Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 2326563, 7 pages
http://dx.doi.org/10.1155/2016/2326563

Research Article

A Chaos-Based Encryption Scheme for DCT Precoded OFDM-Based Visible Light Communication Systems

Zhongpeng Wang[1,2] and Shoufa Chen[1]

[1]*School of Information and Electronic Engineering, Zhejiang University of Science and Technology, Hang Zhou 310023, China*
[2]*State Key Laboratory of Millimeter Waves, Southeast University, Nanjing 210096, China*

Correspondence should be addressed to Zhongpeng Wang; wzp1966@sohu.com

Received 30 April 2016; Revised 26 June 2016; Accepted 19 July 2016

Academic Editor: Maher Jridi

This paper proposes a physical encryption scheme for discrete cosine transform (DCT) precoded OFDM-based visible light communication systems by employing chaos scrambling. In the proposed encryption scheme, the Logistic map is adopted for the chaos mapping. The chaos scrambling strategy can allocate the two scrambling sequences to the real (I) and imaginary (Q) parts of OFDM frames according to the initial condition, which enhance the confidentiality of the physical layer. The simulation experimental results prove the efficiency of the proposed encryption method for DCT precoded OFDM-based VLC systems. The experimental results show that the proposed security scheme can protect the DCT precoded OFDM-based VLC from eavesdropper, while keeping the advantage of the DCT precoding technique, which can reduce the PAPR and improve the BER performance of OFDM-based VLC.

1. Introduction

Visible light communication (VLC) using light emitting diodes (LEDs), where the LEDs are used for both illumination and data wireless transmission, has received increasing attention among the researchers worldwide [1, 2]. Its distinct advantages are the license-free light spectrum, immunity to radio frequency (RF) interference, safety to human body, and the use of inexpensive light emitting diodes (LEDs). VLC can be viewed as a complement to RF in the face of the looming spectrum crunch [3].

Due to the greater immunity to multipath fading and reducing the complexity of equalizer, orthogonal frequency division multiplexing (OFDM) is one of the most popular techniques for high data rate communication. It has been accepted in the IEEE802.11a local area network (LAN), IEEE802.16 WiMax, digital audio broadcasting (DAB), and digital video broadcasting (DVB) and next generation mobile technologies 3GPP LTE [4]. To achieve higher spectral efficiency, OFDM is being considered as a crucial technique for indoor VLC systems. The most practical communication scheme for VLC systems is intensity modulation (IM) along with direct detection (IM/DD), of which the transmitted signal is usually modulated on the instantaneous power of light emitting diodes (LEDs) at the transmitters and photodiodes (PDs) are used at photoelectric converters at the receivers. Therefore, the generated OFDM time domain signal in OFDM-based IM/DD should be real-valued and nonnegative. This can be achieved by enforcing Hermitian symmetry constraint on the input data of the IFFT at the transmitters in order to generate real-valued signal. Depending on how the real-valued signal is converted to a nonnegative signal, three schemes have been proposed: (1) DC-biased optical OFDM (DCO-OFDM), (2) Asymmetrically-Clipped optical OFDM (ACO-OFDM), and (3) pulse-amplitude-modulated discrete multitone (PAM-DMT). For DCO-OFDM scheme, a DC offset is added to the real-valued signal to obtain a nonnegative signal [5]. For improving the throughput and capacity and/or the power efficiency, MIMO techniques, which offer a spatial gain, have been used in VLC. Meantime, in order to achieve higher bit error rate (BER) performance, precoding technique has been employed for OFDM systems, such as DCT precoding and DFT precoding [6, 7].

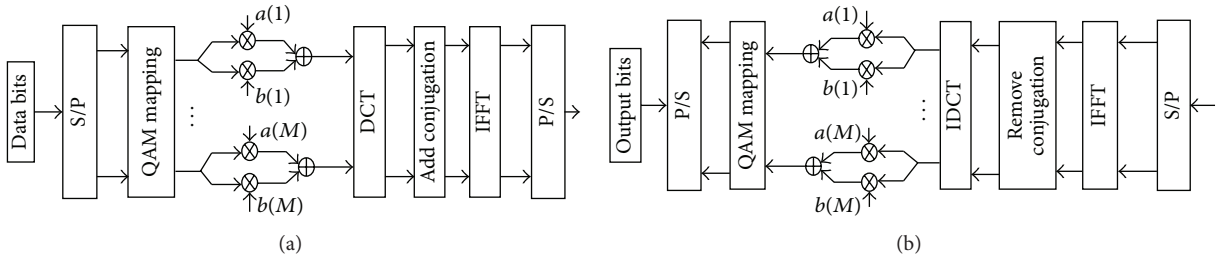

Figure 1: (a) Encryption principle for transmitter. (b) Decryption principle for receiver.

