a special algorithm produced for client's ID number, and returns the encrypted password to the client. The encrypted password has four 8-bit blocks. The client decrypts the received encrypted information, running its own encryption algorithm in reverse. After finding the original password, the client sends it back to the server once again. The server compares its self-obtained password to the one sent by the client. If they are same, the server gives access to the system. Otherwise, the server does not allow access to the system and waits for a new client ID number.

In this proposed synchronous WRCS, the client does not need to produce a password, as all passwords are generated on the server side. The client decrypts the received password sent by the server and then finds the original code. The server generates random passwords that are always different from each other. This process is initiated once an ID number is relayed from the client to the server, providing synchronization between the client and server. This proposed WRCS can be used for secure entry systems with one or more users.

The proposed IR-based WRCS operations can be expressed in 4 steps:

1. The client sends their ID number using the specific IR protocol.
2. The server checks its lookup table for this ID. If it returns true, then it puts forward a random question to the user.
3. The client sends their answer back to the server.
4. The server checks the answer. If it returns true, the user is given access.

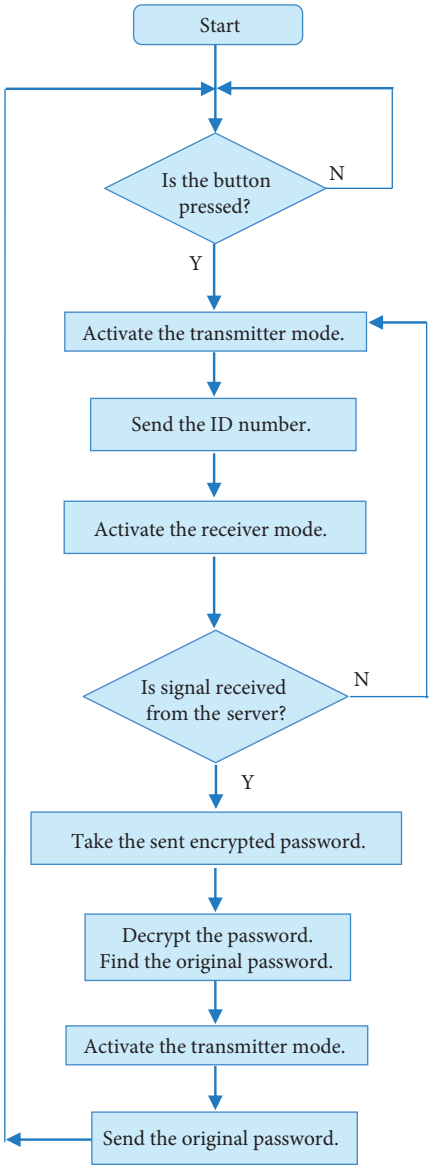

Figure 8. IR-based synchronous communication system client flow chart.

