Secure VLC services and practical applications

Noriharu Miyaho[*], *Noriko Konno*[*], *Takamasa Shimada*[*], *and Takashi Ogawa**
[*]*Tokyo Denki University*
Inzai, Chiba, Japan
miyaho@mail.dendai.ac.jp

Atsuya Yokoi [**]
[**]*Samsung R&D Institute Japan*
Yokohama, Japan

***Abstract*—Visible light communication (VLC) can play a very versatile role in IoT-based future communication services. In this paper, we described the latest encryption technology required to guarantee security specific to VLC and IoT(Internet of Things) to prevent eavesdropping, along with the corresponding communication services.**

Keywords—visible light communication, encryption, IoT

I. INTRODUCTION

Many different visible light communication (VLC) methods have been proposed and developed for commercial release. Visible light communication is characterized by freedom from the constraints of the laws governing radio transmission and allows visual inspection of data transmission/reception. Visual technology can prevent eavesdropping, a risk that is normally difficult to counter in wireless communication. All the light sources around us, such as room lighting, TV screens, traffic signals, and neon signs, have great potential to serve as visible light communication devices.

This paper adopts color shift keying (CSK) for the modulation of visible light communication services and describes the latest security mechanism of encryption of CSK [1]. Considering the potential IoT communication services, the encryption technology required to guarantee security for visible light communication. We describe a practical IoT Big data collection application and propose economically feasible IoT data communication services using VLC technology that provide added values in terms of convenience and safety.

II. SECURE COMMUNICATION REQUIREMENTS IN IOT-BASED COMMUNICATION-SOCIETY

It is becoming increasingly important to provide communication services that are secure and that give users the assurance of safety regardless of location. The information communication environment is characterized by the penetration of Big Data usage, based on widely distributed clouds, in addition to smartphone and IoT communication devices entering into our daily lives. However, the current communication security levels of clouds and communication services are not sufficient to give users the assurance of safety.

In light of this situation, this paper focuses on CSK, a modulation method for visible light communication, and discusses the technology of CSK-based communications between smart phones and other devices. CSK is one of the modulation schemes for VLC that was adopted in the IEEE802.15.7. Substantially, a conventional OOK (On Off Keying)-VLC system, any information are transmitted by the blinking of a light source. The CSK information are transmitted as color symbols that are generated by multi-color light sources such as RGB LEDs. The transmitter converts the data being sent into visible light CSK color information, using a rule that is kept confidential from third parties, and shows it continuously on the display. The receiver decodes the color information as follows. It uses the built-in camera of a smartphone or a Web camera to capture the image on the display, performs signal processing on the color information, and converts it back using the predetermined rule that was specified between the transmitter and the receiver in advance, and thus restores the original information. Because anyone can easily see the display, this information transport method should incorporate a means that ensures a high level of security. To achieve a high communication rate to broaden its potential application, it is necessary to increase the frame rate of the camera or incorporate space-division multiplexing (SDM). This paper proposes possible securely encrypted CSK communication services, where CSK cells are arranged in a specific frame shape.

III. PRINCIPLES OF CSK AND ITS APPLICATION

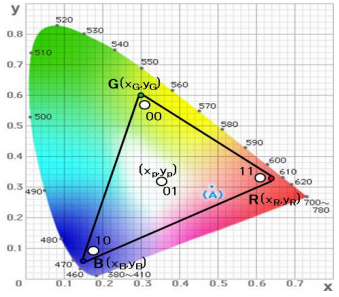

Fig. 1 CSK color symbol mapping on CIE1931 x-y color coordinates

Fig. 1 shows an example of CSK color symbol mapping

Published by Visible Light Communications Associated at "2nd International Conference and Exhibition on Visible Light Communications 2018" on March 16, 2018 in Yokohama, Japan.

on CIE1931 x-y color coordinates [2]. In this figure, R (x_R, y_R), G(x_G, y_G), and B(x_B, y_B) are the x-y color coordinates of the RGB light sources, and (x_p,y_p) is one of the allocated color points used as CSK color symbols. When an sRGB (standard RGB color space) display is used for the light sources, those coordinates are R(0.64,0.33), G(0.30,0.60), and B(0.15,0.06).

