IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 24, 2019, accepted April 16, 2019, date of current version May 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2912535

Cellular Neural Network Encryption Scheme for Time Synchronization and CPAs Resistance in OFDM-PON

MEIHUA BI[1,2], XIANHAO ZHUO[1], XIAOSONG FU[1], XUELIN YANG[2], AND WEISHENG HU[2]

[1]School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China
[2]State Key Laboratory of Advanced Optical Communication System and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding authors: Meihua Bi (bmhua@hdu.edu.cn) and Xuelin Yang (x.yang@sjtu.edu.cn)

This work was supported in part by the National Nature Science Fund of China under Grant 61501157, Grant 61431009, and Grant 61571291, in part by the Natural Science Foundation of Zhejiang Province under Grant LQ16F050004, and in part by the Science Program of Zhejiang Educational Commission under Grant Y201840746.

ABSTRACT In this paper, we first experimentally demonstrate a novel cellular neural network (CNN)-based physical layer encryption scheme to achieve the capability of chosen-plaintext attacks (CPAs) resistance and time synchronization simultaneously in orthogonal frequency division multiplexing passive optical network (OFDM-PON). By utilizing the hyperchaotic phenomena within a certain parameter range characteristics of CNN, a four-dimensional (4-D) CNN-based system is constructed to strengthen the security of data transmission. And, according to CNN, the chaotic Feistel transform is executed after extracting the indexes of QAM data, in which completely dynamic encrypted data can be achieved for the CPAs resistance. Moreover, a chaotic training sequence generated by CNN used as timing sequence is added to the transmitted OFDM signals to obtain time synchronization and further increasing the confidentiality of the encryption system. A verified experimental system with 10-Gb/s 16-QAM encrypted OFDM signals through 20-km single-mode fiber (SMF) transmission is conducted. And, the results show that the Feistel and CNN-based physical-layer encryption scheme can generate completely dynamic ciphertexts for the CPAs resistance and accurately realize the time synchronization, and without apparent receiver sensitivity deterioration (∼0.3dB) is introduced in comparison with other against CPAs schemes.

INDEX TERMS Cellular neural network (CNN) encryption, orthogonal frequency division multiplexing (OFDM), passive optical network (PON), dynamic ciphertexts.

I. INTRODUCTION

With the rapid development of global telecommunication industry, a large-capacity and high-speed communication system is required to solve the rapidly growing user data traffic [1]. Among them, the passive optical network (PON) has been widely deployed to address the high-bandwidth requirements toward the next-generation multiuser access network. Besides, the technique of orthogonal frequency division multiplexing (OFDM) is a highly attractive multi-carrier modulation technique in future PON, owing to its cost effectiveness, strong immunity to multipath fading, high spectral efficiency and robustness to fiber dispersion [2], [3]. Thus, the OFDM-based PON (OFDM-PON) has been considered as one of the powerful candidate in the next generation optical access networks. However, in practical PON system, due to its inherent broadcasting structure, the downstream data from the optical line terminal (OLT) to the optical network unit (ONU) is vulnerable to be eavesdropped by illegal ONUs, thereby causing information leakage.

To effectively establish a reliable end-to-end data transmission, the chaos-based encryption schemes [4]–[16] for secure transmission in OFDM-PON have been attracting significant attention and achieve better encryption performance, benefiting from its inherent advantages, such as unpredictability, high initial sensitivity, low implementation complexity and ergodicity, etc. Among these reported chaotic schemes, the chaotic partial transmit sequences (CPTS) [4]

The associate editor coordinating the review of this manuscript and approving it for publication was Donatella Darsena.

and chaotic selected mapping (CSLM) [5] were proposed to improve the system performance and security simultaneously. Besides, the repeated iterations for the OFDM signals of beyond extension area and chaotic frame interleaving were introduced to achieve the huge key space [6]. And, IQ-encryption based optimal frame transmission (IQ-OFT) [7] scheme was presented by splitting the QAM symbols into In-phase (I) and Quadrature-phase (Q) parts and then multiplying with different phase sequences to obtain data encryption. However, all the above schemes [4]–[7] need additional bandwidth to transmit the optimal phase factor, which increases the system complexity and reduces the real-time processing capability of system. As an improvement, the low computational complexity schemes were proposed for secure transmission in OFDM-PON, such as chaotic coding IQ encryption [8], chaotic Walsh-Hadamard Transform [9], chaotic constellation transformation and pilot-aided [10], hybrid chaotic confusion and diffusion (HCCD) [11], chaotic completely frequency/time permutation [12], chaotic modified-DFT (discrete Fourier transform) [13], discrete cosine transform (DCT) [14], etc. In these schemes, transmission security was originated from the chaotic IQ encryption, processed matrix or frequency/time permutations, which can achieve better security and large key space simultaneously. Nevertheless, for these schemes, only the size of key space or system performance was focused on, while the threatening and aggressive chosen-plaintext attacks (CPAs) were ignored and only static ciphertexts were involved. In this way, by employing the cryptographic system to compare special ciphertexts with different secret keys, the attacker can easily achieve correct secret keys. As an exception, we presented the dynamic ciphertexts for the CPAs resistance, which were the chaotic nonlinear encryption (CNE) [15] and chaotic phase rotation (CPR) [16] schemes via associating with the previous input data and current values. Whereas, for these schemes, the received data error will spread to the subsequent decryption of dynamic ciphertexts, thus deteriorating the system performance. Besides, the new chaotic systems used for encryption have been proposed for security improvement, such as the hybrid symbol substitution and symbol interleaving with the Brownian motion chaotic system [17], three-dimensional Brownian motion in cell (3DBC) [18], chaotic deoxyribonucleic acid encoding [19], which have been a significantly important research point in OFDM-PON's security enhancement.

Meanwhile, the cellular neural network (CNN) [20], [21] as one of the artificial neural network, is characterized by local interconnection among the cells and multidimensional array of neurons, and its connection weights among neurons can be easily performed by nonlinear circuit. Owing to these features, CNN presents more complex dynamic behavior than common chaotic system, such as bifurcation phenomena, hyper-chaotic behaviors within a certain parameter range, periodic solutions and hyper-chaos. And, the dimension of CNN can be easily adjusted to integrate with other encryption scheme for further enhancing system security.