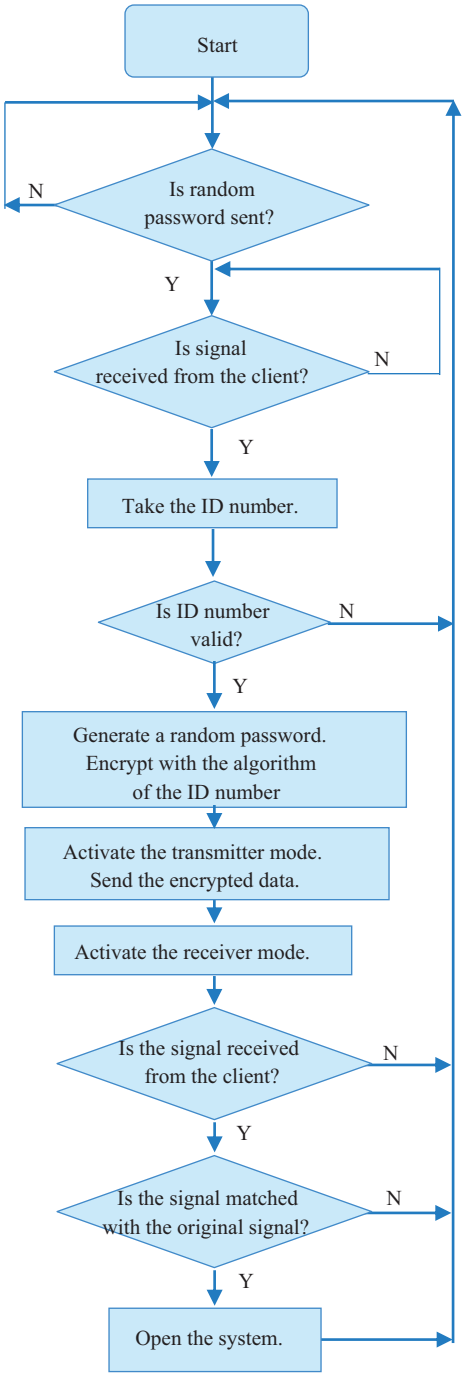

Figure 9. IR-based synchronous communication system server flow chart.

If a third party wants to intrude on the system, first, he/she must seize a valid client ID number, as well as the unique encryption algorithm for this ID number. If a user loses his/her key, the authentication can be made passive for only the lost key. In the meantime, other users can continue to use the WRCS without any problem. In this system, the entrance time of the users can be logged for security reasons, and assigning

different kinds of authorizations to the users is also possible. For instance, day and hour restrictions can be given for a specific group of users, or if there is more than one office room in the building, only authorized users can be permitted to access certain rooms.

4.4. Specific communication protocol for the proposed WRCSs

A specific communication protocol, compatible with the pulse-coded protocol, is also designed for the proposed WRCSs, in which there are 12 bits on the carrier signal of 40 kHz, 4 bits for the address, and 8 bits for the commands.

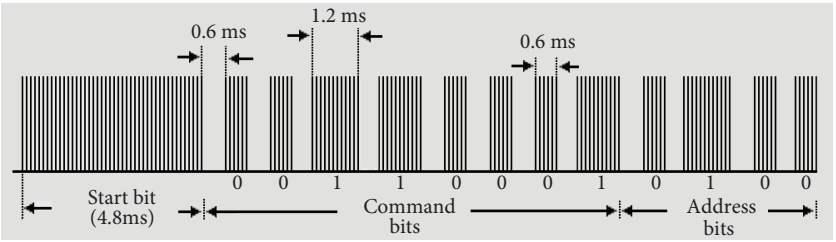

Figure 10. The designed specific communication protocol with command and address bits and durations.

Codes start after the 4.8-ms start bit (Figure 10). The pulse-widths of logic levels '1' and '0' are 1.2 ms and 0.6 ms, respectively. The waiting time between the pulses is set to 0.6 ms. The command and address bits have 4.8-ms start bits. A command package sending time, depending on the content of the information sent, can be calculated as follows. A total of 12 bits for the command and address are sent, and there is a 0.6-ms waiting time before each bit. In addition, there is a 4.8-ms start bit at first. Therefore, considering all of the bits, the '0' total command package sending time is 19.2 ms, while it is 26.4 ms if all the bits are '1'. An overall comparison between the classical RF-based WRCSs and proposed IR- and laser-based WRCSs is shown in Table 2.

Table 2. A Comparison between classical RF-based and the proposed IR- and laser-based WRCSs.

	Classical RF-based WRCSs	Proposed IR-based WRCSs	Proposed laser-based WRCS
Cost	High	Low	Medium
Power requirement	High	Low	Low
Range	Long	Short	Long
Intervention	High	Low	Very low
Interference	High	No	No
Security	Low	High	Very high

5. Conclusions

In this paper, 2 laser- and IR-based WRCSs are proposed, and their design and implementation are also given in detail. They primarily aim at enabling high security and short-range wireless remote access control, while keeping the cost low. A perforated plate is used at the receiver side of the laser-based WRCS, while OTP and mutual interrogation techniques are used in the IR-based WRCS. A specific communication protocol is also proposed, enabling an additional layer of security against unauthorized attempts to access the system, which is compatible with IR and laser frequencies for synchronous and asynchronous communication. A genuine trial study shows that the proposed WRCSs are reliable, accurate, and robust. The main advantage of the proposed

systems is that they utilize IR and laser frequencies instead of RFs to communicate between the client and server.

