

Research Article

Joint Encryption Scheme Based on the Chaotic DCT Matrix and SLM Algorithm in an OFDM-PON System

Shuai Zhang , Liqun Huang, and Mingxu Zhu

Northeastern University at Qinhuangdao, Qinhuangdao, Hebei 066004, China

Correspondence should be addressed to Shuai Zhang; zhangs@stumail.neu.edu.cn

Received 23 September 2020; Revised 18 December 2020; Accepted 26 December 2020; Published 11 January 2021

Academic Editor: Ding Xu

Copyright © 2021 Shuai Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In order to effectively solve the problem of data transmission security and peak-to-average ratio (PAPR) in an orthogonal frequency division multiplexing passive optical network (OFDM-PON) transmission system, in this paper, a joint encryption scheme of discrete cosine transform (DCT) and selective mapping (SLM) based on chaotic mapping is proposed. In this scheme, the chaotic sequence of a 3D Lorenz chaotic system is used as the row and column index of the DCT matrix and the phase factor of SLM to resist selective plaintext attack, and the system encryption is realized while reducing PAPR. The theoretical analysis and numerical simulation show that the common OFDM-PON, the proposed algorithm, can obtain a PAPR suppression gain of ~4.8 dB and improve the receiver sensitivity by ~4 dB ($\text{BER}@10^{-3}$). In addition, it shows that, with the increase of row/column index mismatch of the DCT matrix, the bit error rate of the system increases gradually. An encrypted data transmission of 8 GB/s 16-QAM optical OFDM signals is successfully simulated over a 20 km standard single-mode fiber, which proves the excellent confidentiality of the proposed secure transmission.

1. Introduction

Orthogonal frequency division multiplexing passive optical network (OFDM-PON) technology has the advantages of strong antifiber dispersion, low cost, and high spectrum utilization, which has caused great concern in next-generation optical networks [1–4]. However, because of the broadcast nature of the PON system, data are highly vulnerable to illegal theft during transmission [5]. At the same time, excessive PAPR in the OFDM-PON system will aggravate the damage of optical components and worsen the system performance. Therefore, how to guarantee data security and suppress PAPR is a challenge for the current OFDM-PON system [6, 7].

At present, many methods based on chaotic systems have been proposed to enhance the security of the physical layer of the OFDM-PON system and reduce the PAPR. For example, chaotic sequences are used as the phase factors of selective mapping (SLM) and partial transmission sequence (PTS) to realize data encryption and reduce PAPR [8, 9]. Chaotic sequences generate random interleavers and phase

sequences to scramble OFDM signals [10]. However, the probabilistic methods mentioned above require additional sideband information and bring higher computational complexity with the increase of the number of chaotic sequences required. Different from the abovementioned scheme, the Walsh–Hadamard (WHT) matrix [11], Discrete Hartley Transform matrix (DHT) [12], constant envelope zero autocorrelation (CAZAC) matrix [13], Discrete Fourier transform (DFT) matrix [14], and improved discrete Fourier transform matrix [15] achieve system encryption and reduce PAPR. In addition, the computational complexity of the algorithm is relatively low. However, due to the single encryption method, the encryption level is not very high, and it may be more effective if combined with other encryption methods. There are other schemes, such as encrypting the QAM symbols by separating the virtual and real parts [16], using constellation expansion and chaotic signal interleaving to obtain a large key space and improve system security [17]. In the recently proposed clipping noise compression (CNC) method, a preset normalization factor is introduced to replace the calculation of the average amplitude of clipping

noise in the compression process with the original CNC method to reduce PAPR [18]. A low-complexity PAPR reduction scheme combines multiband- (MB-) Hadamard precoding and clipping for the optical OFDM system [19]. However, these methods only consider the encryption effect or PAPR reduction, and some encryption methods are relatively simple, without combining multiple algorithms to further consider data security and PAPR reduction.

Aiming at the security of the OFDM-PON transmission system and the performance loss caused by high PAPR, this paper proposes a joint encryption algorithm of the DCT matrix and SLM based on chaotic mapping. The algorithm firstly uses the chaotic sequences as the key to perform row-column replacement on the DCT matrix and then uses the sequences to select the phase sequence of the SLM. The numerical simulation results show that compared with the original OFDM signal and the traditional SLM, the double-encrypted signal can obtain PAPR suppression gains of ~ 4.8 dB and ~ 0.8 dB, respectively. Among them, the dual encryption system creates a huge key space of $\sim 6.34 \times 10^{293}$, which has a good ability to resist selective plaintext attack, and well guarantees the antiattack ability of the transmission system. At the same time, an encrypted data transmission of 8 GB/s 16-QAM optical OFDM signals is successfully simulated over 20 km standard single-mode fiber, which proves the excellent confidentiality of the proposed secure transmission.

The rest of this article is arranged as follows. Section 2 presents the block diagram of the OFDM system encryption principle used in the analysis and simulation in this paper. In Section 3, the principle of PAPR is introduced and the theoretical verification and analysis of the proposed method are carried out. Section 4 presents the results and discusses them. Section 5 gives the conclusion.

