| Title       | Security enhancement for OFDM-PON using Brownian motion and chaos in cell |
|-------------|-------------------------------------------------------------------------|
| Author(s)   | Wu, Tingwei; Zhang, Chongfu; Chen, Chen; Hou, Haodong; Wei, Hanhan; Hu, Shaohua; Qiu, Kun |
| Citation    | Wu, T., Zhang, C., Chen, C., Hou, H., Wei, H., Hu, S., & Qiu, K. (2018). Security enhancement for OFDM-PON using Brownian motion and chaos in cell. Optics Express, 26(18), 22857-. doi:10.1364/OE.26.022857 |
| Date        | 2018                                                                    |
| URL         | http://hdl.handle.net/10220/47606                                        |
| Rights      | © 2018 Optical Society of America under the terms of the OSA Open Access Publishing Agreement. Users may use, reuse, and build upon the article, or use the article for text or data mining, so long as such uses are for non-commercial purposes and appropriate attribution is maintained. All other rights are reserved. |
Security enhancement for OFDM-PON using Brownian motion and chaos in cell

Tingwei Wu,1,2,4 Chongfu Zhang,1,2,4,* Chen Chen,3 Haodong Hou,1 Hanhan Wei,1,2 Shaohua Hu,1 and Kun Qiu1

1Key Laboratory of Optical Fiber Sensing and Communication Networks (Ministry of Education), School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
2School of Electronic and Information Engineering, University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China
3School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, 639798, Singapore
4These authors contributed equally to this work
*cfzhang@uestc.edu.cn

Abstract: We propose a novel security enhancement technique for a physical layer secure orthogonal frequency division multiplexed passive optical network (OFDM-PON) based on three-dimensional Brownian motion and chaos in cell (3DBCC). This method confuses an OFDM symbol via transforming it into a 3D symbol matrix and a 3D cell matrix with different size lengths. Different dividing-confusion rules then generate different complementary cumulative distribution functions (CCDFs) of peak-to-average power ratio (PAPR). And we can pre-estimate bit error rate (BER) performance by calculating the CCDF values. We also find that the processing time decreases with the matrix’s side length decreasing simultaneously. A new weighted comprehensive value ($Q_w$) is further used to evaluate the overall performance between the processing time and the BER. Finally, an experiment successfully demonstrates a physical layer secure OFDM signal transmission with 22.06-Gb/s data rate over a 25.4-km standard single mode fiber (SSMF). These results indicate that cell (5×3) has the weighted optimum overall performance, which verifies that the proposed encryption technique is promising for building a physical layer security enhanced OFDM-PON system with a low processing time delay and a good BER for future access network systems.

© 2018 Optical Society of America under the terms of the OSA Open Access Publishing Agreement

OCIS codes: (060.4510) Optical communications; (060.4250) Networks; (060.4080) Modulation.

1. Introduction

Passive optical network (PON) is regarded as an advanced “future-proof” way to solve big demand for next-generation multiuser access networks, and orthogonal frequency division multiplexing (OFDM) has been widely used in wired and wireless systems due to its strong ability to resist multipath interference. Therefore, OFDM-based PON (OFDM-PON) is considered as a promising candidate for next generation access networks with many advantages such as high spectral efficiency, robustness against dispersion, low electrical bandwidth requirements, and reduced multipath interference [1,2]. Various applications based on OFDM-PON also focus on information security [3,4]. The traditional encryption methods of OFDM-PON usually aim at the upper layer, which causes the weakness of unprotected headers and controlling frames. Physical layer encryption has attracted fiercely research interests since it can provide transparent encryption, which is envisioned as an efficient approach to solve the security problem of optical access networks.

