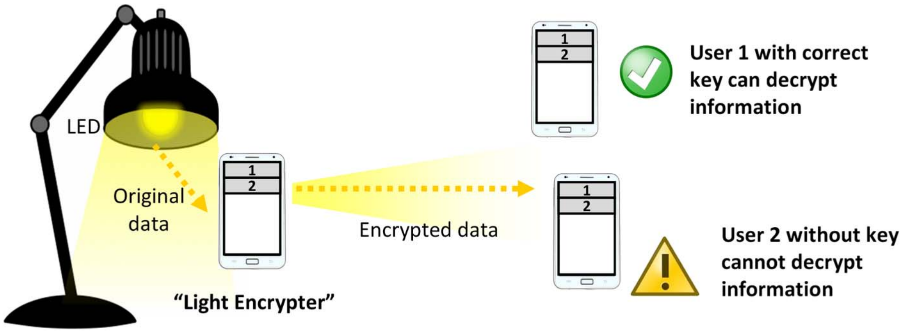
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Light Encryption Scheme Using Light-Emitting Diode and Camera Image Sensor

Volume 8, Number 1, February 2016

Yang Liu
Kevin Liang
Hung-Yu Chen
Liang-Yu Wei
Chin-Wei Hsu
Chi-Wai Chow, Senior Member, IEEE
Chien-Hung Yeh


LED
Original data
1
2
"Light Encrypter"
Encrypted data
User 1 with correct key can decrypt information
User 2 without key cannot decrypt information

DOI: 10.1109/JPHOT.2016.2519287
1943-0655 © 2016 IEEE

Light Encryption Scheme Using Light-Emitting Diode and Camera Image Sensor

**Yang Liu,[1] Kevin Liang,[2] Hung-Yu Chen,[2] Liang-Yu Wei,[2] Chin-Wei Hsu,[2]
Chi-Wai Chow,[2] *Senior Member, IEEE*, and Chien-Hung Yeh[3]**

[1]Philips Electronics Ltd., Shatin, Hong Kong
[2]Department of Photonics and Institute of Electro-Optical Engineering,
National Chiao Tung University, Hsinchu 30010, Taiwan
[3]Department of Photonics, Feng Chia University, Taichung 40724, Taiwan

DOI: 10.1109/JPHOT.2016.2519287
*1943-0655 © 2016 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.*

Manuscript received December 20, 2015; revised January 11, 2016; accepted January 15, 2016. Date of current version January 27, 2016. This work was supported in part by the Ministry of Science and Technology of Taiwan under Grant MOST-104-2628-E-009-011-MY3 and Grant MOST-103-2221-E-009-030-MY3; by Aim for the Top University Plan, Taiwan; and by the Ministry of Education of Taiwan. Corresponding author: C.-W. Chow (e-mail: cwchow@faculty.nctu.edu.tw).

Abstract: Visible light communication (VLC) is regarded as relatively secure communication when compared with other wireless communications using radio frequency (RF). However, due to the visual nature, the VLC signals are still subject to eavesdropping when they are emitted by the light source. Here, we propose a light encryption scheme using devices having light-emitting diode (LED) and a camera image sensor, such as a mobile phone. The original visible signal sending from the lamp can be first received by the proposed light encrypter. The information can be encrypted and then emitted. The light encrypter acts as an encryption gateway for signals in optical domain. The rolling shutter effect of the complementary metal–oxide semiconductor (CMOS) camera in the mobile phone can be used. By demodulating the rolling shutter pattern, the data information can be obtained. We also propose and demonstrate using the Otsu thresholding scheme to define the data logic in the rolling shutter pattern. We show that the Otsu scheme is effective for estimating the bit error rate (BER). The optimum number of intervals (segmentations) and the process time of the Otsu method are also studied.

Index Terms: Free space communication, optical communications, light-emitting diode (LED).