In this paper, we firstly present a CNN-based encryption scheme for resisting the CPAs and time synchronization for secure data transmission in OFDM-PON. Benefiting from CNN's characteristics including highly nonlinear, easy to be implemented in hardware and high-randomness, 4-D CNN system with complex chaotic properties is configured, which can further enhance the transmission security. And, by combining the Feistel transform in data encryption standard (DES) [22] with the CNN-based chaotic integer sequences, the dynamic ciphertexts for the CPAs resistance with the low computational complexity and the completely dynamic QAM data can be achieved. Furthermore, a chaotic training sequence (TS) is added to the transmitted OFDM signals for the symbol time synchronization with further system security improved purpose. At last, the feasibility of our scheme is verified by the secure transmission of ~10Gb/s encrypted 16-QAM OFDM signals through 20-km single mode fiber (SMF). Experiment results show that, the chaotic Feistel transform for the QAM indexes can achieve completely dynamic ciphertexts for both bit case and IFFT-after OFDM signals, thereby providing the capability of CPAs resistance, and chaotic training sequence realizes the accurate time synchronization. Furthermore, almost no apparent BER performance deterioration is introduced comparing with other against CPAs schemes, which realize better system security and system performance keeping.

II. ENCRYPTION PRINCIPLES

The CNN model is a differential equation with many applications and high operation speed. Here, to reduce the complexity, only the simplified model of CNN equation of state is introduced [21], which is presented as,

$$\frac{dx_i}{dt} = -x_j + a_i p_j + \sum\nolimits_{\substack{k=1\\k\neq j}}^{m} T_{jk} p_k + \sum\nolimits_{k=1}^{m} S_{jk} x_k + I_j \qquad (1)$$

where $j = 1, \ldots, m$, x is the state variable, p is the cell nonlinear output associated with x, S and T are the connection weights of the input and output of adjacent cells respectively. α is the constant, I is the threshold value and m represents the dimension of CNN. It has been proved that the minimal dimension of generating hyper-chaotic attractors is four [23], which means at least 4-D chaos is necessary if we want to achieve a hyper-chaotic system. Based on this, the 4-D CNN is employed for obtaining the chaotic sequence, and it can be presented as [23],

$$\begin{cases}\dot{x}(t) = -z - u\\ \dot{y}(t) = 2y + z\\ \dot{z}(t) = 14x - 14y\\ \dot{u}(t) = 100(x - g(u) + w)\end{cases} \qquad (2)$$

where $g(u) = \alpha u - (|u - 0.4| - |u - 0.8| - |u + 0.4| + |u + 0.8|)$, α and w are the system parameters. In particular, the CNN presents hyper-chaotic properties when $\alpha = 1$ and $w = 0$ [23], [24], and the phase portraits of hyper-chaotic attractors are plotted in Fig. 1. It is found that the proposed

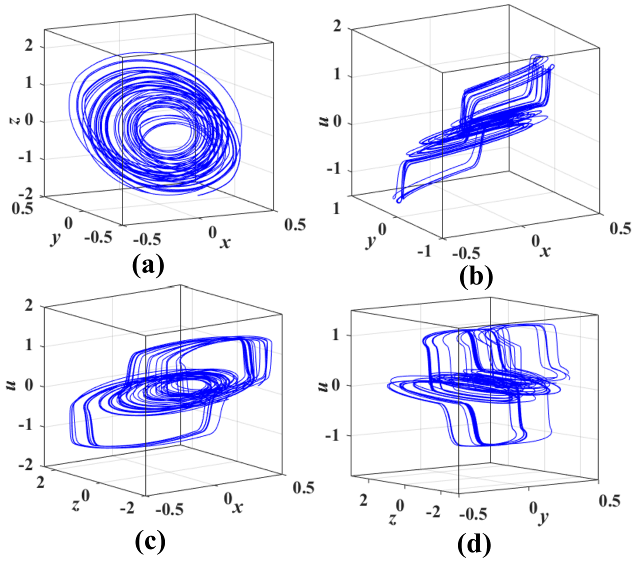


FIGURE 1. The phase portraits of 4-D CNN: (a) *x,y* and *z*; (b) *x*, *y* and *u*; (c) *x,z* and *u*; (d) *y*, *z* and *u*.

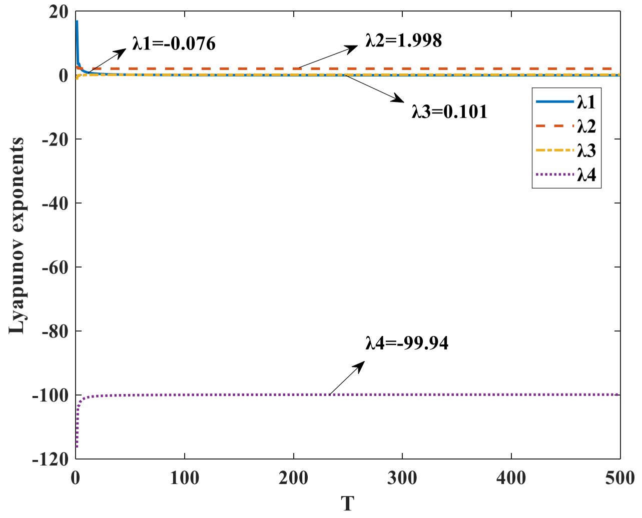


FIGURE 2. The Lyapunov exponents spectrum of 4D-CNN.

TABLE 1. The comparative analysis among the common chaotic system and our proposed 4D-CNN.

Chaotic system	The number of positive Lyapunov exponent	Max Lyapunov exponent
Logistic [26]	1	0.593
Henon [27]	1	0.634
Lorenz [28]	1	1.213
4D-CNN [23]	2	1.998

4-D CNN exhibits excellent random and complexity orbit rather than a clear curve in any phase space projection. This manifests its hyperchaotic behavior, which can further enhance the system confidentiality.