On the other hand, with the dramatic growth in wireless network capacity and accessibility of wireless network, data privacy and confidentiality are becoming a major concern for users. In some public areas such as classrooms, hallway, and planes, the transmitted signals in VLC link are susceptible to the eavesdropping. Many security measures can be adopted at upper layer of the network stack via access control and end-to-end encryption. For instance, the use of encryption end decryption scheme (DES, AES, etc.) can be implemented in the application layer of communication networks. During the past few years, however, the use of physical layer security techniques has attracted wide attention of scholars. Some physical secure strategies have been proposed in wireless communication and optical OFDM communication systems for fiber link [8–12]. Among these proposed schemes, chaos mapping techniques have usually been employed to enhance the security of physical layer. Recently, some related works in [13–16] considered improving the confidentiality of VLC links via physical security methods. However, to the best of our knowledge, the secure researching on precoded OFDM-based VLC systems has not been reported.

Without loss of generality, we will focus on DCO-OFDM-based VLC based in this paper. We firstly propose a novel secure DCT precoded OFDM-based VLC using chaos scrambling technique. In the proposed DCT precoded and encrypted OFDM-based VLC, the transmission security can be realized by the chaos scrambling sequence while the reliability can be improved via using DCT precoding. The simulation results show that the transmitted signal cannot be recovered at the eavesdropper due to the unknown secure key consisting of the initial value, the bifurcation parameter, and iteration step. Thus, the approach can provide scalable secure strategy in DCT precoded OFDM-based VLC application.

This paper is organized as follows. In Section 2, OFDM encryption scheme is introduced and described briefly. In Section 3, the system principle of encrypted and DCT precoded OFDM-based VLC is described. After that, simulation results and analysis are shown. Finally, Section 4 concludes this paper.

2. OFDM Encryption Scheme

In our proposed secure transmission scheme, the OFDM signal is encrypted using chaotic sequence. The chaos sequence is generated based on a Logistic map, which is controlled by the initial value and iteration parameter. A chaos model using Logistic map has the following iterative formula [17]:

$$x(n+1) = f(x(n)) = \mu x(n)(1 - x(n)), \quad (1)$$

where n is a time index, $x(0)$ is the initial value, $x(n)$ is the nth state value of (2), $x(n) \in (-1, 1)$, and $\mu \in [1, 4]$. μ is the bifurcation parameter or control parameter. When μ falls into the domain $3.569945 < \mu \leq 4$, the behavior changing of $x(n)$ will fall into chaos. To obtain a chaos sequence, a transform function is used to x_n; it is expressed as

$$s(n) = \begin{cases} -1, & 0 \leq x(n) \leq 0.5, \\ 1, & 0 \leq x(n) \leq 1, \end{cases} \quad (2)$$

where $s(n)$ is the nth element of the generated chaotic sequence. The chaos sequence can be obtained by (1) and (2). In the practical applications, some initial iterated values $\{x(n),\ n = 1, 2, \ldots, N\}$ are abandoned, where N is iteration step.

Based on (1) and (2), we can get two difference chaos sequences containing values form 1 and −1. The two chaos sequences are employed to encrypt the real and image parts of QAM symbol sequence, respectively. In this scheme, the secure key consists of the initial value x_0, the bifurcation parameter μ, and iteration step N. We assume that a and b are the generated chaos sequences where $a(m) \in \{-1, 1\}$ and $b(m) \in \{-1, 1\}$, respectively.

In the transmitter end, the transmitted data vector S with M length after the encryption can be represented as follows:

$$Z(m) = \text{real}(S(m)) \cdot a(m) + \text{imag}(S(m)) * b(m), \quad (3)$$

where $m = 1, 2, \ldots, M$. This is shown in Figure 1(a).

The receiver can decrypt the encrypted data by using its own key sequence. The decryption process can be written as follows:

$$S(m) = \text{real}\left(Z'(m)\right) \cdot a(m) + \text{imag}\left(Z'(m)\right) \cdot b(m), \quad (4)$$

where $Z'(m)$ is the output of the fast Fourier transform (FFT). The process is shown in Figure 1(b).