1. Introduction

Visible light communication (VLC) [1]–[7] has been considered as one of the promising solutions for future fifth-generation (5G) wireless networks since it is license-free, and it uses the extra electromagnetic spectrum (the visible light spectrum) instead of the congested traditional radio-frequency (RF) spectrum for communications. Besides, VLC is very directional; hence, the communication zone can be confined to a small area [8]. A high density and high capacity wireless communication can be achieved. VLC also works well for under-water communication and future data-center networks [9]. VLC is regarded as a relatively securer communication [8] when compared with other wireless communications using RF, since VLC is directional and does not penetrate walls. Therefore, people outside the illuminance zone cannot receive the information.

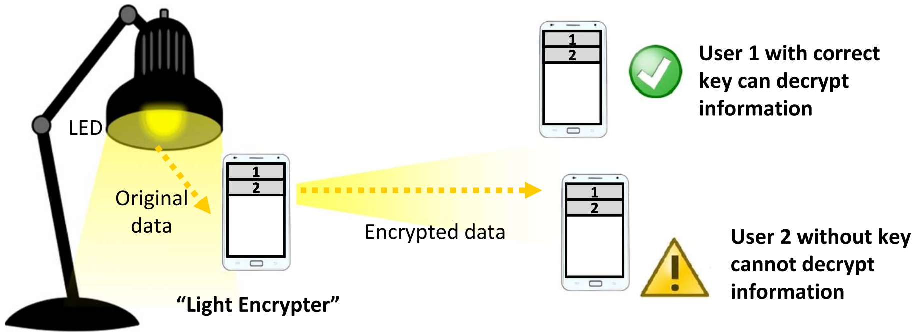

LED
Original data
"Light Encrypter"
Encrypted data
1
2
User 1 with correct key can decrypt information
User 2 without key cannot decrypt information

Fig. 1. Proposed light encryption scheme, using, for example, a mobile phone as a light encrypter.

However, due to the visual nature, the VLC signals are still subject to eavesdropping when they are emitted by the light source.

In this work, we propose and demonstrate a light encryption scheme using devices with light emitting diode (LED) and camera image sensor receiver (Rx), such as a mobile phone, palmtop or laptop computers. The original visible light signal sending from the ceiling lamp or desktop lamp can be first received by the proposed light encrypter; then, the information can be encrypted using a private key or other advanced encryption algorithms. Then, the encrypted signal can be emitted as visible light by this light encrypter. The light encrypter acts as an encryption gateway for signals in optical domain. The Rx in this light encrypter can be a positive-intrinsic-negative (PIN) photodiode (PD), an avalanche photodiode (APD), or a camera image sensor in the mobile phone. As mobile phone plays an important role in our daily lives, in the proof-of-concept demonstration, we use the mobile phone camera image sensor as the VLC light encrypter Rx. Rolling shutter effect of the complementary metal–oxide semiconductor (CMOS) camera can be used to enhance the transmission data rate higher than the frame rate of the camera [10]. Then, by demodulating the rolling shutter pattern (bright and dark fringes received by the camera), the data information can be obtained. However, [11] requires complicated histogram equalization together with Sobel edge detection for the bright and dark fringes extinction ratio (ER) enhancement. Here, we propose and demonstrate using the Otsu thresholding scheme for the first time up to our knowledge to define the data logic in the rolling shutter pattern. The Otsu method is very popular for segmenting a picture in image processing [12]. Here, we show that the Otsu scheme is also effective to define the data logic in the rolling shutter pattern for estimating the bit-error-rate (BER). We also apply the smoothing scheme to reduce the data pattern fluctuation. The optimum number of intervals (segmentations) and the process time of the Otsu method are also studied.