Due to the advantages of chaos including high randomness and sensitivity to the initial values, various approaches based on chaotic encryption have been employed in the physical layer communication systems. We can divide them into two categories. One is the chaos security technique in the optical domain such as chaotic laser communication [5], exclusive or
(XOR) scrambling [6], and laser-based security for military operations [7]. However, the optical domain chaotic encryption suffers from high sensitivity and limitations of key distribution, and small space of encryption key as well as difficulty to control complex key management and protect data or headers. The other is then the chaos security technique in the electric domain such as wireless chaos-based communication systems [8], hybrid chaos encryption [9], chaos and fractional Fourier transform [10] and piecewise chaotic permutation [11]. In these schemes, a high randomness chaotic sequence is limited by the finite accuracy of computer, because the transmission data is confused by directly using chaotic confusion techniques. In order to improve the ability of encryption, we have studied some methods based on chaotic techniques in the electric domain including chaos coding-based QAM IQ-encryption [12], joint peak-to-average power ratio (PAPR) reduction and chaos encryption [13], chaotic constellation transformation and pilot-aided secure key agreement [14], chaos and deoxyribonucleic acid encoding [15], chaotic pseudorandom radio frequency (RF) subcarriers [16], and hybrid chaotic confusion and diffusion [17]. Moreover, chaotic discrete Hartley transform [18], optical DFT-S-OFDM data encrypted by digital chaos [19], chosen plaintext attack resistance and PAPR reduction [20], chaotic nonlinear encryption [21], phase masking and time-frequency chaotic method [22] have been proposed. In addition, a method based on two-dimensional Brownian motion and chaotic (2DBC) encryption for physical layer security in coherent optical OFDM-PON [23] has been studied, and Brownian motion has also been applied to image encryption [24], but three-dimensional Brownian motion has not yet been applied in physical layer secure OFDM-PON systems. Therefore, a security enhancement approach using three-dimensional Brownian motion and chaos (3DBC) combined with chaos in cell (3DBCC) encryption scheme for OFDM-PON is proposed to further reduce processing time delay and improve bit error rate (BER) performance.

In this paper, to the best of our knowledge, we first propose 3DBC and 3DBCC for physical layer security enhanced OFDM-PON systems. For an OFDM signal, we arrange symbols of each subcarrier into a plane and combine all subcarriers into a 3D symbol matrix, and then use 3DBC to confuse each symbol of 3D symbol matrix. In order to reduce processing time delay and improve BER performance, we divide the 3D symbol matrix into 3D cell matrix by applying a suitable common divisor of three sides, so this 3DBCC can confuse each cell. An experiment successfully demonstrates a physical layer secure OFDM signal transmission with 22.06-Gb/s data rate over a 25.4-km standard single mode fiber (SSMF), and the obtained results verify the effectiveness of the proposed scheme for security enhanced OFDM-PON systems.

2. Principles

For one point in the 3D space, it can be written as

\[
\begin{align*}
dx &= \delta \sin a \cos b \\
dy &= \delta \sin a \sin b \\
dz &= \delta \cos a \\
a &= u \times 2 \times \pi, & b &= v \times 2 \times \pi,
\end{align*}
\]

where \(\delta (0 \leq \delta \leq \infty)\) is the length of step movement, and a \((0 \leq a \leq 2\pi)\) and b \((0 \leq b \leq 2\pi)\) denote the movement directions. u, v, and \(\delta\) are derived from the logistic sine system (LSS), the logistic tent system (LTS) and the tent sine system (TSS), respectively [25].

\[
u_{n+1} = \text{LSS}(p_n, v_n) = \begin{cases} 
(p_n v_n (1-v_n) + (4-p_n) v_n / 2) \mod 1 & v_n < 0.5 \\
(p_n v_n (1-v_n) + (4-p_n) (1-v_n) / 2) \mod 1 & v_n \geq 0.5,
\end{cases}
\]