We assume that the M-order chaos scrambling sequence is generated to encrypt I and Q parts of frequency information signal. Here the randomness of Logistic chaos mapping

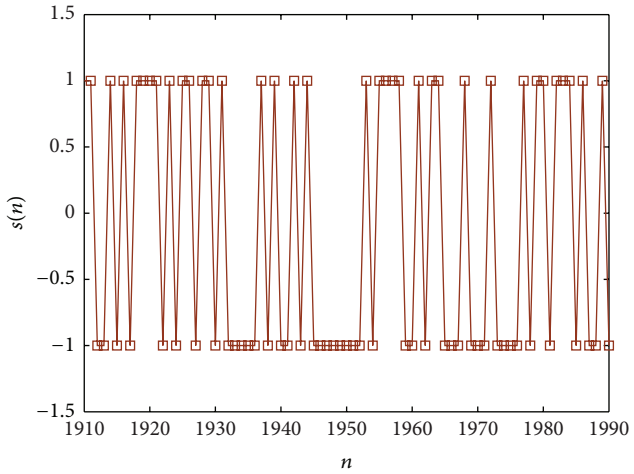

Figure 2: Chaos sequence for $\mu = 4$, $x_0 = 0.329999$, and $N = 2000$.

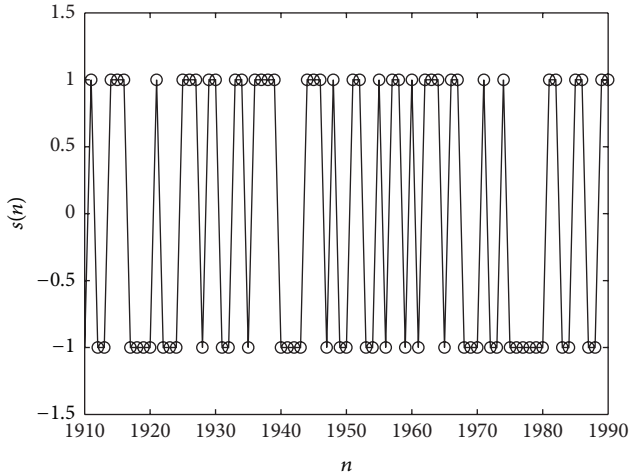

Figure 3: Chaos sequence for $\mu = 4$, $x_0 = 0.329998$, and $N = 2000$.

can be evaluated in terms of autocorrelation and cross-correlation functions of the chaos sequence. The normalized autocorrelation and cross-correlation functions of a random sequence with length M are defined as

$$R_{\text{ac}} = \frac{1}{M}\sum_{m=0}^{M-1} b_j(m)\, b_j(m+k), \quad -(M-1) \le k \le M-1,$$
$$R_{\text{cc}} = \frac{1}{M}\sum_{m=0}^{M-1} b_h(m)\, b_j(m+k), \quad -(M-1) \le k \le M-1. \tag{5}$$

Figures 2 and 3 show the chaos behavior of two different chaos sequences, which are generated by two different initial conditions, for example, with $\mu = 4$, $x_0 = 0.329999$, and $N = 2000$ and $\mu = 4$, $x_0 = 0.329998$, and $N = 2000$. We can see that the difference between the two waveforms of sequences is random. Figures 4 and 5 show the autocorrelation functions of the two chaos sequences, respectively. It can be seen that when lag $k \neq 0$ the value of the autocorrelation function of the chaos sequences is very small. Figure 6 shows the cross-correlation function of the chaos sequences for $x_0 = 0.329999$ and $x_0 = 0.329998$ and $N = 2000$. The values of cross-correlation functions are also around zero for all values of lag k. Therefore, the generated sequence by chaos mapping has very good random properties.

In our proposed scheme, the frequency information of OFDM signal is scrambled with chaos scrambling sequence to enhance the security of the physical layer of OFDM-based VLC. The scrambling sequence is generated from a Logistic mapping, in which the iteration parameters of Logistic mapping are used as security keys. Figure 7 illustrates the schematic of a DCT precoded OFDM-based visible light communications system with chaos scrambling sequence. The pseudorandom binary sequence (PRBS) information data is mapped into m-QAM data symbols and then goes through serial to parallel (S/P) transform. The generated

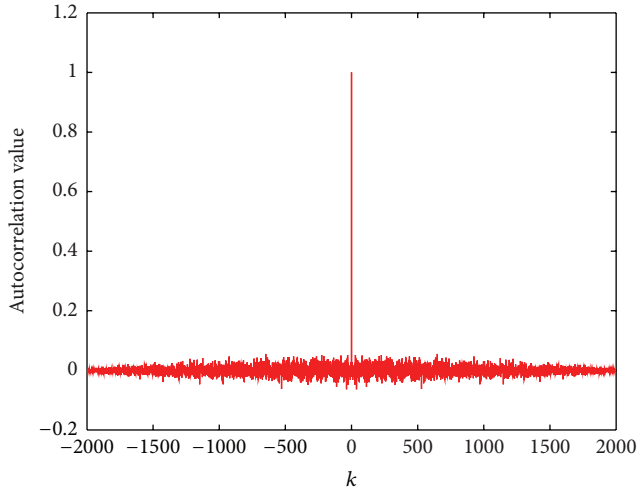

Figure 4: Autocorrelation of chaos sequence for $\mu = 4$, $x_0 = 0.329999$, and $N = 2000$.