2. Proposed Architecture

Fig. 1 shows our proposed light encryption system using mobile phone as the light encrypter. The VLC signal sending from a desk lamp can be received by our light encrypter, which could be any device having optical Rx, such as PIN PD, or an camera image sensor, and having a visible LED for the optical transmitter (Tx). Here, we use mobile phone as the light encrypter since it has a camera and a white-light LED. After the visible light signal is received in the light encrypter, the information can be encrypted using different encryption algorithms. Since we just want to prove the concept, we simply perform a xor operation with a common private key (known as symmetric-key) for the data encryption. At the decryption side, the same key can be used to perform the xor operation with the encrypted signal to retrieve the decrypted signal. It is worth to mention that the proposed scheme can be a multicast system (supporting multiple devices with the correct key). In the symmetric-key scheme, besides the xor operation, other schemes, such as shift-cipher (i.e., shifting the bits forward or backward in a fixed pattern), can be used. More advanced encryption schemes, such as public-key cryptography [13], can be

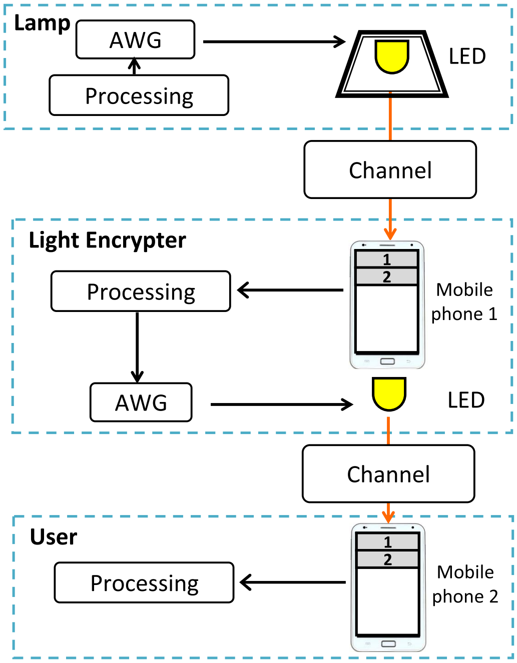


Fig. 2. Proof-of-concept demonstration of the light encryption and decryption.

applied. In the public-key scheme, anyone can have the public key and can encrypt the message, but only the holder of the private key can decrypt it. To increase the level of security, the private key can be send via RF to the mobile-phone instead of via visible light.

3. Experiment, Results, and Discussion

Fig. 2 shows the proof-of-concept experiment. A pseudo-random data is generated by a Matlab program is stored in an arbitrary waveform generator (AWG, Tektronix, AFG 3252C) with 240 MHz bandwidth and 2 GSample/s sampling rate. It acts as a digit-to-analog converter (DAC) to drive the LED. The LED used is a single cool-white LED (Cree XR-E LED) with color temperature of 5000 K. In the experiment, the driving current is about 300 mA, and the measured 3-dB modulation bandwidth is about 1.2 MHz. The white-light signal ("original signal") is then received by our proposed light encrypter (the mobile phone). The original VLC signal is received by a CMOS camera image sensor with resolution of 640 × 480 pixels and frame rate of 28 frame/s. Then xor operation will be performed between the received original signal and a private key to generate the encrypted data, which can then be emitted by a white-light LED in the light encrypter. In this proof-of-concept demonstration, offline signal processing is used. Finally, the encrypted VLC signal is received by another mobile phone. Another xor operation will be performed between the received encrypted signal and the private key; hence the decrypted signal can be retrieved.

As shown in Fig. 2, first, the original signal will be received by a CMOS camera image sensor in the light encrypter. Rolling shutter effect of the CMOS camera is used [10]. Then, by demodulating the rolling shutter pattern, the information can be obtained. In the rolling shutter operation reported in [11], the pixel row is activated without waiting for the scanning completion of the previous pixel row. Hence, the effective number of bits represent in each image frame is smaller than the vertical resolution of the image sensor. Besides, there is also a processing time-gap between each frame [11]. Hence, each packet is transmitted three times successively to ensure each image contains a complete data packet. As a result, the net data rate (by removing the header and the successive packets) is 0.98 kbit/s. In this work, we propose and