Furthermore, the Lyapunov exponent is given to evaluate the dynamic behavior of 4-D CNN as illustrated in Fig. 2. Here, the Lyapunov exponent is used to indicate the rate of separation/convergence of two adjacent orbits in the phase space, where the positive and negative Lyapunov exponents represent separation and convergence respectively. And, the greater the degree of separation, the more sensitive it is to the initial value. The positive Lyapunov exponent is always used as an important parameter to evaluate the sensitivity to the initial values of chaotic system. By employing the Jacobian method with time size 0.001 and time length 500 [25], the Lyapunov exponents can be calculated. From this figure, it is also shown that, the four Lyapunov exponents are $\lambda_1 = -0.076$, $\lambda_2 = 1.998$, $\lambda_3 = 0.101$ and $\lambda_4 = -99.94$ for the case of t $\to \infty$. Furthermore, we compare and analyze the proposed 4D-CNN with other common chaotic systems as list in table 1. Compared to the common Logistic, Henon and Lorenz chaotic system [26]–[28], our proposed 4D-CNN has the largest Lyapunov exponent, thereby proving its complex dynamic behavior can present higher randomness [25]. And, the 4-D CNN has two positive Lyapunov exponent, which further verifies it is the hyperchaotic system. While for the common low dimensional chaos, only one positive Lyapunov exponent exists. It is also easily got that, the 4D-CNN presents more complex dynamic behaviors than the common chaotic system, these properties are essential to ensure the transmission system confidentiality. Here, the time step of h is set to 0.01 and four-order Runge-Kutta method [29] is utilized to solve (2) with the initial values (0.2, 0.5, 0.1, 0.1). After a serval times initial value iteration, the chaotic sequences $\{x\}$, $\{y\}$, $\{z\}$, $\{u\}$ are obtained.

Next, with the (2), the chaotic sequences are generated and then used to achieve the uniform distributed integers for the Feistel transform and chaotic synchronization operations in OFDM signals, the generation of chaotic integer sequences is given as,

$$D_n^x = mod(Ext\left(x_n, a, b, c\right), T) \tag{3}$$

where x_n is the n-th value in chaotic sequence x, $Ext\left(x_n, a, b, c\right)$ function returns the a-th, b-th and c-th digits of x_n to construct a chaotic integer. The $mod(m, n)$ function generates the reminder of m divides n, and T represents the maximum values in the sequence which is set to 256. After digitization by (3), the sequences $\{x\}$, $\{y\}$ and $\{z\}$ are converted into the chaotic integer sequences $\{D^x\}$, $\{D^y\}$ and $\{D^z\}$. By adopting the CNN-based chaotic sequences, the encryption scheme can be constructed. And the corresponding schematic diagram of our scheme is given in Fig. 3, in which the pseudo-random binary sequence (PRBS) is served as the plaintexts to execute quadrature amplitude modulation (QAM) mapping after the operation of serial-to-parallel (S/P) conversion. The QAM mapped data block is denoted as $X = [X_1, X_2 \ldots X_N]$, where N represents the number of subcarriers in each OFDM symbol. Then,

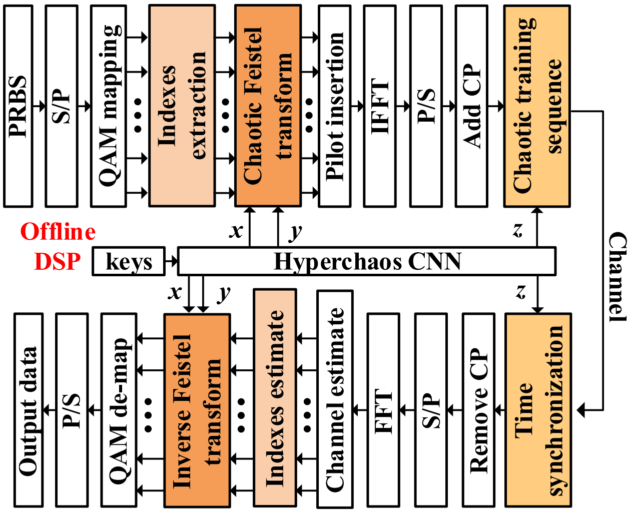


FIGURE 3. Schematic diagram of the proposed CNN-based Feistel transform and chaotic synchronization encryption scheme in OFDM-PON.

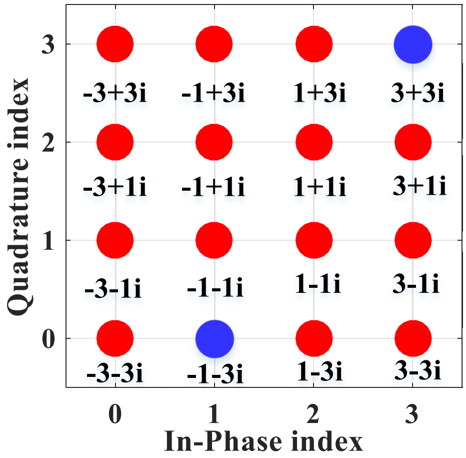


FIGURE 4. The QAM data indexes of 16-QAM constellation diagram.

the chaotic Feistel transform encryption for QAM data in each OFDM symbol is implemented as follows.

For the CNN-based QAM indexes encryption, the Feistel structure in DES [22] is introduced for CPAs resistance. In this paper, the 16-QAM mapping is employed for the OFDM signal modulation, and the constellation diagrams are plotted in Fig. 4, where QAM data indexes are divided from 0 to 3 for In-phase and Quadrature-phase parts respectively. First, the In-phase (I) and Quadrature-phase (Q) parts indexes are extracted from an OFDM symbol, which is set as $I = \{I_1, I_2 \ldots I_N\}$ and $Q = \{Q_1, Q_2 \ldots Q_N\}$ respectively, where I_i represents the i-th In-phase index of QAM data in the constellation diagrams. Similarly, Q_i denotes the i-th Quadrature-phase index. After the index extraction, the CNN-based chaotic Feistel encryption is built as the following rules,

$$\begin{aligned} L_i &= \left(I_i + R_{i-1} + D_i^x\right) mod\ M \\ R_i &= \left(Q_i + L_{i-1} + D_i^y\right) mod\ M \end{aligned} \tag{4}$$

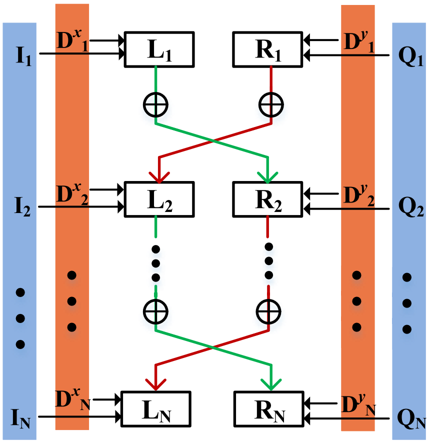


FIGURE 5. The principle of chaotic Feistel transform encryption for the QAM indexes in an OFDM symbol.

where L_i and R_i are the i-th output of the Feistel transform, D_i^x and D_i^y represent the generated chaotic integers in (3), and M is set to $log_2 16$ according to the 16-QAM constellation order, hence the generated values from (4) are between 0 to 3. To realize the Feistel transform, the QAM index are split into two parts (I_i, Q_i). For each round, we compute new QAM index L_i or R_i by (4), and achieve the encrypted index location (L_i, R_i), then the new generated i-th QAM data X_i' is,

$$X_i' = \varphi(L_i, R_i) \tag{5}$$

here, φ represents the constellation diagrams indexes in Fig. 4. And an example of QAM variation is also illustrated to exhibit the random characteristics before and after chaotic Feistel transform, where 3+3i is converted to −1-3i. In this way, the encrypted QAM data block $X' = \left[X_1', X_2' \ldots X_N'\right]$ can be achieved.