References

[1] P. Margaronis, L. Konstantinos, G. Stefanos, A. Emmanouil, C. Ilias, "Design and implementation of a cipher system (LAM) on a FPGA based on PCI architecture?, 6th International Conference on Microelectronics, Nanoelectronics, Optoelectronics, pp. 12–18, 2007.

[2] G. Jin, G. Xiang, "Design and simulation of electronic code lock using STC89C52 MCU based on C language, Modern Electronics Technique, doi: CNKI:SUN:XDDJ.0.2010-19-058, 2010.

[3] J. Cao, J. Sun, X. Sun, L. Ren, K. Du, "Design of the electronic password locks?, Journal of Chengdu University of Information Technology, doi: CNKI:SUN:CDQX.0.2010-02-004, 2010.

[4] G. Zhou, "The design of auto-alarming electronic cipher lock system with AT89C2051?, Journal of Mianyang Normal University, doi: CNKI:SUN:MYSF.0.2007-05-028, 2007.

[5] G. Jayendra, S. Kumarawadu, L. Meegahapola, "RFID-based anti-theft auto security system with an immobilizer", International Conference on Industrial and Information Systems, pp. 441–446, 2007.

[6] T. Hamalainen, M. Kivikoski, "Secure infrared control system for automotive applications", IEEE 22nd International Conference on Industrial Electronics, Control, and Instrumentation, Vol. 2, pp. 852–857, 1996.

[7] B. Fung, K. Al-Hussaeni, M. Cao, "Preserving RFID data privacy", IEEE International Conference on RFID Technologies and Applications, pp. 200–207, 2009.

[8] J. Al-Jaroodi, J. Aziz, N. Mohamed, "Middleware for RFID systems an overview", 33rd Annual IEEE International Computer Software and Applications Conference, Vol. 2, pp. 154–159, 2009.

[9] A.I. Alrabady, S.M. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved design", IEEE Transactions on Vehicular Technologies, Vol. 54, pp. 41–50, 2005.

[10] K.S. Khangura, N.V. Middleton, M. Ollivier, "Vehicle security systems", IEE Colloquium, pp. 41–47, 1993.

[11] M.J. Conrad, I. Howitt, "Introducing students to communications concepts using optical and low-power wireless devices", Turkish Journal of Electrical Engineering & Computer Sciences, Vol. 14, pp. 55–66, 2006.

[12] L. Wuming, H. Pingyang, Z. Ruilin, "Study on design and application of wireless sensor network based on communication of RFID system", 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–6, 2009.

[13] J. Landt, Shrouds of Time: The History of RFID, Pennsylvania, Association for Automatic Identification and Mobility, 2001.

[14] Y. Yalman, F. Akar, A High Capacity Reversible Data Hiding Method: HCRHide?, Imaging Science Journal, Volume. 62, Issue: 2, pp. 121–126, 2014.

[15] S.M. Mahmud, S. Shanker, "In-vehicle secure wireless personal area network (SWPAN)", IEEE Transactions on Vehicular Technology, Vol. 55, pp. 1051–1061, 2006.

[16] F. Zhang, D. Huang, Z. Dong, Y. Huang, "Design and implementation of automatic clearance control system based on RFID", Proceedings of the 7th World Congress on Intelligent Control and Automation, pp. 6621–6626, 2008.

[17] E.E. Aaron, Wireless Security Handbook, Florida, Auerbach Publications, 2006.

[18] A. Jain, K. Kant, M.R. Tripathy, "Security solutions for wireless sensor networks", 2nd International Conference on Advanced Computing and Communication Technologies, pp. 330–333, 2012.

[19] V. Aravinthan, V. Namboodiri, S. Sunku, W. Jewell, "Wireless AMI application and security for controlled home area networks", IEEE Power and Energy Society General Meeting, pp. 1–8, 2011.

[20] F. Ari, F. Ozek, O. Ozturk, O. Geren, "Techniques for link security in outdoor mobile laser optical wireless", International Transparent Optical Networks Conference, Vol. 3, pp. 160–163, 2006.

[21] Z. Li, K. Xi-Zheng, L. Jian, "The model and key technique researches of atmosphere laser communication system", 7th International Symposium on Antennas, Propagation and EM Theory, pp. 1–4, 2006.