2. System Model

The principle of DCT-SLM algorithm implemented in the OFDM-PON system for data encryption is shown in Figure 1. The pseudorandom binary sequence (PRBS) is serial-to-parallel (S/P) transformed, and the sequences after QAM (Quadrature Amplitude Modulation) mapping are sent to the encryption module for data encryption. After the chaotic DCT matrix and the SLM encrypted signals, the sequences with the smallest PAPR value are selected for transmission in the optical channel. At the sending end, the encryption algorithm is mainly divided into two parts. First, the chaotic sequence after double preprocessing will be used as the index value of the specific row/column permutation of the DCT matrix to implement the first encryption. Secondly, the signal transformed by the DCT matrix is multiplied by the corresponding chaotic phase factor to achieve the second encryption, thereby enhancing the security performance of the transmission system.

3. Description and Analysis of the Proposed Method

3.1. Description of PAPR. The PAPR value of each symbol of an OFDM signal is defined as

$$\text{PAPR} = \frac{\max(|s(t)|^2)}{E\{|s(t)|^2\}}, \quad (1)$$

where $E\{\cdot\}$ is a mathematical expectation operator And $s(t)$ is the discrete time-domain signal. If the amplitudes of all subcarriers are normalized, then $E\{|s(t)|^2\} = N$. Therefore,

$$\text{PAPR} = \frac{\max(|s(t)|^2)}{N}, \quad (2)$$

where N is the number of system subcarriers. Among them,

$$\begin{aligned} |s(t)|^2 &= s(t) \cdot s^*(t) = \sum_{k=0}^{N-1} y_k e^{j2\pi k(t/T)} \cdot \sum_{m=0}^{N-1} y_m^* e^{-j2\pi m(t/T)}, \\ &= \sum_{n=-(N-1)}^{N-1} C_Y(n) e^{-j2\pi n(t/T)}, \\ &= N + 2\Re \left\{ \sum_{n=1}^{N-1} C_Y(n) e^{-j2\pi n(t/T)} \right\}. \end{aligned} \quad (3)$$

In (3), T is the OFDM symbol length, $\Re\{\cdot\}$ is the operation of taking the real part, and $C_Y(n)$ is the nonperiodic autocorrelation function of the matrix transformed sequence, which is defined as

$$C_Y(n) = \begin{cases} \sum_{k=0}^{N-1-n} y_k y_{k+n}^*, & 0 \leq n \leq N-1, \\ \sum_{k=0}^{N-1+n} y_{k-n} y_k^*, & -(N-1) \leq n \leq -1. \end{cases} \quad (4)$$

From the definition of the aperiodic autocorrelation function, we can get $C_Y(n) = C_Y^*(-n)$.

$$\text{PAPR} = \frac{\max(|s(t)|^2)}{N} \leq 1 + \frac{2}{N} \sum_{n=1}^{N-1} |C_Y(n)|. \quad (5)$$

Therefore, the PAPR value of the OFDM signals has a certain relationship with the nonperiodic autocorrelation function of the input sequence before IFFT. The peak value of the nonperiodic autocorrelation function is the average energy of the input sequence. If the system subcarrier does not change, the peak value depends only on the input sequence. Therefore, the smaller the aperiodic autocorrelation function of the input sequence before IFFT, the smaller the PAPR value of the signals.

A more effective definition method is to describe the PAPR properties of the signals using the complementary

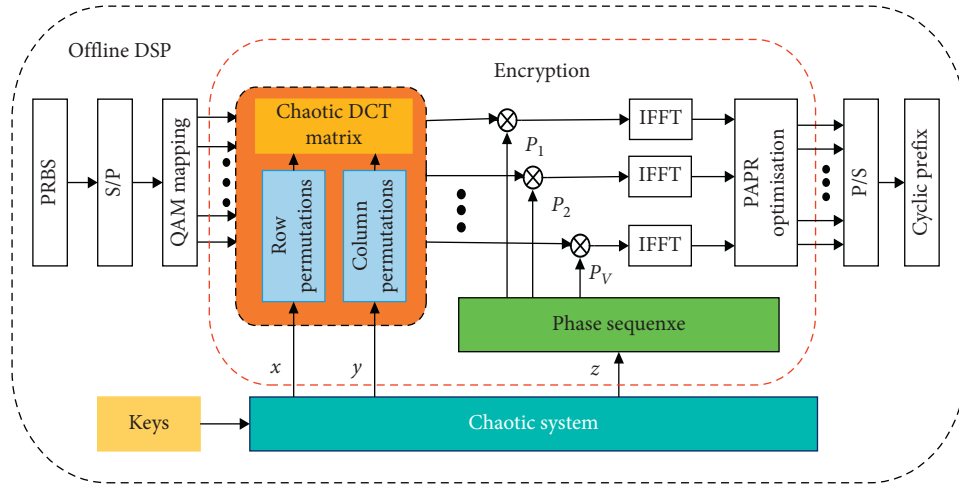


FIGURE 1: Schematic diagram of the double-encryption system based on DCT-SLM algorithm.

cumulative distribution function (CCDF) from the probabilistic perspective [20]. The CCDF of PAPR is defined as

$$\text{CCDF}_{\text{PAPR}} = \text{prob}(\text{PAPR} > \text{PAPR}_t), \quad (6)$$

where PAPR_t is the reference level and $\text{prob}(\cdot)$ is the probability operator.