To further describe the chaotic CNN-based Feistel transform scheme, we give the detailed structure as depicted in Fig. 5. From this figure and (4), it is easily got that, the newly generated ciphertext index L_i is determined by current index I_i, current chaotic integers D_i^x and previous right part value R_{i-1}. With the same way, the ciphertext index R_i can be obtained. These generated indexes are completely dynamic with respect to input data or chaotic integers, hence achieving dynamic QAM data for OFDM signals. Meanwhile, to obtain absolutely correct encrypted data, all of the input data and same chaotic integers are required to reconstruct the inverse Feistel transform, which can effectively against CPAs if eavesdroppers want to steal system keys via comparing special plaintexts.

After the chaotic Feistel transform, these encrypted QAM data are sent for the pilot insertion, inverse fast Fourier transform (IFFT) and cyclic prefix (CP) insertion. In a common OFDM system, a training sequence is needed to insert in front of the transmitted OFDM signals for symbol timing synchronization [30]. In our proposed encryption scheme, in order to improve the system security and realize the synchronization, the chaotic sequence $\{D^z\}$ is convert into chaotic binary

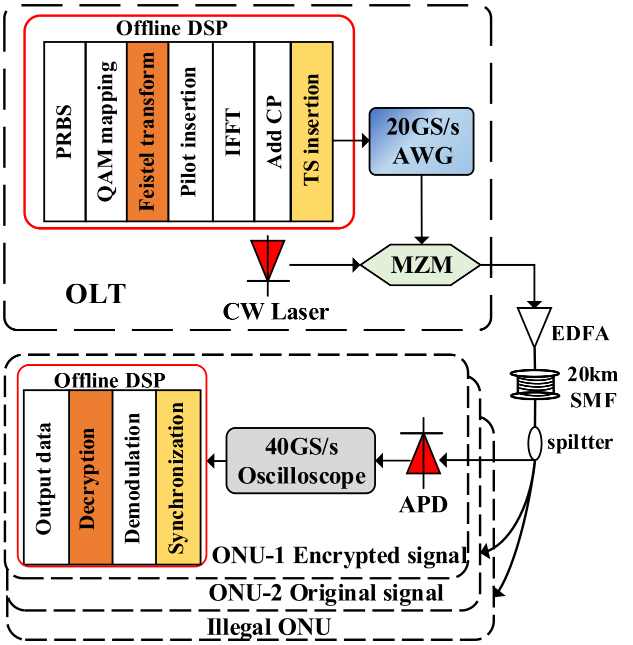


FIGURE 6. Experimental setup of the proposed CNN-based Feistel transform and time synchronization scheme in OFDM-PON.

sequence and inserted to the transmitted signals as training sequence due to its good auto-correlation. Finally, these encrypted OFDM signals are sent for the SMF transmission.

At the receiving end, the OFDM signals are firstly executed time synchronization to find the beginning position of each symbol via auto-correlation of chaotic training sequence. Then, the pre-demodulation QAM data are implemented index estimation firstly by (6), to find the most likely index in 16-QAM constellation diagrams, which is denoted as,

$$[I, Q] = min\,(abs(A' - A)) \tag{6}$$

where A' presents the received data on the frequency domain after FFT, and A is 16-QAM symbols in the standard 16-QAM mapping constellation. The function $abs()$ is employed to calculate absolute value, and $min()$ returns the minimum absolute value. With the (6), the most similar QAM index for current received QAM data A' can be achieved, hence realizing data recovery. In addition, since the indexes of constellation points in each QAM symbol are fixed, the signals distortion or constellation expansion can be rectified to the correct constellation point with this equation, except for the obviously incorrect data. Therefore, this pre-estimate processing of (6) can achieve better demodulation performance comparing with the directly QAM data recovery.

III. EXPERIMENTAL SETUP

Following the configuration mentioned above, we construct the experiment of our proposed CNN-based Feistel transform and time synchronization encryption scheme as shown in Fig. 6, where two regular ONUs and one illegal ONU are adopted to verify encryption performance. At the transmitter, the initial values of CNN are used as the security keys and stored in advance on the legal ONUs. Here, 512 IFFT points are applied for the OFDM signal modulation, where 128 subcarriers are used to carry encrypted 16-QAM data and another 128 subcarriers are filled with the corresponding complex conjugate data, thereby outputting real data for intension modulation. Here, the channel estimation is performed by inserting block-pilot with equal interval. After performing IFFT and parallel-to-serial (P/S) conversion on the encrypted data, the cyclic prefix (CP) with 1/8 OFDM symbol length is appended to each OFDM symbols. Besides, the TS generated by the CNN is inserted into OFDM symbols to achieve the time synchronization. The data encryption and modulation procedures are processed offline by the MATLAB. Then, these encrypted OFDM signals are injected into the arbitrary waveform generator (AWG, Tektronix, 7122C) to generate electrical OFDM signals, where the sampling rate of AWG is 20-GSa/s. Then, a continuous-wave (CW) laser with a central wavelength of 1550nm is employed to drive the Mach-Zehnder modulator (MZM) to convert the electrical signals into 10Gb/s optical signals. After that, the optical signals are boosted by an Erbium Doped Fiber Amplifier (EDFA) and then launched into 20km SMF.

At the ONUs, after SMF transformation, the received optical OFDM signals are distributed to corresponding ONUs by the power splitter. Then, optical OFDM signals are converted to electrical OFDM signals through a special avalanche photodiode (APD) [31], [32]. After that, the generated electrical signals are sampled and digitalized by a real-time oscilloscope (LeCroy SDA 830Zi-A) at a sampling rate of 40 GSa/s. Finally, by using the offline MATLAB program, time synchronization, data decryption and demodulation with the inverse operation as implemented at transmitter can be executed.