3. Results
\[
\delta_{n+1} = TSS(p_\delta, \delta_n) = \begin{cases} 
(p_\delta \delta_n / 2 + (4 - p_\delta) \sin(\pi \epsilon_\delta) / 4) \mod 1 & \delta_n < 0.5 \\
(p_\delta (1 - \delta_n) / 2 + (4 - p_\delta) \sin(\pi \epsilon_\delta) / 4) \mod 1 & \delta_n \geq 0.5 
\end{cases}
\]  

(5)

where \(p_\delta, p_\nu, p_\delta\) are the iteration parameters. When \(p_\delta, p_\nu, p_\delta \in (0, 4]\), the LSS, LTS and TSS chaotic systems have good chaotic behaviors. One point in a space can be considered as a Brownian particle in the 3D space. Adding one movement direction and a step length can generate a new 3D Brownian motion trajectory. Figure 1 shows a normalized motivation path with 200-step length of 3DBC. The motion path has good randomness and unpredictability based on 2DBC [23]. But compared with Fig. 1, the movement path of 3DBC has a more complicated trajectory, because 3DBC adds one more extra dimension scrambling. 3DBC can well confuse the symbols via scrambling the positions of these symbols.

\[
\text{Fig. 1. Normalized 3DBC motivation path of one particle.}
\]

If there is a 3D matrix \((M_{3D})\) with the length \(L\), the width \(W\) and the high \(H\) \((M_{3D} = L \times W \times H)\), as shown in Fig. 2, 3DBC can directly scramble the positions of all points in the matrix. Assuming the \(k^{th}\) point position coordinate \(T_k (x_k, y_k, z_k)\) in the space as shown by the red point in Fig. 2(a), the encryption process can be expressed as

\[
x_k^{en} = \text{ceil}\left(\left( x_k + dx_{x,y,z} \right) \mod L \right) \\
y_k^{en} = \text{ceil}\left(\left( y_k + dy_{x,y,z} \right) \mod W \right), \\
z_k^{en} = \text{ceil}\left(\left( z_k + dz_{x,y,z} \right) \mod H \right)
\]

(6)

where \(\text{ceil}(\cdot)\) is the upper bound operation, and \(dx_{x,y,z}, dy_{x,y,z}, dz_{x,y,z}\) are the elements of the matrices \(dx, dy\) and \(dz\), as shown in Fig. 1, which are determined by Eqs. (1)-(5) and the original parameters \((u_0, v_0, \delta_0, p_\nu, p_\delta)\) of LSS, LTS, TSS. These parameters \((u_0, v_0, \delta_0, p_\nu, p_\delta)\) can be saved as a key of 3DBC. Figure 2(b) shows the position of the encrypted red point.

After confusing all the points in \(M_{3D}\), we can obtain an encrypted matrix \(M_{3D}^{en}\) as

\[
M_{3D}^{en} = \sum_{i=1}^{L} \sum_{j=1}^{W} \sum_{k=1}^{H} \text{exchange}(T_i (x, y, z), T_i^{en} (x_i^{en}, y_i^{en}, z_i^{en})),
\]

(7)

where \(\text{exchange}(\cdot)\) stands for an exchange between the original symbol position and the confused symbol position. Due to the static security key allocation technique by using pre-shared security key, the decryption processing can be shown as
\[ x_k^{de} = \text{ceil}((x_k^{en} - dx_{k,y,z}) \mod L) \]
\[ y_k^{de} = \text{ceil}((y_k^{en} - dy_{k,y,z}) \mod W) \]
\[ z_k^{de} = \text{ceil}((z_k^{en} - dz_{k,y,z}) \mod H) \] (8)

Fig. 2. Symbol scrambling in a 3D matrix using 3DBC.

If \( x_k^{en} = 0, y_k^{en} = 0, \) or \( z_k^{en} = 0, \) they are replaced by \( x_k^{en} = L, \) \( y_k^{en} = W \) or \( z_k^{en} = H, \) respectively. The positions of decryption in the \( M_{3D}^{en} \) can be given as

\[ F^{de} = \sum_{x=1}^{L} \sum_{y=1}^{W} \sum_{z=1}^{H} \text{exchange}(T_k^{en}(x_k^{en}, y_k^{en}, z_k^{en}), T_k^{de}(x_k^{de}, y_k^{de}, z_k^{de})). \] (9)

Here, \( F^{de} \) represents the decrypted signal, which is the original signal.