The information data mapped in Fig. 1 are coded into x-y values by the color mapping block, according to the color mapping rule. Four color points are placed in the RGB triangle as CSK color symbols. Those allocated color points are called a CSK color constellation. Moreover, this constellation example with four color points is called 4-CSK. Also defined in the IEEE standard are 8-CSK and 16-CSK. The x-y values are transformed into P_R, P_G, and P_B, each representing the power of the primary colors emitted by the RGB LEDs. The color of point (x_p, y_p) is determined by the relative strengths of the emitted primary colors from the three LEDs: P_R, P_G, and P_B. The relationship among (x_R, y_R), (x_G, y_G), (x_B, y_B), (x_p, y_p), P_R, P_G, and P_B are shown by the following simultaneous equations.

$$x_p = P_R \cdot x_R + P_G \cdot x_G + P_B \cdot x_B \quad (1)$$

$$y_p = P_R \cdot y_R + P_G \cdot y_G + P_B \cdot y_B \quad (2)$$

$$P_R + P_G + P_B = 1 \quad (3)$$

As Eq. (3) shows, the total power (P_R+P_G+P_B) is always constant. Furthermore, these power values are normalized to the value of one. Therefore, the actual total power can be arbitrarily set and can even be changed during CSK communication. The x-y values on the receiver's side are calculated from the received RGB light power P_R', P_G', and P_B'. Then, the x-y values are decoded into the received data. As mentioned above, the CSK color symbols are provided as visible colors that are generated by the RGB light sources, and the information is transmitted as the intensity ratio among the RGB light sources. CSK has the following advantages over the conventional OOK (On Off Keying)-VLC system.

1) Good connectivity guaranteed by the color coordinates
2) High speed and variable data rate with CSK constellation design
3) Illumination dimming available because of the constant normalized total power.

Furthermore, CSK is particularly suitable for image sensor communications from displays to cameras because it uses visible colors for its communication. All displays can be used as transmitters and all cameras can be used as receivers of CSK without additional hardware.

Let us consider the environments where the symbol rate is limited to 30 fps and the symbol rate of CSK is 15 Hz, and the data bit rate would be at most 60 bps when using 16-CSK. Two-dimensional CSK codes can be adopted to communicate from a display to a camera. The scheme is called Space Division Multiplexing CSK (SDM-CSK). If we use a 16×16 cell sized CSK code for SDM-CSK, the bit rate

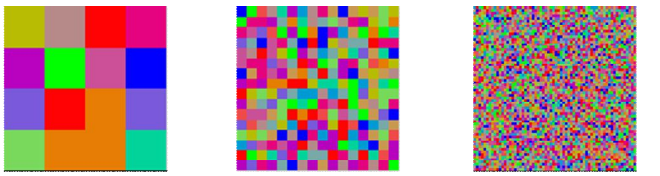

Fig. 2 Two-dimensional SDM-CSK code

increases 256-fold compared with normal CSK. Examples of SDM-CSK codes at 16-CSK are shown in Fig. 2.

In experiments with non-real time test system, the SDM-CSK system achieved 238 kbps data rate using 64×64 SDM-16CS at a symbol rate of 15Hz. A real time system which can send contents from a display to a smart phone, achieved a 1.44kbps data rate at 8 meters distance using 8×8 SDM-8CSK and a 12kbps data rate at 2 meters distance using 16×16 SDM-16CSK [3].