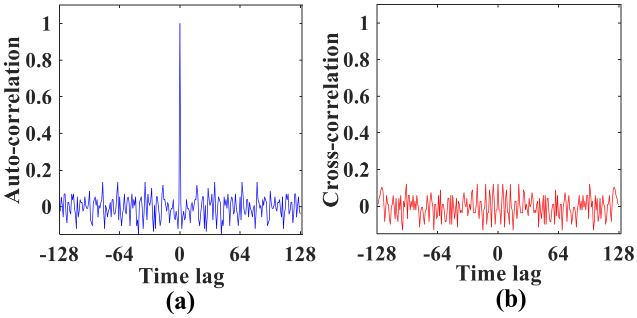


FIGURE 7. (a) Auto-correlation and (b) cross-correlation of the chaotic training sequence of time synchronization.

IV. RESULTS ANALYSIS AND FURTHER DISCUSSION

For the OFDM signals decryption and demodulation, the chaotic training sequence is added to the transmitted signals for time synchronization thereby obtaining the beginning of the receive data. To verify this function, Fig. 7 presents the auto-correlation and cross-correlation function of chaotic training sequences with different initial

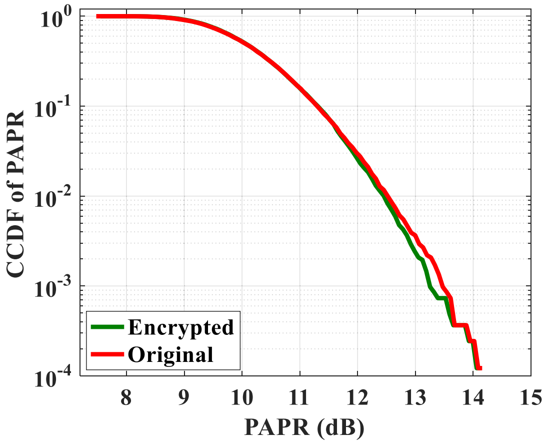


FIGURE 8. CCDF of PAPR for original and encrypted signals in OFDM-PON.

values. From Fig. 7(a), we can find that a sharp peak is appeared between the chaotic training sequence and received data in the condition of without time lag, and the auto-correlation value is sufficiently approximate to 1, which can correctly locate the received OFDM signals. However, another different chaotic sequences which generated by CNN with different initial values cannot achieve any peak value no matter what time lags in the received data, and the cross-correlation function is around zero, as shown in Fig. 7(b). As a result, the generated chaotic synchronization sequence by CNN has a quite good random feature and auto-correlation for the secure transmission.

Then, to directly evaluate the peak to average power ratio (PAPR) of the original and the encrypted OFDM signals, the curves of complementary commutative distribution function (CCDF) of PAPR are presented in Fig. 8, where 16384 OFDM symbols are adopted for the measurement. From Fig. 8, we observed that the PAPR of encrypted OFDM signals is almost the same as original ones, without measurable PAPR fluctuation, which verified that the proposed chaotic Feistel transform encryption can maintain PAPR stability as the original case.

Moreover, the BER curves for original and encrypted data in both back-to-back (BtB) and 20km SMF transmission are also measured, which is presented in Fig. 9. For the legal ONUs, these encrypted OFDM signals are correctly decrypted and demodulated with pre-concerted secret keys. On the contrary, due to the initial values sensitivity of CNN-based chaos system, any illegal ONUs cannot recover the original signals and obtain ~0.5 BER when one of the initial values has 10^{-15} discrepancy from the correct key. The received constellation diagrams of channel estimation for legal and illegal ONUs are also presented in Fig. 9(a) and Fig. 9(b), to further verify the security performance. In contrast to the 16-QAM constellation points in Fig. 9(b), the illegal ONU's constellation in Fig. 9(a) is completely distorted and unable to be distinguished for the signals recovery.

Besides, in the common encrypted OFDM system with the implementation of CPAs resistance, the received data with a certain amount of errors will obviously introduce ~1dB BER deterioration (BER@10^{-3}) due to the repeatedly dynamic ciphertexts decryption [15], [16]. And, for our scheme, the CPAs resistance is achieved via chaotic Feistel transform to generate completely dynamic ciphertexts as previous schemes [15], [16]. However, the dynamic data recovery by (6) is different from the common against CPAs schemes [15], [16], where QAM indexes estimation are implemented to replace the directly QAM data recovery. With these processing, our scheme has lower receiver sensitivity distortion than previous CPAs resistance schemes [15], [16] due to the CPAs noise accumulation correction. From Fig. 9, we observed that the proposed encrypted case without apparent BER deterioration, only ~0.3dB (BER@$10^{-3)}$ receiver sensitivity difference is introduced after correct data demodulation, which verifies that the proposed Feistel transform encryption scheme with the CPAs resistance capability can realize the receiver sensitivity keeping and physical layer security improvement simultaneously.

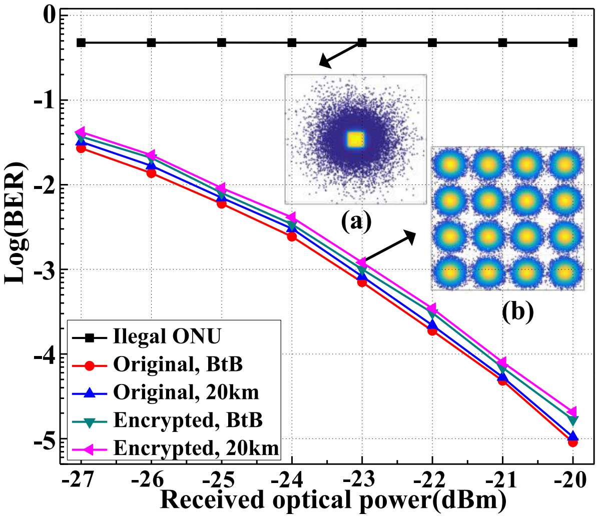


FIGURE 9. BER curves for original and encrypted OFDM signals in OFDM-PON.

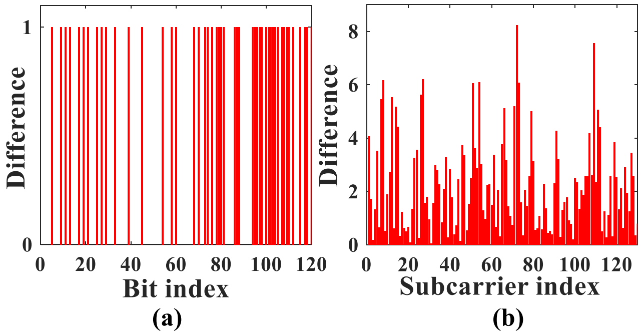


FIGURE 10. OFDM ciphertext variations with one original QAM data change: (a) the bit case. (b) IFFT-after case.