Based on the symbol scrambling in a 3D matrix using 3DBC, we then propose a modified encryption algorithm to reduce the processing time delay and the BER performance loss. In this method, it divides \( M_{3D} \) into different cells, where we choose a suitable common divisor (R) of L, W and H to divide \( M_{3D} \) into a cube matrix (\( M_{\text{cell}} \)). The length of \( M_{\text{cell}} \) is R and each cell has \( N = L \times W \times H/R^3 \) red symbols, as shown in Fig. 3. Regarding each cell as a unit in a 3D matrix, when we apply 3DBCC to confuse the cells, the number of iterations would turn into \( 1/N, \) so the iteration time delay can be greatly reduced. And the security key is also the original parameters of \((u_0, v_0, 0_0, p_u, p_v, p_0)\).

Fig. 3. Cell scrambling in a 3D matrix-cell using 3DBCC.

For an OFDM frame, the symbols can be arranged as \( M_{3D} \) in 3D space and \( M_{\text{cell}} \) in 3D cell, as shown in Figs. 2 and 3, respectively, where H represents the frequency of subcarriers with different colors and each carrier has \( L \times W \) QAM symbols. The method can apply 3DBC and 3DBCC to confuse the symbols and cells respectively.
Since different coding rules can generate different CCDF curves of PAPR, the PAPR influences the BER performance [26]. We then define the value \( V_{\text{PAPR}} \) of multiplying by CCDF and PAPR as

\[
V_{\text{PAPR}} = \sum_{n=1}^{K} p(n)i(n),
\]

where \( p(.) \) is the probability of CCDF and \( i(.) \) is the corresponding PAPR.

In order to reduce time delay and BER performance loss, different \( R \) is used to divide \( M_{\text{3D}} \). Assuming that \( k_1 \) is the weighted ratio of processing time (T) and \( k_2 \) is the weighted ratio of \( V_{\text{PAPR}} \), then the weighted optimum coefficient \( Q_w \) of the comprehensive performance in the system can be defined as

\[
Q_w = k_1 \times T + k_2 \times V_{\text{PAPR}}.
\]

3. Experiment Setup and Results

![Experiment setup](image)

We conduct an experiment as illustrated in Fig. 4 and the symbol encryption is executed offline. MATLAB generates a pseudorandom series of bit streams with a length of \( 1.92 \times 10^5 \) and conducts 16-QAM modulation to convert into \( 4.8 \times 10^4 \) QAM symbols. Serial-to-parallel conversion makes these QAM symbols into a plane matrix \( M_{\text{2D}} \) \((120 \times 400)\). The subcarrier number is 120, and the symbol number is 400 and the IFFT size is 256. Converting each subcarrier symbol into a \( 20 \times 20 \) plane generates a 3D matrix \( M_{\text{3D}} = 120 \times 20 \times 20 \). 3DBC can confuse \( M_{\text{3D}} \) as shown in Fig. 2. In addition, these symbols are transformed into cells and \( R \) is equal to 20, 10, 5 and 4. The side length of \( M_{\text{cell}} \) is 20, 10, 5, 4 and each cell has 6, 48, 384, 750 symbols, respectively. 3DBCC can confuse the cells as shown in Fig. 3. After that IFFT converts the signal from the frequency domain into the time domain. A cyclic prefix (CP) of 1/16 is added in the data sequence. The encrypted signal is sent to an arbitrary waveform generator (AWG Tektronix 7102A) to complete digital analog conversion (DAC) process with a sampling rate of 12.5 GSa/s. It drives a single-drive Mach-Zehnder modulator (MZM). The laser diode (LD) emits a light with a wavelength of 1550 nm, and the output power is 14.49 dBm. The signal passes through a 25.4-km SSMF. A tunable optical attenuator (TOA) can adjust the received optical power. The light is detected by a photodetector (PD) and recorded by a digital phosphor oscilloscope (DPO Tektronix TDS 7404B) with a sampling rate of 25 GSa/s. The resultant digital signal is decrypted offline. In an optical line terminal (OLT), the key \( (u_0, v_0, \delta_0, p_u, p_v, p_\delta) \) of \((0.679702676853675, 0.655098003973841, 0.162611735194631, 2.837459323432290, 3.018746727929444, 1.104100307994314) \) is used as the iterative initial values. When a single-float is applied, the key space of this encryption approach is equal to \( 10^{15} \times 10^{15} \times 10^{15} \times 4 \times 10^{15} \times 4 \times 10^{15} = 6.4 \times 10^{99} \), which has a strong ability to resist exhaustive attack from an illegal receiver.
We calculate the bifurcation diagrams of LSS, LTS and TSS as illustrated in Fig. 5. It shows that these maps have wider chaotic ranges. Due to the characteristic of chaos, these maps have high randomness, unpredictability and sensitivity to the initial values. This indicates that the proposed encryption approach has a good security.