IV. Security Technology Specific to CSK Communication and Its Application

The proposed CSK communication system converts data into visible light color information based on a specified rule. In general, a CSK code has a high risk of third-party eavesdropping. Therefore, it is essential for CSK communication to incorporate an encrypted communication function. This paper proposes a new form of communication and a new communication service taking advantage of the characteristics of a scheme in which CSK color symbols are arranged and displayed in a specific frame shape. One possible means of encryption is for the transmitter and receiver to share a conversion table that associates the correspondence between an item of data to be transmitted and its chromaticity coordinates with the shape of the frame in which the cells are arranged. The specific data transmission procedure that guarantees secure communication between the transmitter and the receiver involves the following sequence of signal processing. Based on the correspondence (mapping table) between an item of data and its chromaticity coordinates:

(i) The transmitter associates the item of data with a frame shape type.
(ii) The transmitter changes the frame shape type at specified time intervals.
(iii) The receiver identifies the frame shape type and selects the associated mapping table.

Using these methods, CSK code encryption can be achieved by adopting either a different frame shape or a chromaticity coordinate area as an encryption key. Alternatively, both a frame shape and a chromaticity coordinate area can be used as encryption keys simultaneously.

These proposed methods make it extremely difficult to eavesdrop visible CSK code information. The level of security can be enhanced by extending the above methods. For example, multiple mapping table types and rules for their modification is predefined for each frame shape. The

transmitter changes the correspondence (mapping table) between an item of data and its chromaticity coordinates over time, and the modification rule is predefined as a hopping pattern (color hopping).

The CSK color symbols conversion method shown in Fig. 3 is based on the settings of the encryption keys. In Fig. 3, a triangular and a circular frame shape are separately predefined in mapping tables that show the correspondence between an item of data and its chromaticity coordinates. Needless to say, the kinds of frame shapes are not limited to the triangular or the circular frame. An ellipse, a square or other intricate patterns cab be applied as well [4].

The rules are predefined such that the two color symbols within the triangular frame are identified as information A and B, and the same two color symbols within the circular frame are identified as different information C and D, respectively. This mechanism can make eavesdropping impossible.

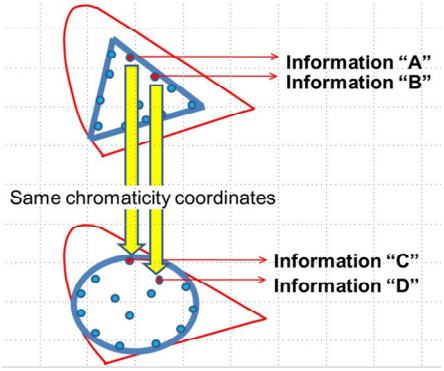

Fig.3 CSK color symbols conversion depending on the chromaticity coordinates

Fig.4 shows a configuration example of a CSK communication system having the ability to recognize the frame shape at a bank ATM using a CSK code displayed on the user's smartphone. The transmitter such as a smartphone, sends data by making the color of the chromaticity coordinates blink at a specific position within the frame shape using the data modulation section, which converts an item of data into chromaticity coordinates. The transmitter and receiver must use the same mapping table. A CMOS image sensor, which is used in mobile phones, can be used as a CSK code reception element. The receiver can identify a CSK code using the Web camera installed at a bank ATM. After identifying the displayed frame shape, it converts the chromaticity coordinates of the CSK code into data using a mapping table, which is associated with a specific frame shape type.

An error correction code, which automatically corrects CSK code reception errors, can be added as necessary. The transmitter can confirm correct data transmission as follows.

The transmitter sends a predefined test data pattern. If the receiver receives the pattern correctly, it notifies the acceptance to the transmitter by using a control signal. By making use of this confirmation method, it allows the transmitter to change the mapping table as it deems appropriate. The receiver can also demodulate data in synchronization with the transmitter. Since existing technologies can be applied to the transmitter and receiver in this way, new secure CSK communication services can be implemented economically.