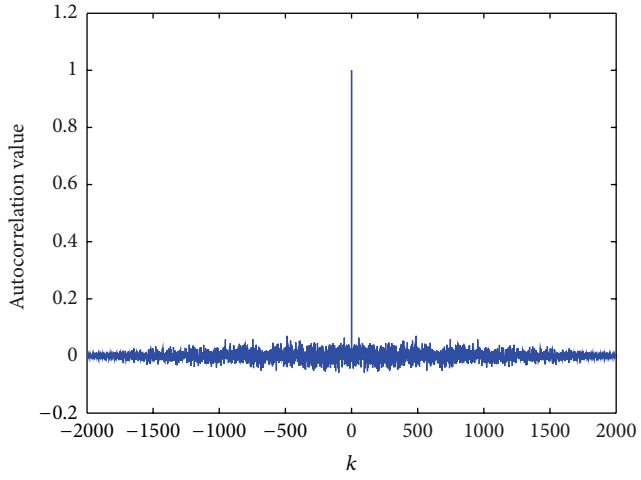

Figure 5: Autocorrelation of chaos sequence for $\mu = 4$, $x_0 = 0.329998$, and $N = 2000$.

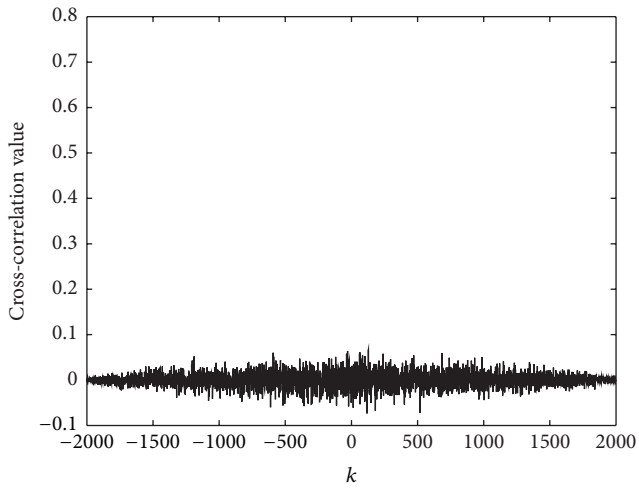

Figure 6: Cross-correlation of chaos sequences for $x_0 = 0.329998$ and $x_0 = 0.329999$, $\mu = 4$, and $N = 2000$.

complex vector of size M can be expressed as $S = [S(0)\ \ S(1)\ \ \cdots\ \ S(M-1)]^T$. After that the obtained m-QAM symbols are divided into I and Q parts. The encryption is performed by multiplying I and Q parts of the complex signal vector by a pair of chaos scrambling sequences separately according to (3).

The encrypted complex vector with size M can be written as $Z = [Z(0)\ \ Z(1)\ \ \cdots\ \ Z(M-1)]^T$. Then DCT precoding is applied to this complex vector which transforms this vector into new vector of length M that can be written as

$$Y = PZ = [Y(0)\ \ Y(1)\ \ \cdots\ \ Y(M-1)]^T, \tag{6}$$

where $[\,]^T$ denotes the matrix transpose and P is DCT matrix with $M \times M$ dimension. The DCT precoded matrix can be stated as follows:

$$P = \begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0(M-1)} \\ p_{10} & p_{11} & \cdots & p_{1(M-1)} \\ \vdots & \vdots & \ddots & \vdots \\ p_{(M-1)0} & p_{(M-1)1} & \cdots & p_{(M-1)(M-1)} \end{bmatrix}. \tag{7}$$

The DCT kernel is real and can be expressed as

$$P_{lm} = \begin{cases} \dfrac{1}{\sqrt{M}}, & l = 0,\ 0 \le m \le M-1, \\ \sqrt{\left(\dfrac{2}{M}\right)} \cos\left[\dfrac{(2m+1)\,l\pi}{2M}\right], & 1 \le l \le M-1,\ 0 \le m \le M-1, \end{cases} \tag{8}$$

where $l = 0, 1, \ldots, M-1$, $m = 0, 1, \ldots, M-1$ and p_{lm} means lth row and mth column of DCT precoding matrix.

In the receiver end, after FFT and equalization operation the inverse DCT precoding matrix is employed in receiver to recover the original data symbols. Assume that the chaotic map and secure key at the receiver are identical to those of the transmitter; they can provide sufficient information to generate identical chaotic scrambling sequences for decryption easily. Without knowledge of the secure key, the data cannot be recovered from the received signal by an eavesdropper.