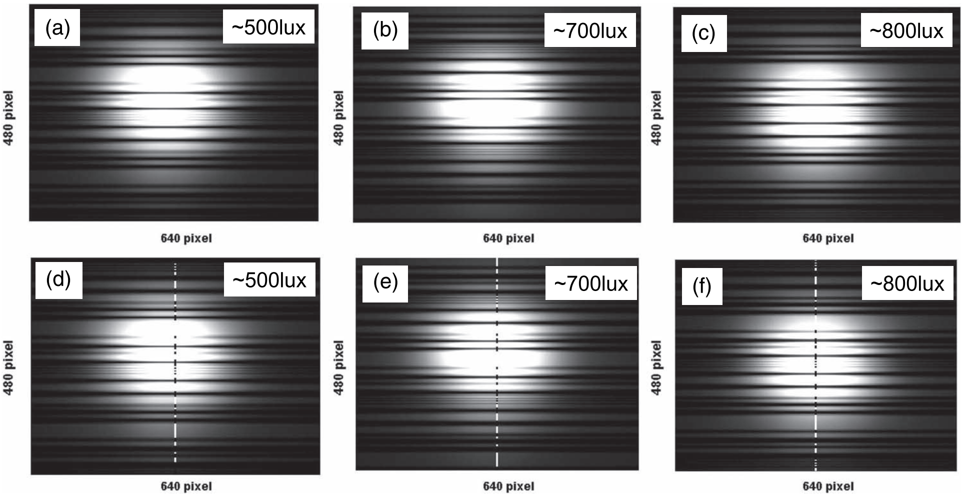


Fig. 3. (a)–(c) Rolling shutter patterns (bright and dark fringes) obtained by the CMOS image sensor at difference illuminance levels. (d)–(f) By the automatic vertical column pixel selection scheme, the selected column patterns are pasted on top of the original rolling shutter patterns to illustrate the improvement in the contrast.

demonstrate using the Otsu thresholding scheme to define the data logic in the rolling shutter pattern. Fig. 3(a)–(c) show the rolling shutter patterns (bright and dark fringes) obtained by the CMOS image sensor at difference illuminance levels. Higher illuminance produces clearer image (i.e., more distinguishable fringes). The VLC signal is packet-based and each packet is composed of a 4-bit Manchester coded header and a 35-bit on-off keying (OOK) payload. The Manchester coded header is used for signal synchronization. Since each bit of the Manchester signal is consist of a low-level and a high-level; much narrower periodic bring and dark fringes can be easily observed in the image of the rolling shutter pattern. Then, by estimating the frequency of these narrower header fringes, the payload clock rate can be estimated. A two minutes video is recorded for each BER measurement. In the demodulation of the rolling shutter pattern, the recorded movie file is converted into grayscale format, so that grayscale level of 255 represents total brightness and 0 represents total darkness. As also shown in Fig. 3(a)–(c), "booming" effect can be observed. Hence, an automatic vertical column pixel selection scheme described in [11] is applied. This scheme can avoid the booming region (too bright) and the too dark region (at the edges of the image). Then, the selected column patterns are pasted on top and at the center of the original rolling shutter patterns to illustrate the improvement in the contrast, as shown in Fig. 3(d)–(f).

Even though we applied the column pixel selection scheme, ER fluctuation still critical particularly at the fast changing region of the data pattern. Then, we apply the "smoothing" scheme [14] to enhance the ER. The idea is to construct a second order polynomial fitting equation ["poly-smoothing 1" in Fig. 4(a)] that can approximately connect a series of grayscale data values. Then the grayscale values greater than the "poly-smoothing 1" equation are assigned equal to the values of that equation. Next, another polynomial fitting equation ["poly-smoothing 2" in Fig. 4(a)] is constructed, so that the grayscale values smaller than the "poly-smoothing 2" equation are assigned equal to zero. Therefore, the ER fluctuation is significantly reduced, as shown in Fig. 4(b).