3.2. The Proposed Method. In this paper, the DCT-SLM algorithm is encrypted using the chaotic sequence generated by the 3D Lorenz chaotic system. The iterative expression is shown as follows [21]:

$$\begin{cases} \dot{x} = -a(x - y), \\ \dot{y} = -xz + rz - y, \\ \dot{z} = xy - bz, \end{cases} \quad (7)$$

where a , b , and r are the parameters of the hyperchaotic system. When $a = 10$, $b = 8/3$, $r = 28$, the system is in the hyperchaotic state, and the generated chaotic sequence shows good randomness. We set the initial value of the hyperchaotic system to $x_0 = 5.25$, $y_0 = 1.24$, $z_0 = 0.5$ and use MATLAB for numerical simulation. The Runge–Kutta method step is set to $h = 0.02$. After several iterations, three sets of chaotic sequence values are generated: $\{x_n\}$, $\{y_n\}$, and $\{z_n\}$, where $\{x_n\}$ and $\{y_n\}$ are used for DCT matrix row and column permutation encryption and $\{z_n\}$ will be used to construct the phase factor of the SLM method. However, each chaotic sequence needs to be preprocessed. The specific process is shown as follows [22]:

$$D_{x,i} = \text{mod}(\text{Extract}(x, m, n, w, v), N), \quad (8)$$

where $\text{Extract}(x, m, n, w, v)$ returns a random integer consisting of the m^{th} , n^{th} , w^{th} , and v^{th} digits of the fractional part of the chaotic sequence value $\{x_n\}$. The values of m , n , w , and v range from 1 to 15. $\text{mod}(f, N)$ returns the integer that f is the remainder of N , and N indicates the number of sub-carriers. Then, each random integer between 0 and $N - 1$ is

used as the encryption key. After the first preprocessing, $\{x_n\}$ and $\{y_n\}$ are also sorted, and then, the position is indexed for DCT matrix encryption. The specific operation method is as shown as follows:

$$\begin{aligned} D_{x,i} &= \text{sort}(x), \\ D_{y,i} &= \text{sort}(y), \end{aligned} \quad (9)$$

where the sort function defaults to returning the index value in ascending order.

The DCT matrix can be represented by [23]

$$C(m, n) = \begin{cases} \frac{1}{\sqrt{N}}, & m = 1, \\ \frac{\sqrt{2}}{\sqrt{N}} \cos \frac{(m-1)(2n-1)\pi}{2N}, & \\ m = 2, \dots, N, \end{cases} \quad (10)$$

where m is the row number of the matrix; $n = 1, 2, \dots, N$ is the column number of the matrix; and N is the size of the matrix. The DCT matrix is also an orthogonal matrix, $CC^T = C^TC = NI$, and T is the transpose of the matrix.

In this paper, we assume that the standard DCT matrix is represented by $C_{N \times N}^{(0)}$:

$$C_{N \times N}^{(0)} = [\phi(1); \phi(2); \dots; \phi(N)], \quad (11)$$

where $\phi(1); \phi(2); \dots; \phi(N)$ represents the row vector of matrix C . The matrix after the row permutation with the digital chaotic $D_{x,n}$ can be expressed as

$$C_{N \times N}^{(1)} = [\phi(D_{x,n}(1)); \phi(D_{x,n}(2)); \dots; \phi(D_{x,n}(N))], \quad (12)$$

and similarly, by column permutation by $D_{y,n}$, the matrix after row and column permutation is as follows:

$$C_{N \times N}^{(2)} = [\phi(D_{y,n}(1)); \phi(D_{y,n}(2)); \dots; \phi(D_{y,n}(N))]. \quad (13)$$

Assuming that P and Q are the row and column permutation matrices on the DCT matrix, respectively, the DCT matrix after chaotic row and column permutation has the following properties:

$$\begin{aligned} C^{(1)} &= PC, \\ C^{(2)} &= PCQ, \\ C^{(2)T} &= Q^T C^T P^T, \end{aligned} \quad (14)$$

$$C^{(2)} C^{(2)T} = PC(QQ^T)C^T P^T = PCIC^T P^T = NI. \quad (15)$$

It can be seen from (15) that the encrypted DCT matrix also has orthogonality, which means that we can decrypt by multiplying its orthogonal matrix.

It is assumed that the signals processed by DCT matrix encryption can be expressed as $\beta = [\beta_0, \beta_1, \dots, \beta_{N-1}]$, where β_k represents the k^{th} subcarrier and N indicates that the length of the phase sequences is also the number of subcarriers. In order to implement chaotic SLM encryption, we assume that there are V different random phase sequences and the chaotic sequence $D_{z,n}$ is used to generate all phase sequences P_v .

$$P_v = [P_{v,0}, P_{v,1}, \dots, P_{v,N-1}], \quad (1 \leq v \leq V), \quad (16)$$

where $P_{v,k}$ is represented by

$$P_{v,k} = \exp^{j2\pi D_{z,k} I^N}, \quad (0 \leq k \leq N-1), \quad (17)$$

and after the sequence β is multiplied by the phase sequences P_v , the secondary encryption of the DCT-SLM algorithm is completed. The encrypted signal λ_v is

$$\lambda_v = \beta \otimes P_v = [\beta_0 P_{v,0}, \beta_1 P_{v,1}, \dots, \beta_{N-1} P_{v,N-1}], \quad (18)$$

where \otimes denotes the component-wise vector multiplication.