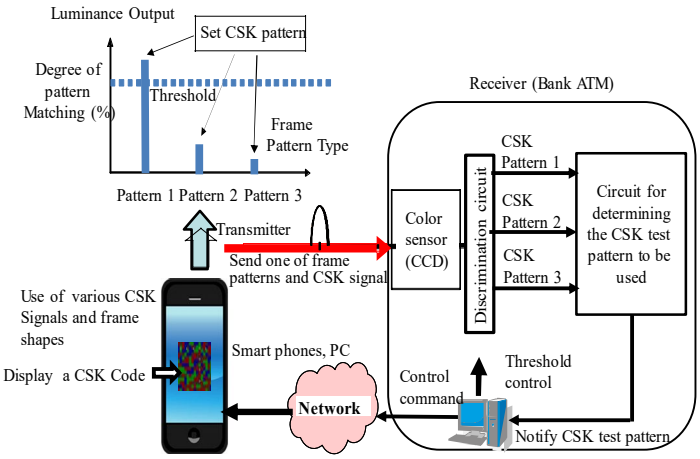

Fig.4 CSK communication system with a function to authenticate the frame shape pattern of a CSK code

V. PROPOSED NEW VLC COMMUNICATION SERVICES

A. New form of communication made possible by CSK

As mentioned before, the communication rate can be determined by changing the number of CSK code cells and encryption can be realized by changing frame shapes. The frame shape can be arbitrarily and appropriately pre-determined. In this section, we discuss the secure information transmission speed by using the jellyfish-shaped frame.

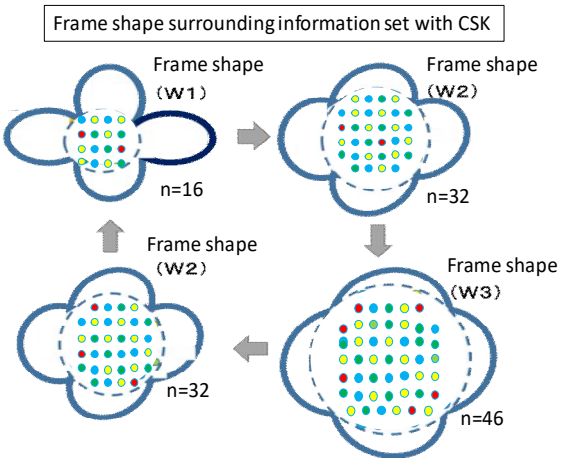

Fig.5 Example of enlarged and reduced patterns for a jellyfish-shaped frame

Fig.5 shows one form of encrypted communication

achieved by changing the frame shape of CSK code from W1 ⇨ W2 ⇨ W3 ⇨ W2 ⇨ W1 and changing the number of CSK code cells within the frame. The number of cells, n, contained in a frame shape varies depending on the shape, W1, W2 or W3. A frame shape can contain various cells, such as symbols for synchronization, dummy codes and an error correction code, in addition to the cells used to transfer information. When communication with a sufficiently high level of resolution is enabled, the amount of information and the code rate can be changed as appropriate depending on the size of the frame shape. In cases where the Reed-Solomon code is used as the error correction code, it is known that the following Eq. (4) must be met:

$$n = k + 2 \times t \quad (4)$$

where n is the number of symbols transmitted in one frame, t is the number of symbols that are corrected, and k is the number of information symbols (number of CSK code cells subject to error correction). One CSK code cell represents one symbol, and the net amount of information subject to coding is $k \times 4$ bits for 16-CSK. Since the number of newly required redundant symbols is 2t, the code rate becomes $(n\text{-}2t)/n$.

Thus, the use of the Reed-Solomon code, for example, enables effective utilization of the cell placement area using one of the specific multiple frame types. As a result, both error correction and enhanced encryption security can be achieved simultaneously. Using this communication method in a visible communication system, it is possible to display the CSK code frame shape in changing patterns resembling a swimming jellyfish and transmit data as the frame shape moves. This scheme presents a new option of providing a healing stimulus to a user. Reference [5] reports that when a video of a jellyfish was shown to subjects who had become irritable after performing complicated calculations, the levels of their salivary chromogranin A, which is used for a quantitative biochemical marker of affective state in patients' stress level, dropped, and their pulse waves stabilized. Also, in an experiment using optical topography, which is used to determine brain activity, a drop in the subjects' blood flow rates was observed. These experimental results suggest that a form of CSK communication that simulates swimming jellyfish can potentially provide a healing effect and help the user to recover from a feeling of fatigue. Fig.5 shows an example of enlarged, reduced, and moving patterns in a jellyfish-shaped frame.