Then, a suitable thresholding scheme is required to define the data logic. As mentioned in the introduction, the Otsu method is very popular for segmenting a picture in image processing. Here, we show that it is also a very effective method for define the data logic in the rolling shutter pattern. Its basic idea is to look for a threshold that can minimize the within-class variance (or intra-class variance). Assume the threshold value of the grayscale data pattern is t, and $0 < t < 255$. Hence the grayscale data pattern can be divided into two groups: One group has

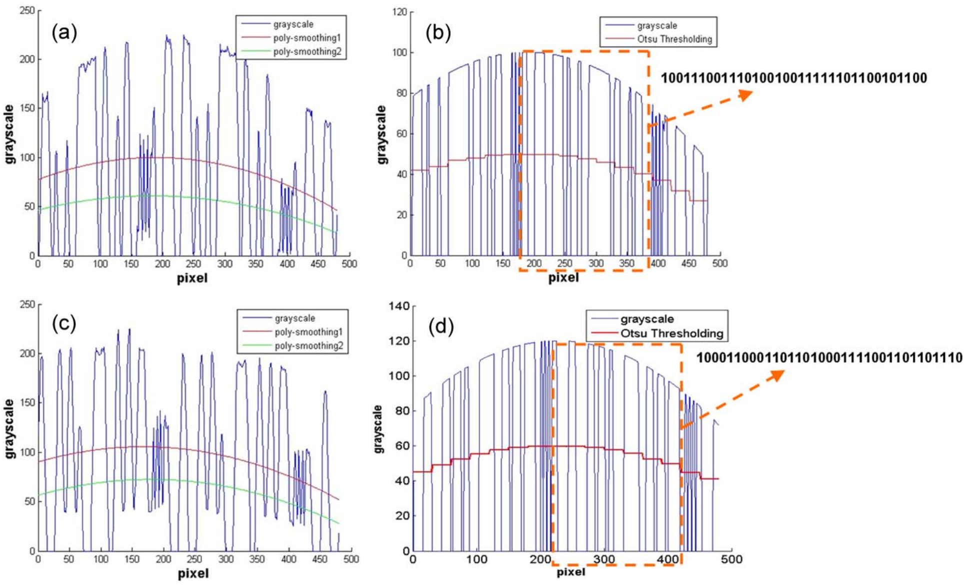


Fig. 4. Data pattern of original signal (a) before and (b) after applying the polynomial smoothing and the data pattern of the encrypted signal (c) before and (d) after applying the polynomial smoothing. The dotted areas indicate the payload data before and after the encryption.

element with grayscale value smaller than t, and the other group with greyscale value larger than t. Assume that N, $N_1(t)$, and $N_2(t)$ are the total number of pixels, number of pixels in group 1 $(\text{grayscale} < t)$, and number of pixels in group 2 $(\text{grayscale} > t)$ respectively. The class probabilities can be calculated as

$$\omega_1(t) = \frac{N_1(t)}{N}, \quad \omega_2(t) = \frac{N_2(t)}{N}. \tag{1}$$

Then, the class means can be calculated as

$$\mu_1(t) = \sum_{i=1}^{t} \frac{P_i}{\omega_1(t)}, \quad \mu_2(t) = \sum_{i=t+1}^{255} \frac{P_i}{\omega_2(t)} \tag{2}$$

where P_i is the probability of the ith grayscale value. Then, the individual class variances are

$$\sigma_1^2(t) = \sum_{i=1}^{t} \frac{iP_i}{\omega_1(t)} \left[i - \mu_1(t)\right]^2, \quad \sigma_2^2(t) = \sum_{i=t+1}^{255} \frac{iP_i}{\omega_2(t)} \left[i - \mu_2(t)\right]^2. \tag{3}$$