Next, to verify the CPAs resistance of our scheme, the ciphertexts variations with corresponding plaintext change are present in Fig. 10, where *y*-axis shows ciphertexts

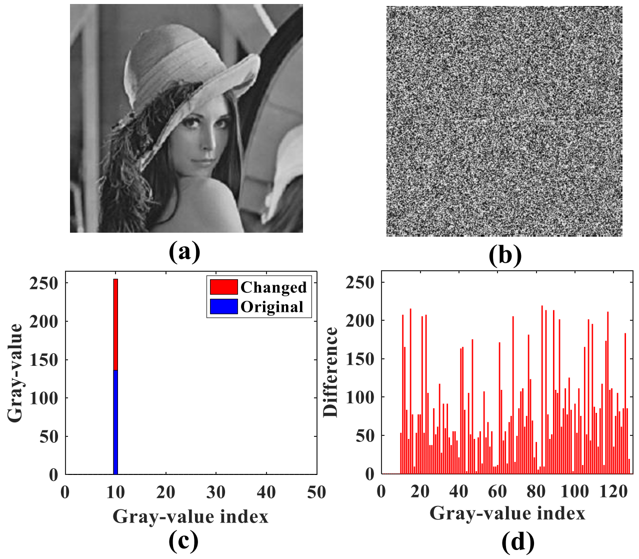


FIGURE 11. (a) original image. (b) encrypted image. (c) one gray value change in the original image. (d) corresponding gray-value difference in encrypted image.

difference after one 16-QAM data change in plaintext, such as1+1i substituted by 3-1i. From the bits ciphertext variations of Fig. 10(a), we can intuitively find that the plaintext difference is spread to the entire OFDM symbol, which leads to irregular bit difference. Furthermore, Fig. 10(b) plots the OFDM signal variations after IFFT between original and generated ciphertexts, it is shown that the plaintext variation also brings about obviously OFDM signals difference and distributed among all of the subcarriers. Meanwhile, the encryption capability of the proposed scheme is also verified via a classical figure, as shown in Fig. 11. The encryption effect is presented in Fig. 11(a) and Fig. 11(b), the original image has been distorted and indistinguishable absolutely, which cannot achieve any meaningful information. And, with one gray value change in the original image (136 substituted by 255) as shown in Fig. 11(c), Fig. 11(d) provides gray-value difference in an encrypted image to demonstrate huge gray values fluctuations. The dynamic ciphertext variations in Fig. 10 and Fig. 11 is mainly attributed to the Feistel transform in (4). With this equation, the current QAM index is determined by the previous encrypted index and chaotic value, which would bring the significant change for the QAM data of PRBS or images. In this way, the next ciphertext in the whole OFDM symbol would generate completely dynamic variations, which can effectively resist the CPAs attacks even if some eavesdroppers want to break encryption system via comparing special plaintexts. Besides, to evaluate the multi-fold encryption capability of the proposed scheme, the BER with the case of only chaotic synchronization decryption and only Feistel decryption are plotted in Fig. 12. The complete decryption process can effectively recover correct original data, whereas the independent decryption processes either chaotic synchronization decryption in Fig. 12(a) or Feistel decryption in Fig. 12(b) will incur ~0.5 BER, which reveals an effective independent and complete encryption performance.

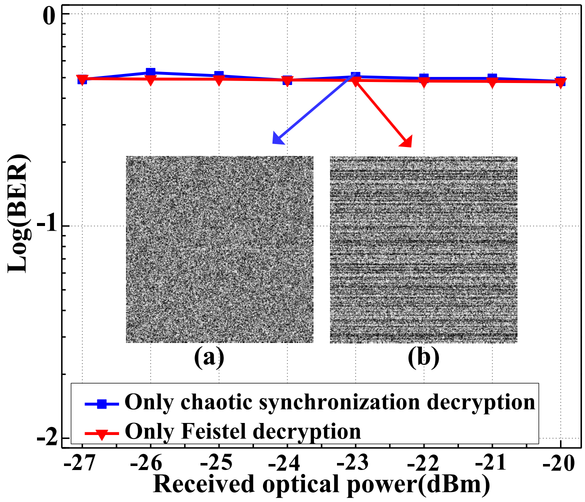


FIGURE 12. BER performance: (a) only chaotic synchronization decryption. (b) only Feistel transform decryption.

TABLE 2. The comparative analysis among the proposed physical layer encryption schemes and our proposed scheme.

Scheme	BER	PAPR	CPAs Resistance
WHT [9]	~1dB(Improvement)	~1dB(Reduction)	No
DFT [13]	~1dB(Improvement)	~2.6dB(Reduction)	No
DCT [14]	~1dB(Improvement)	~1dB(Reduction)	No
CNE [15]	~0dB(Deterioration)	~2.8dB(Reduction)	Yes
CPR [16]	~1dB(Deterioration)	~0dB (Invariant)	Yes
our	~0.3dB(Deterioration)	~0dB (Invariant)	Yes

In addition, the comparative analysis of the BER, PAPR and CPAs resistance among other schemes and ours are given in Table 2. The schemes such as the WHT [9], DFT [13] and DCT [14] based on chaotic precoding can achieve the PAPR reduction for improving the system performance, while the CPAs resistance are not involved. Our scheme and the CPR in [16] can achieve the good capacity of CPAs resistance without improving PAPR. Whereas, the BER deterioration induced by the CPAs resistance is introduced for CPR [16], CNE [15] and ours. It should be noted that, as for our previous report [15], the BER deterioration can be compensated by the PAPR reduction. While, for the case of no any PAPR reduction operation, the lowest (~0.3dB) BER deterioration for our method can be achieved in comparison with the CPR and CNE schemes, which indicates that our scheme can also obtain good BER performance with the capacity of resisting the CPAs. And, all the PAPR reduction methods in Table 2 can also be applied to our scheme.

Moreover, we also give the computational complexity comparison for our scheme and others with the same parameter configuration in table 3. Here, the number of subcarriers

TABLE 3. Comparison of computation complexity of our scheme and other physical layer encryption schemes.