Figures 2(a) and 2(b) are autocorrelation and cross-correlation curves of chaotic sequences, respectively. Among them, the autocorrelation function of the chaotic sequences approximates the δ function, the cross-correlation value is very small, and the overall distribution is zero, indicating that the correlation of the chaotic sequences is low. The correlation of candidate signals in the SLM algorithm depends largely on the correlation of the phase sequences. The lower the correlation, the better the suppression effect of PAPR.

On the basis of the property of sensitive dependence on initial conditions, only a minor deviation from the original value will transform the chaos into another significantly different status. Figure 3 shows that the initial value has only a slight change (1×10^{-15}), which also gets different chaotic sequences. Therefore, the chaotic sequences generated by (7) are suitable for encryption of the OFDM-PON system and protect legitimate users from being attacked.

4. Simulation Results and Discussion

4.1. Simulation Results of PAPR. The number of simulated OFDM symbols is 10^4 , the modulation mode is 16-QAM, and the number of subcarriers is 64. Figure 4 shows the PAPR suppression based on the number of random phase sequences (V) between the original SLM and the chaotic SLM algorithm. It can be seen that both the original SLM and the encrypted SLM have obvious a PAPR suppression effect, and the effect is roughly the same. Therefore, compared with the original SLM, the chaotic encrypted SLM only plays the role of encryption and does not affect the effect of PAPR. In addition, with the increase of V , the PAPR suppression effect of the system is also better (in this article, V is 8).

As can be seen from Figure 5, at $\text{CCDF} = 10^{-4}$, the encrypted DCT matrix and original DCT matrix have a nearly identical effect on PAPR suppression. The encrypted SLM is also roughly the same as the original SLM. In other words, compared with the original algorithm, the single chaotic encryption algorithm only plays the role of encryption. However, in addition to the encryption effect of the joint encryption algorithm mentioned in this article, PAPR also has a good reduction effect. Compared with the original OFDM signal, DCT matrix, and SLM method, the joint encryption scheme can improve the PAPR suppression performance by ~ 4.8 dB, ~ 2.6 dB, and ~ 0.8 dB, respectively.

Figure 6 shows the PAPR reduction of the SLM algorithm and other precoding matrices. It can be seen that, among many matrix algorithms, the WHT matrix has the worst effect of reducing PAPR, only about 1 dB; the effect of CAZAC, DFT, and DCT in reducing PAPR is basically the same, about 2.2 dB. In addition, compared to the precoding matrix algorithm alone, the SLM algorithm has the most obvious suppression of PAPR. In order to better compare the effect of combining various precoding matrices with SLM algorithm to reduce PAPR, it can be seen from Figure 7 that when various preprocessing matrices are combined with the SLM algorithm, the DCT-SLM algorithm has the best PAPR reduction effect of about 4.8 dB. The remaining preprocessing matrix combined with the SLM algorithm cannot achieve the effect of further reducing the PAPR, which is roughly the same as the effect of the SLM algorithm alone.

4.2. Simulation Results of Encryption. In order to discuss the security performance of the joint encryption scheme, we analyzed the bit error rate of the system when the row and column index values of the chaotic DCT matrix do not match. Among them, 128-IFFT point is applied, of which 64 subcarriers are used to load the 16-QAM mapped data and another 64 subcarriers load corresponding complex conjugate data to meet the requirement of Hermitian symmetry, thereby achieving the real output data. The cyclic prefix (CP) of 1/8 OFDM symbol length is added to each OFDM symbol. All the mentioned procedures are performed offline by

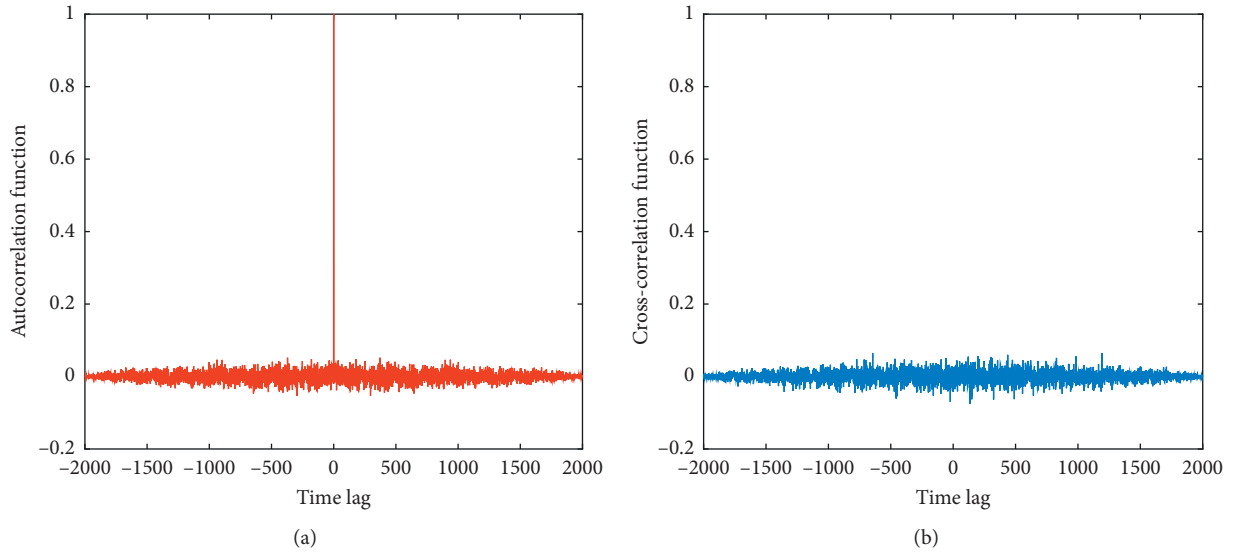


FIGURE 2: Properties of the 3D Lorenz chaotic system. (a) Autocorrelation function. (b) Cross-correlation function.