Finally, the intra-class variance is obtained in

$$\sigma_w^2(t) = \omega_1(t)\sigma_1^2(t) + \omega_2(t)\sigma_2^2(t). \tag{4}$$

Now, all we need to do is to run through the t from 0 to 255, and find the value that minimizes $\sigma_w^2(t)$. After this, the threshold in the data pattern can be defined [the red-curves in Fig. 4(b) and (d)]. The data logic of the 35-bit original payload data is {10011100111010010011111101100101100}. The xor operation will be performed between the original payload data and a 35-bit key {0001000010000100001000010}. After this, the encrypted data pattern of {10001100011011010001111001101101110} can be generated. This data will be re-emitted by another white-light LED in the light encrypter. Finally, the "user" mobile phone in Fig. 2 can receive the encrypted optical signal as shown in Fig. 4(c). Then, we apply the same column pixel selection scheme, polynomial smoothing scheme, and Otsu thresholding scheme as described above. Finally, the encrypted data pattern with reduced ER fluctuation and properly

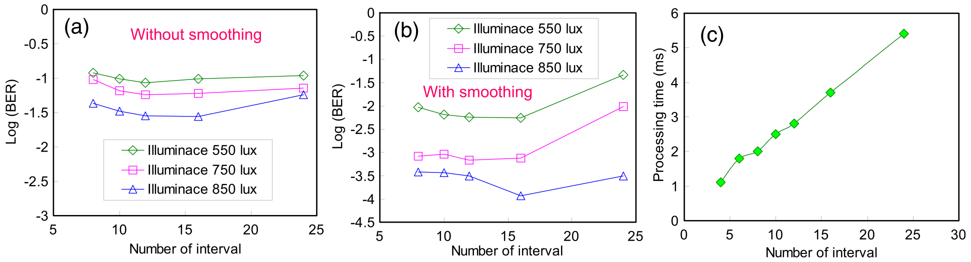


Fig. 5. (a) and (b) BER performance against different number of Otsu intervals under different illuminance levels without and with applying the smoothing scheme. (c) Processing time to perform the Otsu thresholding scheme.

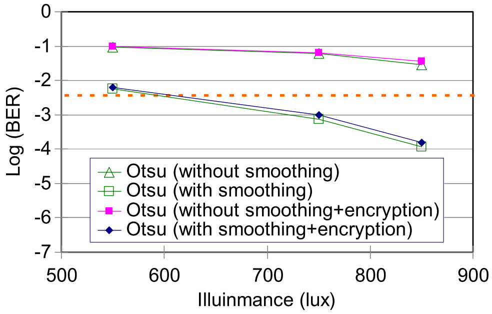


Fig. 6. Measured BER of the original data and the encrypted data under different illuminance.

thresholding can be obtained in Fig. 4(d). The dotted areas indicate the payload data before and after the encryption.

Then, we analyze the number of intervals needed and the processing time to perform the Otsu thresholding scheme. Fig. 5(a) and (b) show the BER performance against different number of Otsu intervals under different illuminance levels without and with applying the smoothing scheme. We can observe that at low illuminance, dividing the data pattern into 12 and 16 Otsu-intervals can provide the lowest BER. At high illuminance, using 16 Otsu-intervals is better; hence, in our proof-of-concept experiment, 16 Otsu-intervals are selected. Besides, when the number of Otsu-intervals increases, the processing time needed for thresholding the whole data pattern increases, as shown in Fig. 5(c). Here, the computer we use for the off-line processing has an Intel i5-4210U central processing unit (CPU); 4 GB random access memory (RAM), and Matlab 2007. The processing times for the 12 and 16 Otsu-intervals are 2.8 ms and 3.7 ms, respectively.

Finally, the BER analysis of the original data and the encrypted data under different illuminance levels are studied, as shown in Fig. 6. Negligible power penalty is observed in the encryption. In this proof-of-concept experiment, only a single white-light LED is used, and the transmission distance at ~550 lux is ~25 cm. A LED array or a higher brightness LED can be used to increase the transmission distance. Fig. 6 shows that using the proposed smoothing scheme can enhance the BER due to the reduction of ER fluctuation. A significant BER enhancement with up to 2 orders of magnitude can be observed at high illuminance cases. Furthermore, by using the smoothing scheme, BER satisfying the forward error correction (FEC) limit can be achieved.