B. Relation between CSK frame shape and error correction capability

We have already mentioned that the potential exist to improve the information transmission speed and provide a pleasant psychological effect by changing the CSK frame shape.

Here we note the theoretical trends in information transmission speed and symbol error correction capability, and offer practical examples.

By making use of Reed-Solomon code, since the number of newly required redundant symbols is 2t, the code rate becomes $(n-2t)/n$, where $t = (n-k)/2$, as mentioned above.

We assume that the size of a frame of any shape can be enlarged by a power of 2 in a range of psychologically comfortable environments. We assume for example, that n can be flexibly changed using the factor 2^m, where m is an integer.

In this paper, we do not present a precise evaluation of psychological effects, instead focusing on the effect of changing the number of correctable symbols along with changes in the CSK frame size. In this case, $t = 2^{m-1} - (k/2)$, where $t \le k$, should be taken into account.

It is preferable from the user's perspective if the amount of information inside the frame sent using CSK code is proportional to the size of the frame rather than its shape. In addition, the number of symbol error corrections should take the receiver's sensitivity to the CSK signals into consideration. The number of symbols, "k" that are genuine information-carrying signals may be assumed to vary from about 70% of n to about 90%.

Considering the conditions mentioned above,

$$t = 2^{m-1} - (k/2) = 2^{m-1} - (9/10) \times (2^{m-1}) = 2^{m-1} \times (1 - 9/10) = 0.1 \times 2^{m-1}$$

When k is set at about 70% of n, k equals $1.3 \times 2^{m-1}$.

As for the correction capability, when m is greater than 4 (meaning that the original cell size is increased by a factor of 16 or more), the number of error corrections reaches 5 symbols, which is sufficient to yield high quality communication. Generally speaking, the frame size can be enlarged by powers of 2 as long as the user's psychological comfort is taken into consideration and adequate reception of the signal is assured given the camera's capability.

Consider case W1 in Fig.5, where $n = 16$, so that $(n-k)/2 = (16-12)/2 = 2$.

This means that two symbol codes can be corrected in the case of about 80% n information utilization. In 16-CSK, which supports 30 symbols/s as a frame rate, the bit rate is equal to $4 \times 30 \times 12 = 1440\,(bps)$, and the inclusion of 12 symbols becomes possible. We can assume that this information transmission speed is adequate for use in a variety of warnings and messages. In the case of W2, the corresponding information utilizations are calculated to 80%, as well.

VI. VLC application service for secure mass data collection

If processing a great amount of data collected by the machine devices is assumed, the traffic load on the clouds will become too heavy to judge reasonable solutions. In order to prevent this kind of situation, edge computing has been proposed in which only primary processing of data is carried out and the detailed processing and analysis will be executed in the cloud. Thus in the edge computing, the level of the

communication traffic load between the edge and the cloud can be reduced. An example is described as follows.

Many sensor nodes and IoT devices are deployed for monitoring and measuring environmental changes between these device nodes to detect natural disasters and environmental influences . Detailed data will be transferred to the cloud and procssed there for a final judgment. For example, if photos taken by the street cameras match the registered suspcious characteristics, then detection can be accurately attained and images of the suspicious person will be transferred to the cloud and analyzed there.

If a high-speed link such as LTE or wireless LAN is continuously used between the edge, the cost and power consumption of the edge will become enormous. To solve this problem, Low Power Wireless Access (LPWA) networks such as Sigfox [6] and LoRa [7] should be deployed and used as much as possible. By limiting the communication speed to a narrow band, LPWA can economically accommodate terminals. Though this method is not suitable for communicating a large amount of data, however we can change it economical system by combining the LPWA, high-speed LTE/Wi-Fi, and secure VLC.