In our proposed scheme, I and Q parts of QAM signal are both encrypted independently by chaos sequences. Therefore, there are two secret keys in our encryption algorithm. Every secret key of this chaos system contains three members, initial parameter x_0, control parameter μ, and iteration step N. By this, it can enhance secret key numbers and secret space. In our encrypted algorithm, the security keys can be expressed as $\{x_0^I, \mu^I, N^I, x_0^Q, \mu^Q, N^Q\}$, of which $\{x_0^I, \mu^I, N^I\}$ and $\{x_0^Q, \mu^Q, N^Q\}$ are the keys of I and Q parts of QAM signal, respectively.

The chaos state is highly sensitive to its initial values; only a slight change from the correct key value will fall into another absolute different chaotic state. This is beneficial for creating a huge key space which cannot be broken for illegal receiver. In our proposed system, there are four variables x_0^I, μ^I, x_0^Q, and μ^Q which are declared as Matlab type long. Every of the variables is scaled fixed point format with 15 digits precision for double. According to the IEEE floating-point standard [18], the computational precision of the 64-bit double-precision number is about 10^{-15}. After considering parameters involved, the key space size is approximately $10^{15\times4} \approx 2^{199}$, which is much larger than 2^{100}. Therefore, a sufficiently large key space is guaranteed in the proposed algorithm for application. The proposed encrypted scheme can efficiently resist the brute-force attack [19].

3. Simulation Results and Analysis

The chaos scrambling sequence is very import to ensure the security of the proposed encryption technique. In this work, we will evaluate the effect of scrambling sequence on the PAPR and BER performances of DCT precoded OFDM-VLC over multipath optical wireless channel by simulation. In the simulation setup, The OFDM frame structure has 192 data subcarriers and 8 pilot tones for channel estimation and equalization and 56 unused tones for the guard band. So the size of IFFT is 256. However, due to the Hermitian symmetry of input data of IFFT of DCO-OFDM systems, there are only 96 effective data subcarriers in OFDM frame. Therefore, the length of chaos scrambling sequence in the proposed scheme is set to 96. In the proposed encrypted scheme, the chaotic scrambling sequence can be generated based on Logistic map according to (1) and (2). In following simulation,

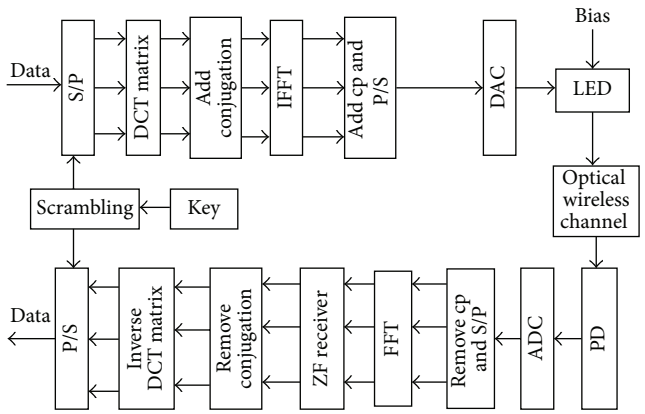

Figure 7: DCT precoded OFDM-based VLC system with encryption and decryption.

the security keys of I or Q part of QAM signal can be fixed at $\{0.329999, 4, 2000\}$ and $\{0.329998, 4, 2000\}$.

3.1. PAPR Performance. One major drawback of OFDM is the peak-to-average power ratio (PAPR). It is verified that DCT precoding can reduce the PAPR and improve the BER performance of OFDM systems. In our proposed scheme, chaos scrambling is employed to improve security of physical layer of DCT precoded OFDM-based VLC. It is noteworthy to mention that the proposed encryption only changes the sign of the real and image parts of the transmitted symbols. Thus, the PAPR of the DCT precoded OFDM is kept unaffected. Therefore we mainly evaluated the effect of the chaos scrambling on the PAPR of OFDM signals in terms of the complementary cumulative distribution function (CCDF). Figure 8 shows the CCDF comparison of the PAPR of the scrambled and DCT precoded OFDM with that of conventional DCT precoded OFDM. From Figure 8 we can also see that the CCDF curves of the two cases are close to each other. Thus, the influence of the proposed encrypted scheme on the PAPR is negligible.