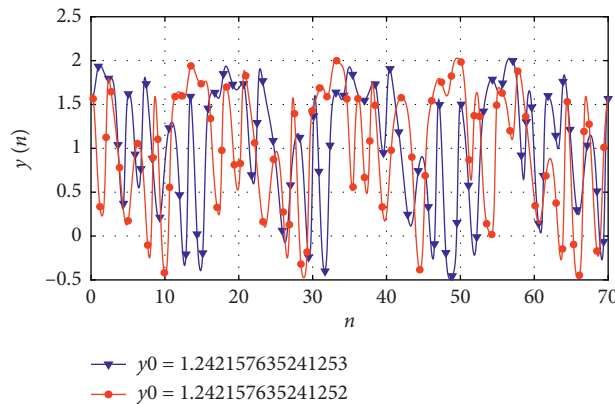


FIGURE 3: Chaotic sequences under tiny change of the initial value.

MATLAB programs. Then, the encrypted OFDM signals are loaded into Optisystem software for transmission. As shown in Figure 8, as the number of row and column index mismatches increases, the system’s bit error rate increases significantly, where the received optical power is set to -9 dBm. Also, we can also see from the constellation diagram of the system that when the number of mismatches is 0, the constellation diagram is restored normally. When the number of mismatches is 1, the constellation diagram has begun to show slight deflection and divergence. When the number of mismatches is 9, the system’s constellation is very confused and unrecognizable. According to the above-mentioned analysis, after the row and column permutation encryption is performed on the DCT matrix, PAPR suppression is achieved, and the security performance of the system is also increased.

Figure 9 is a plot of the bit error rate (BER) and constellation diagram for the different received optical powers of double-encrypted signals, original signals, and the illegal

ONU under an optical transmission of 20 km and back-to-back (B2B) conditions. When the BER is 10^{-3} , in the case of B2B transmission, compared with the original SLM and the original OFDM signals, the receiving sensitivity of the double-encryption scheme can be improved by ~ 1 dB and ~ 3 dB, respectively; In the case of 20 km SSMF transmission, the receiving sensitivity of the proposed scheme can be increased by ~ 1.7 dB and ~ 4 dB, respectively. In the case of illegal OUN, the BER under each received optical power is almost stable at around 0.5, which shows that the correct transmission data cannot be stolen at all. At the same time, when the received optical power is -9 dBm, the data constellation received by the illegal ONU is almost unrecognizable, which further proves that the double-encryption system has strong confidentiality and feasibility and can successfully resist illegal users from stealing data.

The comparative analysis on key space, complexity, and PAPR improvement with the existing schemes is listed in Table 1. For the WHT matrix scheme, since its own elements

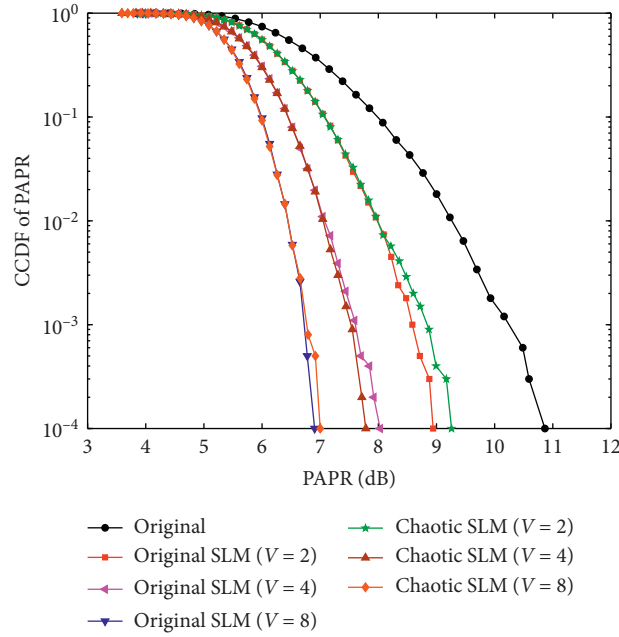


FIGURE 4: CCDF of PAPR for different number of random phase sequences in the SLM system.