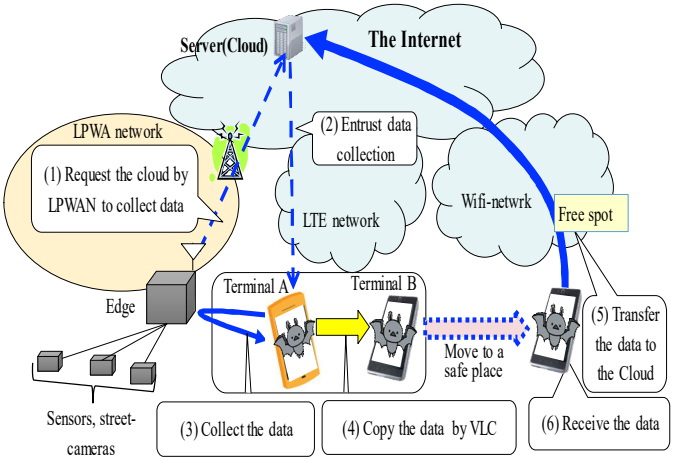

Fig.6 Secure IoT big data collection service by using VLC

The proposed hybrid mass data collection service is shown in Fig.6. For Big data collection application services, the terminals such as smartphones near the edge can be used for continuously transmitting data to the cloud. In this proposed system the GPS information will be used in the cloud. The edge is always connected to the cloud with LPWA. When it is necessary to transmit a large amount of data, it requests data collection to the cloud via LPWA ((1) of Fig. 7). The cloud entrusts data collection to terminal A in the vicinity of the edge and transmits the position information of the edge, the wireless LAN SSID and the password to the terminals ((2) of Fig.6). Terminal A sends a wireless LAN probe request notifying the data collection to the edge. If the edge detects the probe request, it wakes up the Wi-Fi circuit and sets up a Wi-Fi connection (3). Then it transmits the data addressed to the cloud to terminal A. Here we assume the introduction of a VLC terminal for secure and assured data transmission to Terminal B which can move and use safe and free wireless LAN environments. Then Terminal B can transfer the data to the cloud (5) after secure acquisition of them. Since almost all types of smartphone have display and camera functions, VLC can be easily utilized simply by adding the corresponding software functions. As VLC is used for close proximity communication, interception by a third party is impossible and a high level of security can be ensured, unlike communications using electromagnetic waves. Therefore, the total communication cost and power consumption of edges can be minimized. By utilizing VLC technology properly, a highly secure communication service can be ensured. We are currently developing a prototype, and planning field trials.

VII. Conclusions

This paper has presented the technology that can use the principle of CSK communication to provide secure and economical communication services in the near future. We clarified the innovative communication service concepts that can be implemented with the current technological level of CSK communications. To introduce CSK communication for commercial purposes, security must be highly enhanced by adopting encryption technologies which enhances the advantage of CSK communication. It should also be noted that changing the shape of the CSK frame cells can significantly improve security and the error free performances can be attained by increasing the number of CSK symbols in a frame.

References

[1] Sridhar Rajagopal, et al., "IEEE 802.15.7 Visible Light Communication: Modulation Schemes and Dimming Support," IEEE Communications Magazine, Vol.50, N0.3, pp72-82, Mar. 2012.

[2] CIE (1932) Commission Internationale de l'Eclairage Proceedings, Cambridge University Press, Cambridge, 1931.

[3] Atsuya Yokoi, Sangon Choi, Hiroki Mizuno, "A New Image Sensor Communication System Using Color Shift Keying," ICEVLC2015, Nov., 2015.

[4] Patent (pending), WO/2015/163746, 2015.

[5] Representative Researcher Professor Juro Hiromi, Department of Marine Science and Resources, "Scientific Verification of the Healing Effects of Jellyfish – From the Viewpoint of Exploring New Resource Value of Marine Life," General Research Grant, Department of Marine Science and Resources, Nihon University, pp.8-11, 2007 (in Japanese).

[6] SIGFOX, available from (https://w3bin.com/domain/sigfox.com) (2017/12/6)

[7] LoRa Alliance, available from https://www.woorank.com/en/www/lora-alliance.org (2017/10/1).