3.2. BER Performance. In following simulation experiment, the ceiling-bounce model developed by Carruthers and Kahn in [20] is chosen as the optical wireless channel model. This model is the most practical model and accurately represents the multipath dispersion of an indoor wireless optical channel. A single infinite-plane reflector with Lambertian reflectance is assumed. The continuous impulse response of an optical wireless link $h(t)$ is defined as

$$h_c(t) = H(0)\frac{6a^6}{(t+a)^7}u(t), \quad (9)$$

where $H(0)$ is the channel DC gain, $u(t)$ is the step function, $a = 2H/c$, H is the ceiling height above the transmitter, and c is the velocity of light. The delay spread of a channel is a remarkably accurate predictor of ISI-induced signal-to-noise ratio (SNR) penalties, which is independent of the particular time dependence of the impulse response of that channel. This channel $h(n)$ was employed in the simulation.

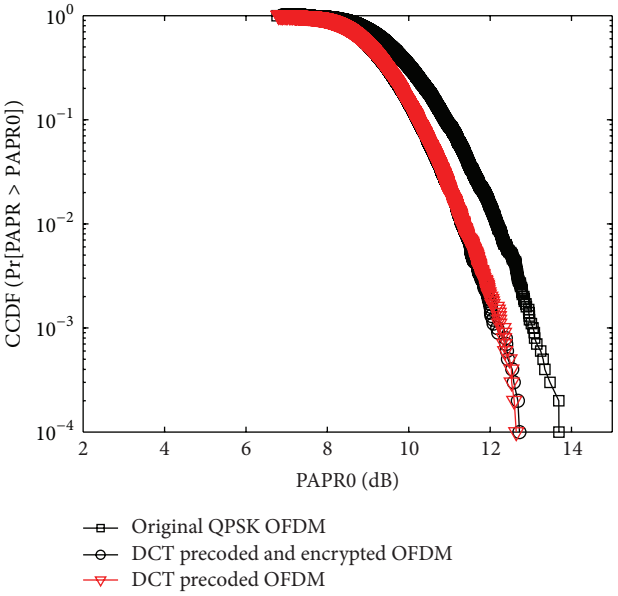

Figure 8: Comparison of the PAPRs of the precoded 16 QAM OFDM signals with and without chaos scrambling.

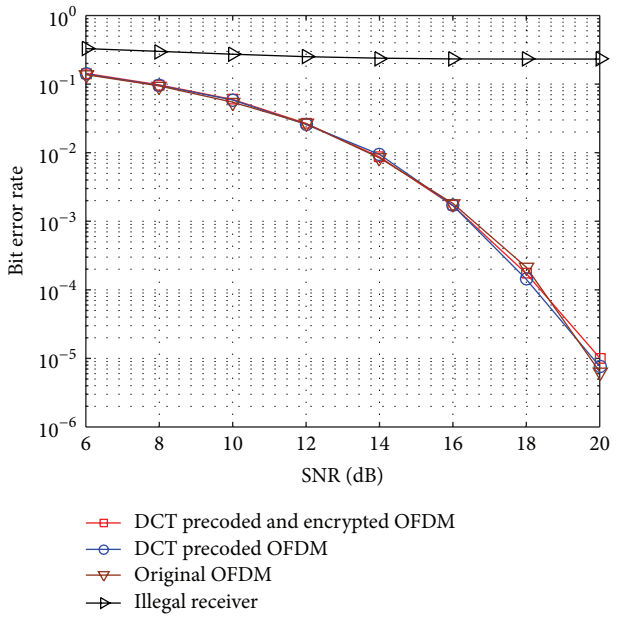

Figure 9: BER performance for AWGN channel.

The sample rate of the channel is represented by the symbol rate R_s. We mainly study the BER performance of DCT precoded 16 QAM OFDM-based system with and without chaos scrambling for AWGN and multipath optical wireless channel. In our simulation, the main parameters are shown in Table 1.

Figure 9 shows the BER performance demodulated by legitimate receiver and illegal receiver in the additive white Gaussian noise (AWGN) channel. The BER performance of the DCT precoded OFDM is almost the same as that of the conventional DCT precoded OFDM for the legitimate

Table 1: Simulation parameters.

R_s	125 M symbols/s
Modulation	16 QAM
FFT size	256
Number of pilot data	8
Length of CP	32
Scrambling size	96
H	3.5 m

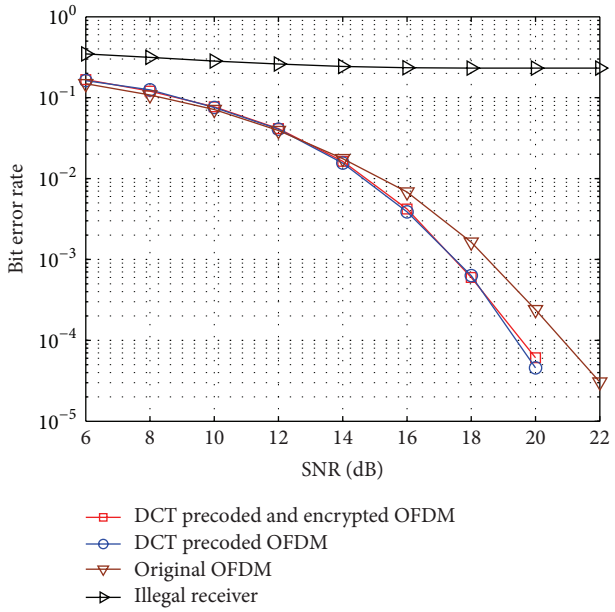

Figure 10: BER performance for multipath optical wireless channel.