Scheme	Real Addition (N=128)	Real Multiplication (N=128)
WHT [9]	32512 ($2N(N$-1))	65536 ($4N^2$)
DFT [13]	32512 ($2N(N$-1))	65536 ($4N^2$)
DCT [14]	32768 ($2N$+$2N(N$-1))	33536 ($6N$+$2N^2$)
CNE [15]	33534 ($2N(N$-1)+2($4N$-1))	65536 ($4N^2$)
CPR [16]	128 (N)	512 ($4N$)
our	512 ($4N$)	256 ($2N$)

is set to N, and only one OFDM symbol is used. For fair comparison, according to the [33] and [34], the computational complexity of these schemes are presented in terms of real multiplication and real addition. By using the method as in [35], all complex operation for some schemes are uniformly converted into the real one. It is noted that, since the time synchronization operation is almost the same for any OFDM-based system even with in non-encryption OFDM-PON, the complexity of CPR [16] and our scheme induced by the chaotic synchronization can be ignored for fair comparison. In this way, only the complexity of the chaotic Feistel transform operation is needed to be analyzed. As described in (4) of section II, it is easily obtained that our scheme only contains $2N$ multiplication and $4N$ addition operations. And, from this table, we can get that, our scheme and the method CPR in [16] can achieve the lower complexity in comparison with the WTH [9], DFT [13], DCT [14] and CNE [15] methods. It can be attributed to that, for these two schemes, no any matrix multiplication operation is involved in the encryption processing. Furthermore, from the results of table 2 and table 3, we can get that our scheme can achieve the lower BER distortion even with the similar low computational complexity as the other CPAs resistance schemes.

Finally, after the CPAs resistance implementation, the robustness of against brute force attacks can be realized by the large key space, which is quantitatively evaluated as follows. Firstly, as mentioned in Fig. 9, the initial values sensitivity will result in data recovery failure when has 10^{-15} discrepancy from hyper-chaos CNN system, so four chaotic initial values can provide a key space of $10^{60}(10^{15} \times 10^{15} \times 10^{15} \times 10^{15})$. Secondly, sixteen points location of standard 16-QAM constellation diagrams in Fig. 4 can be arbitrarily moved and do not affect the encryption effect after Feistel transform, hence achieving $\sim 10^{13}(16!)$ key space. Thirdly, the Feistel transform is implemented and the number of subcarriers is 128 for an OFDM symbol, the number of exhaustive attacks is $\sim 10^{154}(16^{128})$ if eavesdroppers want to construct a correct OFDM symbol with 16-QAM data. Therefore, the total key space of $\sim 10^{227}$ is created. And, other key space enhanced scheme (like chaotic completely frequency/time permutation [12], etc) can be combined with this proposed encryption scheme to further enlarge the key space of this scheme, which provides a reliable security for the brute force attacks. Therefore, the capability of CPAs resistance and brute force attacks resistance are implemented simultaneously in our proposed encryption scheme and provide a secure transmission in OFDM-PON.

V. CONCLUSION

This paper proposes a chaotic Feistel transform and chaotic time synchronization scheme based on CNN system for the physical layer security improvement in OFDM-PON, which provides the capability of CPAs resistance and obtains $\sim 10^{227}$ key space to resist brute force attacks, as well as keeps better receiver sensitivity when compared with previous against CPAs schemes. The feasibility of the encryption algorithm is verified by the ~10Gb/s secure transmission experiment over 20km SMF. Moreover, our scheme has the low computational complexity, which can be utilized jointly some PAPR reduction methods or key space enhanced schemes to simultaneously realize security enhancement and PAPR reduction, thereby providing a promising candidate scheme for next generation optical access network.

REFERENCES

[1] H. S. Abbas and M. A. Gregory, "The next generation of passive optical networks: A review," *J. Netw. Comput. Appl.*, vol. 67, pp. 53–74, May 2016.

[2] X. Hu *et al.*, "High-capacity and low-cost long-reach OFDMA PON based on distance-adaptive bandwidth allocation," *Opt. Express*, vol. 23, no. 2, pp. 1249–1255, 2015.

[3] S.-Y. Jung, C.-H. Kim, S.-M. Jung, and S.-K. Han, "Optical pulse division multiplexing-based OBI reduction for single wavelength uplink multiple access in IM/DD OFDMA-PON," *Opt. Express*, vol. 24, no. 25, pp. 29198–29208, 2016.

[4] 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 Photon. Technol. Lett.*, vol. 27, no. 23, pp. 2429–2432, Dec. 1, 2015.

[5] X. Hu, X. Yang, and W. Hu, "Chaos-based selected mapping scheme for physical layer security in OFDM-PON," *Electron. Lett.*, vol. 51, no. 18, pp. 1429–1431, Sep. 2015.

[6] J. Zhong, X. Yang, and W. Hu, "Performance-Improved secure OFDM transmission using chaotic active constellation extension," *IEEE Photon. Technol. Lett.*, vol. 29, no. 12, pp. 991–994, Jun. 15, 2017.

[7] W. Zhang, C. Zhang, C. Chen, W. Jin, and K. Qiu, "Joint PAPR reduction and physical layer security enhancement in OFDMA-PON," *IEEE Photon. Technol. Lett.*, vol. 28, no. 9, pp. 998–1001, May 1, 2016.

[8] W. Zhang, C. F. Zhang, W. Jin, C. Chen, N. Jiang, and K. Qiu, "Chaos coding-based QAM IQ-encryption for improved security in OFDMA-PON," *IEEE Photon. Technol. Lett.*, vol. 26, no. 19, pp. 1964–1967, Oct. 1, 2014.

[9] A. A. E. Hajomer, X. Yang, and W. Hu, "Chaotic Walsh–hadamard transform for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 6, pp. 527–530, Mar. 15, 2017.

[10] W. Zhang, C. Zhang, C. Chen, and K. Qiu, "Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement," *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1524–1530, May 1, 2017.

[11] W. Zhang, C. Zhang, C. Chen, H. Zhang, W. Jin, and K. Qiu, "Hybrid chaotic confusion and diffusion for physical layer security in OFDM-PON," *IEEE Photon. J.*, vol. 9, no. 1, Feb. 2017, Art. no. 7201010.

[12] M. Bi *et al.*, "A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON," *IEEE Photon. J.*, vol. 9, no. 2, Apr. 2017, Art. no. 7901510.

[13] X. Fu, M. Bi, X. Zhou, G. Yang, Q. Li, and Z. Zhou, "A chaotic modified-DFT encryption scheme for physical layer security and PAPR reduction in OFDM-PON," *Opt. Fiber Technol.*, vol. 42, pp. 126–131, May 2018.

[14] Z. Wang, F. Chen, W. Qiu, S. Chen, and D. Ren, "A two layer chaotic encryption scheme of secure image transmission for DCT precoded OFDM-VLC transmission," *Opt. commun.*, vol. 410, pp. 94–101, Mar. 2018.