4. Conclusion

VLC is regarded as a relatively securer communication when compared with other wireless communications using RF. However, due to the visual nature, the VLC signals are still subject to eavesdropping when they are emitted by the light source. Here, we proposed a light encryption scheme. The original visible light signal sending from the lamp can be first received by our proposed light encrypter; then, the information can be encrypted, which can then be emitted as visible light by this light encrypter. In this work, we also proposed and demonstrated using the Otsu thresholding scheme to define the data logic in the rolling shutter pattern. We analyzed that at high illuminance using 16 Otsu-intervals was better. Processing time was also studied. Besides, the proposed smoothing scheme can significantly enhance the BER with up to 2 orders of magnitude at high illuminance due to the reduction of ER fluctuation.

References

[1] B. Janjua *et al.*, “Going beyond 4 Gbps data rate by employing RGB laser diodes for visible light communication,” *Opt. Exp.*, vol. 23, no. 14, pp. 18746–18753, Jul. 2015.

[2] Y. C. Chi *et al.*, “450-nm GaN laser diode enables high-speed visible light communication with 9-Gbps QAM-OFDM,” *Opt. Exp.*, vol. 23, no. 10, pp. 13051–13059, May 2015.

[3] W. Y. Lin *et al.*, “10 m/500 Mbps WDM visible light communication systems,” *Opt. Exp.*, vol. 20, no. 9, pp. 9919–9924, Apr. 2012.

[4] C. W. Chow, C. H. Yeh, Y. Liu, and Y. F. Liu, “Digital signal processing for light emitting diode based visible light communication,” *IEEE Photon. Soc. Newslett.*, vol. 26, pp. 9–13, 2012.

[5] H. H. Lu *et al.*, “A multiple-input-multiple-output visible light communication system based on VCSELs and spatial light modulators,” *Opt. Exp.*, vol. 22, no. 3, pp. 3468–3474, Feb. 2014.

[6] Z. Wang, C. Yu, W. D. Zhong, J. Chen, and W. Chen, “Performance of a novel LED lamp arrangement to reduce SNR fluctuation for multi-user visible light communication systems,” *Opt. Exp.*, vol. 20, no. 4, pp. 4564–4573, 2012.

[7] S. Wu, H. Wang, and C. H. Youn, “Visible light communications for 5G wireless networking systems: From fixed to mobile communications,” *IEEE Netw.*, vol. 28, no. 6, pp. 41–45, Nov./Dec. 2014.

[8] C. W. Chow *et al.*, “Secure communication zone for white-light LED visible light communication,” *Opt. Commun.*, vol. 334, pp. 81–85, Jun. 2015.

[9] C. H. Chang *et al.*, “A 100-Gb/s multiple-input multiple-output visible laser light communication system,” *J. Lightw. Technol.*, vol. 32, no. 24, pp. 4723–4729, Dec. 2014.

[10] P. Luo *et al.*, “Experimental demonstration of RGB LED-based optical camera communications,” *IEEE Photon. J.*, vol. 7, no. 5, Oct. 2015, Art. ID 7904242.

[11] C. W. Chow, C. Y. Chen, and S. H. Chen, “Enhancement of signal performance in LED visible light communications using mobile phone camera,” *IEEE Photon. J.*, vol. 7, no. 5, Oct. 2015, Art. ID 7903607.

[12] N. Otsu, “A threshold selection method from gray-level histograms,” *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-9, no. 1, pp. 62–66, Jan. 1979.

[13] N. Ferguson and B. Schneier, *Practical Cryptography*. New York, NY, USA: Wiley, 2003.

[14] Y. Liu *et al.*, “Visible light communication using receivers of camera image sensor and solar cell,” *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2015, Art. ID 7800107.