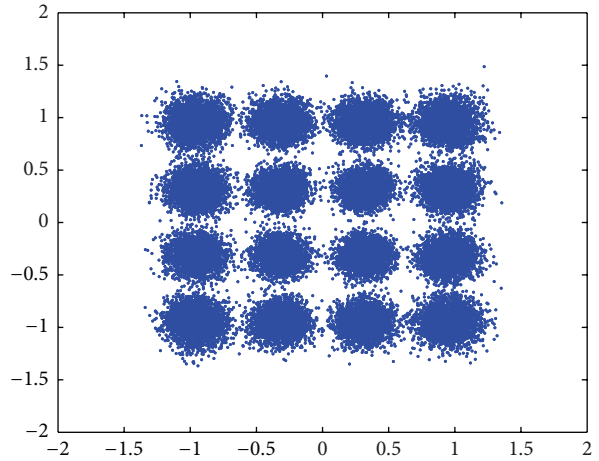

Figure 11: Received constellations of legitimate receiver for multipath optical wireless channel.

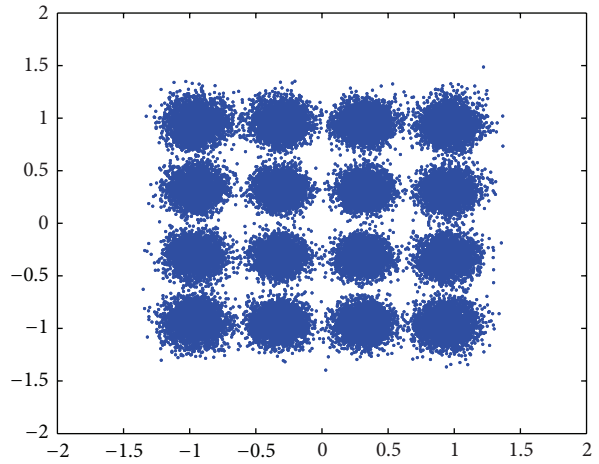

Figure 12: Received constellations of illegal receiver for multipath optical wireless channel.

receiver. Therefore, the encryption measure does not influence the BER performance of legal receiver. We also see that DCT precoding technique does not improve the BER of OFDM systems over AWGN channel. However, for the illegal receiver, the BER is around 0.5 because illegal receiver does not know the right secret key.

Figure 10 shows the BER performance comparison in a multipath VLC link. We can see that the BER performance of the encrypted and DCT precoded system is almost the same as that of the conventional DCT precoded system without encryption. For DCT precoded scheme with and without encryption, the improvement by DCT precoding can be clearly observed when the SNR is higher than 14 dB. At BER = 10^{-3}, the BER performance of the proposed DCT precoded system with chaos scrambling can be improved by an approximately 1 dB gain compared with that of the original OFDM system. The using of the chaos encryption maintains the advantage of DCT precoding technique, which can reduce the PAPR and improve the BER performance in OFDM systems. Form Figure 10, we can also see that illegal receiver cannot demodulate out the correct data if it does not know the right encryption keys. For the illegal receiver without right encryption keys, the BER is around 0.5. It is shown that the proposed scheme can enhance both the reliability and security of OFDM-based VLC data transmission.

From Figure 10, it can be seen that the improvement of BER performance of the proposed DCT precoded and encrypted system is due to obtaining frequency diversity by using DCT precoding. Furthermore, in order to further improve the BER performance of the proposed system, channel coding such as convolution code and turbo-codes can be employed.

Figures 11 and 12 show the received constellations of legitimate receiver and illegal receiver for 16 QAM DCT precoded and encrypted OFDM signals, of which the signal-to-noise ratio is 18 dB, respectively. The legitimate receiver adopts chaos scrambling encryption technique while the illegal receiver does not adopt chaos scrambling encryption. Though the illegal receiver can obtain the right constellation it cannot demodulate the transmitted information due to have not the right encryption key.