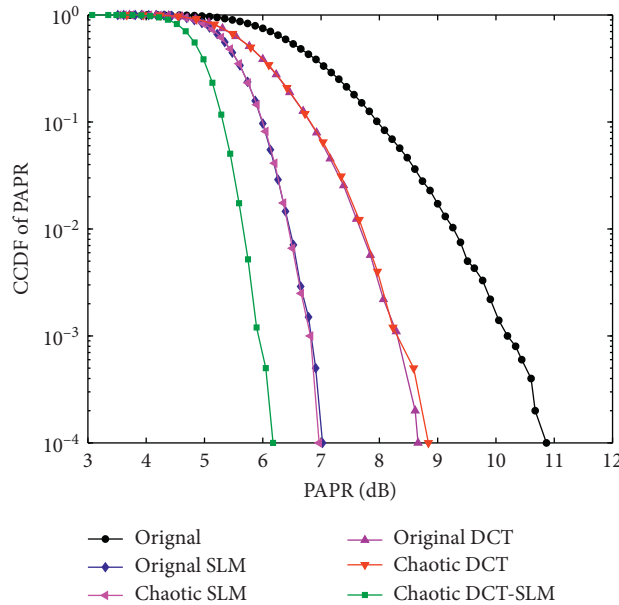


FIGURE 5: Comparison of PAPR between the proposed joint encryption scheme and single encryption scheme.

are selected between $[-1, 1]$, the calculation complexity of the row and column permutation of the matrix is very low, but the reduction of PAPR is very small. The CAZAC matrix scheme only needs bit replacement, XOR operation, extraction operation, and a small amount of matrix multiplication, so the proposed scheme also has medium computational complexity. But, the reduction effect of PAPR is not the best. For the DFT scheme, the computational complexity is very high due to the introduction of chaotic subcarrier allocation. In addition, if two real constants are tested exhaustively, the DFT matrix will be destroyed and the

security of the system will be greatly reduced. Compared with the abovementioned solution of the preprocessing matrix, in the double-encryption algorithm we proposed, because the calculation complexity of the row and column permutation of the DCT matrix is very low, the calculation complexity of the entire algorithm is concentrated on the IFFT calculation inside the SLM, and the computational complexity after the combination also belongs to the relationship of addition, not multiplication. Therefore, the computational complexity will increase based on the DCT matrix, but it has a very obvious effect on reducing PAPR.

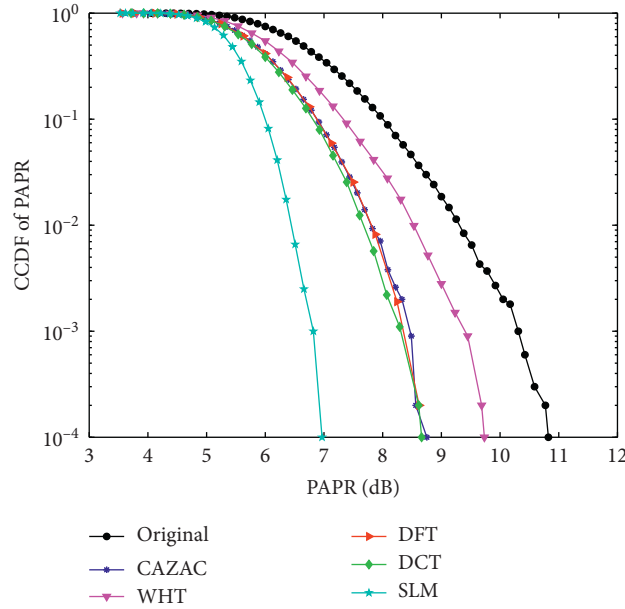


FIGURE 6: PAPR comparison between the SLM algorithm and preprocessing matrix scheme.

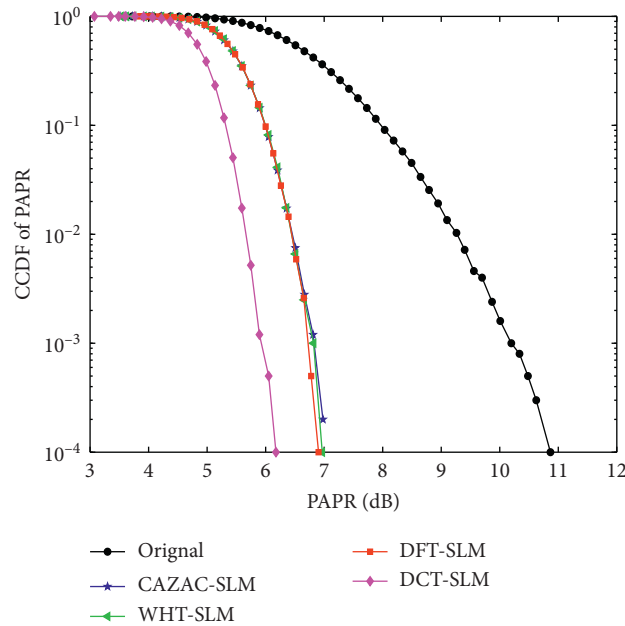


FIGURE 7: PAPR comparison between the preprocessing matrix and SLM algorithm combination.

The double-encryption scheme of the DCT matrix and the SLM algorithm can complement each other in encryption methods, further promote PAPR suppression, and provide a very large secret key space to guarantee the secure OFDM-PON data transmission.

The ability to defend against theft by illegal users depends on the size of the key space of the encryption system. The key space of the double-encryption algorithm is mainly determined by the order of the DCT matrix and the phase

factor of the SLM algorithm. Among them, the order of the DCT matrix is 64, which can create a key space of $64! \times 64!$ ($\sim 1.61 \times 10^{178}$), and the number of phase factors of the SLM can also provide a key space of about 64^{64} ($\sim 3.94 \times 10^{115}$). Therefore, the total key space of the double-encryption system is $\sim 6.34 \times 10^{293}$. The current calculation speed is $\sim 3.38 \times 10^{17} \text{ s}^{-1}$ [10], and it takes $\sim 5.95 \times 10^{268}$ years to obtain the transmission data of the system through an endless brute force experiment.