[15] 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 Photon. Technol. Lett.*, vol. 29, no. 24, pp. 2147–2149, Dec. 15, 2017.

[16] X. Yang, Z. Shen, X. Hu, and W. Hu, "Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission," *IEEE Photon. Technol. Lett.*, vol. 28, no. 22, pp. 2499–2502, Nov. 15, 2016.

[17] W. Zhang, C. Zhang, C. Chen, H. Zhang, and K. Qiu, "Brownian motion encryption for physical-layer security improvement in CO-OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 12, pp. 1023–1026, Jun. 15, 2017.

[18] T. Wu *et al.*, "Security enhancement for OFDM-PON using Brownian motion and chaos in cell," *Opt. Express*, vol. 26, no. 18, pp. 22857–22865, Sep. 2018.

[19] C. Zhang, W. Zhang, C. Chen, X. He, and K. Qiu, "Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding," *J. Lightw. Technol.*, vol. 36, no. 9, pp. 1706–1712, May 1, 2018.

[20] B. Norouzi and S. Mirzakuchaki, "An image encryption algorithm based on DNA sequence operations and cellular neural network," *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13681–13701, Jun. 2017.

[21] X. Wang, B. Xu, and H. Zhang, "A multi-ary number communication system based on hyperchaotic system of 6th-order cellular neural network," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 1, pp. 124–133, Jan. 2010.

[22] C. J. Mitchell, "On the security of 2-key triple DES," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6260–6267, Nov. 2016.

[23] X. Huang, Z. Zhao, Z. Wang, and Y. Li, "Chaos and hyperchaos in fractional-order cellular neural networks," *Neurocomputing*, vol. 94, pp. 13–21, Oct. 2012.

[24] F. Chen and J.-B. Li, "Hyperchaos in RTD-based cellular neural networks," *Int. J. Bifurcation Chaos*, vol. 18, no. 11, pp. 3439–3446, Dec. 2007.

[25] K. Ramasubramanian and M. S. Sriram, "A comparative study of computation of Lyapunov spectra with different algorithms," *Phys. D, Nonlinear Phenomena*, vol. 139, no. 1, pp. 72–86, May 2000.

[26] S. Li *et al.*, "Secure strategy for OFDM-PON using digital chaos algorithm with fixed-point implementation," *J. Lightw. Technol.*, vol. 36, no. 20, pp. 4826–4833, Oct. 15, 2018.

[27] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Process.*, vol. 153, pp. 11–23, Dec. 2018.

[28] Q. Jia, "Hyper chaos generated from the Lorenz chaotic system and its control," *Phys. Lett. A*, vol. 366, no. 3, pp. 217–222, Jun. 2007.

[29] N. Razali, R. R. Ahmad, M. Darus, and A. S. Rambely, "Fifth-order mean Runge-Kutta methods applied to the Lorenz system," in *Proc. 13th WSEAS Int. Conf. Appl. Math. (MATH)*, 2008, pp. 333–338.

[30] Z. Hu and C.-K. Chan, "A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON," *J. Lightw. Technol.*, vol. 36, no. 16, pp. 3373–3381, Aug. 15, 2018.

[31] M. Bi, S. Xiao, H. He, J. Li, L. Liu, and W. Hu, "Power budget improved symmetric 40-Gb/s long reach stacked WDM-OFDM-PON system based on single tunable optical filter," *IEEE Photon. J.*, vol. 6, no. 2, pp. 1–8, Apr. 2014.

[32] H. He, J. Li, M. Bi, and W. Hu, "20-Gbps low cost WDM-OFDM-PON downstream transmission with tunable f ilter and linear APD module ," *Chin. Opt. Lett.*, vol. 12, no. 4, Apr. 2014, Art. no. 040603.

[33] A. A. E. Hajomer, X. Yang, and W. Hu, "Secure OFDM transmission precoded by chaotic discrete Hartley transform," *IEEE Photon. J.*, vol. 20, no. 2, Apr. 2018, Art. no. 7901209.

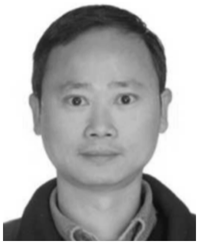
[34] Y. Wu, C. He, Q. Zhang, Y. Sun, and T. Wang, "Low-complexity recombined SLM scheme for PAPR reduction in IM/DD optical OFDM systems," *Opt. Express*, vol. 26, no. 24, pp. 32237–32247, 2018.

[35] Z. Hu and C.-K. Chan, "A real-valued chaotic orthogonal matrix transform-based encryption for OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 30, no. 16, pp. 1455–1458, Aug. 15, 2018.

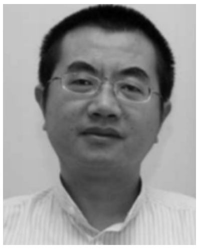
MEIHUA BI received the Ph.D. degrees in communication and information systems from the State Key Laboratory of Advanced Optical Communication System and Networks, Shanghai Jiao Tong University, China, in 2014. She joined the School of Communication Engineering, Hangzhou Dianzi University, China. She has published over 20 journal and conference papers, such as *Optics Express*, *Photonics Technology Letters*, and The Optical Networking and Communication Conference & Exhibition. Her major research interests include next generation passive optical access networks, optical-wireless access networks, optical system-based fronthaul/backhaul, and free-space optical communications.

XIANHAO ZHUO received the B.S. degree in electronic information engineering from the Henan University of Technology, Zhengzhou, Henan, China, in 2017. He is currently pursuing the M.Sc. degree with the School of Communication Engineering, Hangzhou Dianzi University. His research interest includes physical layer encryption based on digital chaos in the optical access networks.

XIAOSONG FU received the B.S. degree in communication engineering from Hangzhou Dianzi University, Hangzhou, Zhejiang, China, in 2016, where he is currently pursuing the M.Sc. degree with the School of Communication Engineering. His research interests include data encryption and peak to average power ration reduction in orthogonal frequency division multiplexing passive optical networks.



XUELIN YANG is currently a Professor with Shanghai Jiao Tong University. His research interests include ultrafast all-optical signal processing in optical fiber communication, applications of semiconductor optical amplifiers, security of optical networks, optical orthogonal frequency division multiplexing transmission, and passive optical networks.



WEISHENG HU is currently a Professor with Shanghai Jiao Tong University. He serves on the Editorial Board of *Optics Express*, the *Journal of Lightwave Technology*, and *Chinese Optics Letters*.