4. Conclusions

In this paper, a physical layer encryption method is proposed to effectively enhance the security of a DCT precoded OFDM-based VLC system, where Logistic map is adopted to generate chaos scrambling sequences. The experimental results show that the chaos scrambling sequences can lead to a successful confidential data transmission in physical layer. Meanwhile, the proposed scheme does not influence the PAPR and BER performances of DCT precoded OFDM-based VLC. The advantage of DCT precoding technique can remain.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported in part by the Open Fund of the State Key Laboratory of Millimeter Waves (Southeast University, Ministry of Education, China) under K201214 and by the Zhejiang Provincial Natural Science Foundation of China under LY13F050005.

References

[1] D. Karunatilaka, F. Zafar, V. Kalavally, and R. Parthiban, "LED based indoor visible light communications: state of the art," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1649–1678, 2015.

[2] Y. Wang, N. Chi, Y. Wang, L. Tao, and J. Shi, "Network architecture of a high-speed visible light communication local area network," *IEEE Photonics Technology Letters*, vol. 27, no. 2, pp. 197–200, 2015.

[3] C. Rohner, S. Raza, D. Puccinlli, and T. Voigt, "Security in visible light communication: novel challenges and opportunities," *Sensors & Transducers*, vol. 192, no. 9, pp. 9–15, 2015.

[4] J. Liu, W. Noonpakdee, and S. Shimamoto, "Design and performance evaluation of OFDM-based wireless services employing radio over optical wireless link," *International Journal of Wireless & Mobile Networks*, vol. 3, no. 5, pp. 173–184, 2011.

[5] J. Tan, Z. Wang, Q. Wang, and L. Dai, "Near-optimal low-complexity sequence detection for clipped DCO-OFDM," *IEEE Photonics Technology Letters*, vol. 28, no. 3, pp. 233–236, 2016.

[6] B. Ranjha and M. Kavehrad, "Precoding techniques for PAPR reduction in asymmetrically clipped OFDM based optical wireless system," in *Broadband Access Communication Technologies VII, 86450R*, Proceedings of SPIE, International Society for Optics and Photonics, January 2013.

[7] L. Tao, J. Yu, Y. Fang, J. Zhang, Y. Shao, and N. Chi, "Analysis of noise spread in optical DFT-S OFDM systems," *Journal of Lightwave Technology*, vol. 30, no. 20, Article ID 6298919, pp. 3288–3294, 2012.

[8] T. Allen and N. Al-Dhahir, "Performance analysis of a secure STBC with coherent and differential detection," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '15)*, pp. 522–527, IEEE, New Orleans, La, USA, March 2015.

[9] F. Huo and G. Gong, "A new efficient physical layer OFDM encryption scheme," in *Proceedings of the 33rd IEEE Conference on Computer Communications (IEEE INFOCOM '14)*, pp. 1024–1032, Toronto, Canada, May 2014.

[10] B. Liu, L. Zhang, X. Xin, and J. Yu, "Physical layer security in CO-OFDM transmission system using chaotic scrambling," *Optics Communications*, vol. 291, pp. 79–86, 2013.

[11] L. Deng, M. Cheng, X. Wang et al., "Secure OFDM-PON system based on chaos and fractional fourier transform techniques," *Journal of Lightwave Technology*, vol. 32, no. 15, pp. 2629–2635, 2014.

[12] W. Zhang, C. Zhang, W. Jin, C. Chen, N. Jiang, and K. Qiu, "Chaos coding-based QAM IQ-encryption for improved security in OFDMA-PON," *IEEE Photonics Technology Letters*, vol. 26, no. 19, pp. 1964–1967, 2014.

[13] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proceedings of the 1st IEEE International Conference on Communications (ICC '14)*, pp. 3342–3347, Sydney, Australia, June 2014.

[14] H. Le Minh, A. T. Pham, Z. Ghassemlooy, and A. Burton, "Secured communications-zone multiple input multiple output visible light communications," in *Proceedings of the IEEE Globecom Workshops*, pp. 505–511, Austin, Tex, USA, December 2014.

[15] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: secure barcode-based visible light communication for smartphones," in *Proceedings of the 33rd IEEE Conference on Computer Communications (IEEE INFOCOM '14)*, pp. 2661–2669, IEEE, Toronto, Canada, May 2014.

[16] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806–1818, 2015.

[17] S.-L. Chen, T. T. Hwang, and W.-W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 12, pp. 996–1000, 2010.

[18] IEEE Computer Society, *IEEE Standard for Binary Floating-Point Arithmetic*, ANSI/IEEE Standards 1985-754, 1985.

[19] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 16, no. 8, pp. 2129–2151, 2006.

[20] J. B. Carruthers and J. M. Kahn, "Modeling of nondirected wireless infrared channels," *IEEE Transactions on Communications*, vol. 45, no. 10, pp. 1260–1268, 1997.