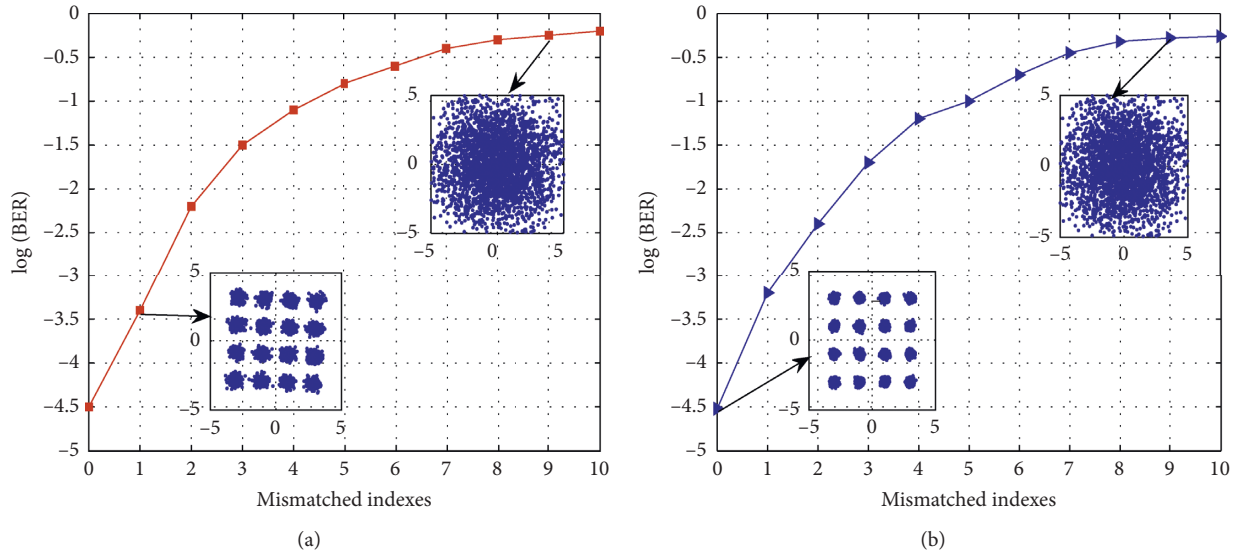


FIGURE 8: BERs versus the row and column index mismatches in the chaotic DCT matrix. (a) Row index mismatches. (b) Column index mismatches.

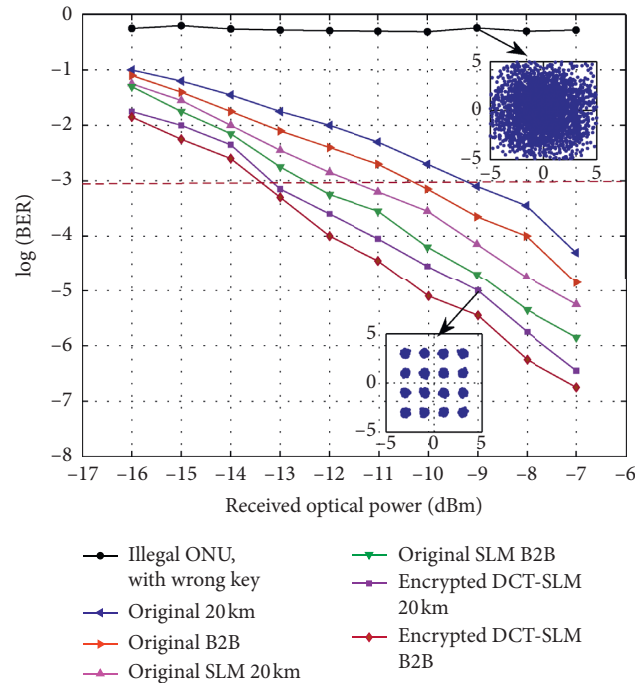


FIGURE 9: BER curve and constellation diagram of the double-encrypted signal and original signal.

TABLE 1: The comparative analysis among our scheme and other preprocessing matrix schemes.

Scheme	Complexity	PAPR reduction	Key space
WHT [11]	L	~1 dB	$\sim 10^{179}$
CAZAC [13]	M	~2.8 dB	$\sim 10^{166}$
DFT [14]	H	~2.6 dB	$\sim 10^{45}$
Our	H	~4.8 dB	$\sim 10^{293}$

WHT: Walsh–Hadamard transform; CAZAC: constant envelope zero autocorrelation; DFT: discrete Fourier transform; L: low; H: high; M: medium.

5. Conclusions

In this paper, a double-chaotic encryption algorithm combining a DCT matrix and SLM is proposed to enhance the physical layer security in OFDM-PON. The encrypted DCT matrix and SLM algorithm enhance the security of the system, while reducing the PAPR, further demonstrating the high confidentiality of the double-encryption algorithm. The simulation results show that, for the original optical OFDM signals, the algorithm can obtain a PAPR suppression gain of ~ 48 dB (@CCDF of 10^{-4}) and increase the receiving sensitivity of ~ 4 dB (BER@ 10^{-3}). Therefore, the scheme can be applied in a next-generation OFDM-PON system for improving system security and system performance.

Data Availability

Some or all data, models, and codes generated or used during the study are available in a repository.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] S. B. Wu, L. Tang, and M. H. Chen, "OFDM-PON technology and its applications," *Optical Communications*, vol. 38, pp. 31–34, 2012.
- [2] J. Kani, M. Teshima, K. Akimoto et al., "A WDM-based optical access network for wide-area gigabit access services," *IEEE Communications Magazine*, vol. 41, no. 2, pp. 43–48, 2003.
- [3] Y. Fang, J. Yu, J. Zhang, N. Chi, J. Xiao, and G.-K. Chang, "Ultrahigh-capacity access network architecture for mobile data backhaul using integrated W-band wireless and free-space optical links with OAM multiplexing," *Optics Letters*, vol. 39, no. 14, pp. 4168–4171, 2014.
- [4] N. Cvijetic, "OFDM for next-generation optical access networks," *Journal of Lightwave Technology*, vol. 30, no. 4, pp. 384–398, 2012.
- [5] A. W. Azim, Y. Le Guennec, and G. Maury, "Decision-directed iterative methods for PAPR reduction in optical wireless OFDM systems," *Optics Communications*, vol. 389, pp. 318–330, 2017.
- [6] W. O. Popoola, Z. Ghassemlooy, and B. G. Stewart, "Pilot-assisted PAPR reduction technique for optical OFDM communication systems," *Journal of Lightwave Technology*, vol. 32, no. 7, pp. 1374–1382, 2014.
- [7] M. Cheng, L. Deng, X. Gao et al., "Security-enhanced OFDM-PON using hybrid chaotic system," *IEEE Photonics Technology Letters*, vol. 27, no. 3, pp. 326–329, 2015.
- [8] X. Hu, X. Yang, and W. Hu, "Chaos-based selected mapping scheme for physical layer security in OFDM-PON," *Electronics Letters*, vol. 51, no. 18, pp. 1429–1431, 2015.
- [9] X. Hu, X. Yang, Z. Shen, H. He, W. Hu, and C. Bai, "Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON," *IEEE Photonics Technology Letters*, vol. 27, no. 23, pp. 2429–2432, 2015.
- [10] M. X. Han, Y. T. Wu, and Q. W. Zhang, "Secure algorithm for suppressing peak-to-average power ratio in OFDM-PON systems," *Acta Optica Sinica*, vol. 39, no. 5, Article ID 0506004, 2019.
- [11] A. A. E. Hajomer, X. Yang, and W. Hu, "Chaotic walsh-hadamard transform for physical layer security in OFDM-PON," *IEEE Photonics Technology Letters*, vol. 29, no. 6, pp. 527–530, 2017.
- [12] A. A. E. Hajomer, X. L. Yang, and W. S. Hu, "Secure OFDM transmission precoded by chaotic discrete Hartley transform," *IEEE Photonics Journal*, vol. 10, no. 2, p. 7901209, 2018.
- [13] M. Bi, X. Fu, X. Zhou, X. Yang, S. Xiao, and W. Hu, "Chaotic nonlinear encryption scheme for CPAs resistance and PAPR reduction in OFDM-PON," *IEEE Photonics Technology Letters*, vol. 29, no. 24, pp. 2147–2150, 2017.
- [14] Z. W. Shen, X. L. Yang, H. He, and W. S. Hu, "Secure transmission of optical DFT-S-OFDM data encrypted by digital chaos," *IEEE Photonics Journal*, vol. 8, no. 3, p. 7904609, 2016.
- [15] X. Fu, M. Bi, X. Zhou et al., "A chaotic modified-DFT encryption scheme for physical layer security and PAPR reduction in OFDM-PON," *Optical Fiber Technology*, vol. 42, pp. 126–131, 2018.
- [16] 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.
- [17] J. Zhong, X. Yang, and W. Hu, "Performance-improved secure OFDM transmission using chaotic active constellation extension," *IEEE Photonics Technology Letters*, vol. 29, no. 12, pp. 991–994, 2017.
- [18] B. Tang, K. Y. Qin, C. W. Chen, and Y. Cao, "A novel clipping-based method to reduce peak-to-average power ratio of OFDM signals," *Information*, vol. 11, no. 2, p. 113, 2020.
- [19] P. Miao, P. Chen, and Z. M. Chen, "Low-complexity PAPR reduction scheme combining multi-band hadamard precoding and clipping in OFDM-based optical communications," *Electronics*, vol. 7, no. 2, p. 11, 2018.
- [20] Y. Rahmatallah and S. Mohan, "Peak-to-average power ratio reduction in OFDM systems: a survey and taxonomy," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 1567–1592, 2013.
- [21] Q. Jia, "Hyperchaos generated from the Lorenz chaotic system and its control," *Physics Letters A*, vol. 366, no. 3, pp. 217–222, 2007.
- [22] B. Liu, L. Zhang, X. Xin, and N. Liu, "Piecewise chaotic permutation method for physical layer security in OFDM-PON," *IEEE Photonics Technology Letters*, vol. 28, no. 21, pp. 2359–2362, 2016.
- [23] L. Y. Xu, H. B. Qiu, Y. L. Li, and J. L. Fu, "DCT-S peak-to-average ratio suppression algorithm in DCO-OFDM system," *Application Research of Computers*, vol. 37, no. 6, 2019.