![Bifurcation diagrams](image)

Fig. 5. Bifurcation diagrams of LSS, LTS and TSS. (a) LSS, (b) LTS, (c) TSS.

Table 1 shows the Lyapunov exponent (LE) and the permutation entropy (PE) of each parameter \( u, v, \delta, dx, dy, dz \) based on the mixed chaotic system of LSS, LTS and TSS. Compared with 2DBC, one extra-dimensional substitution \( dz \) added in the system, 3DBC can improve the complexity of trajectory.

|       | \( u \) | \( v \) | \( \delta \) | \( dx \) | \( dy \) | \( dz \) |
|-------|--------|--------|--------|--------|--------|--------|
| **LE** | 0.6879 | 0.6813 | 0.6585 | 0.8313 | 0.8713 | 0.7614 |
| **PE** | 0.6811 | 0.6830 | 0.6796 | 0.9076 | 0.9711 | 0.7641 |

When the transmitted information is fixed, the bit stream of the information is unchanged. Figure 6 shows the CCDF curves of PAPR for each dividing rule of the generated confusion signal. These results indicate that with the PAPR increasing such as more than 9 dB, the performances of cell \( 20^3 \) and cell \( 4^3 \) are the best and the worst, respectively.

![CCDF curves of PAPR](image)

Fig. 6. CCDFs of PAPR for different dividing rules.

A personal computer (PC) with 8-GB memory, Intel core™ i3-8100 and Windows 10 system is used to calculate the processing time of different dividing rules. The encryption and decryption time for 3DBC and 3DBCC is shown in Table 2, in which we can find that the encryption and decryption time of 3DBC are 0.0298 and 0.0281. Compared with the time of 3DBC, only 3DBCC with cell \( 20^3 \) simplified by cell \( 20^3 \) is longer than 3DBC. This may be
caused by transforming the symbols from point into cell. However, when \( R < 10 \), all the encryption and decryption time is less than that of 3DBC. The processing time decreases with the \( M_{cell} \)'s side length decreasing. When \( R \) is equal to 4, the processing time is 0.0029 and 0.0011, respectively.

### Table 2. The processing time of 3DBC and 3DBCC with cell \((20^3,10^3,5^3,4^3)\)

|                   | 3DBC | Cell \((20^3)\) | Cell \((10^3)\) | Cell \((5^3)\) | Cell \((4^3)\) |
|-------------------|------|----------------|----------------|----------------|----------------|
| Encryption time (s)| 0.0298 | 0.0443         | 0.0079         | 0.0033         | 0.0029         |
| Decryption time (s)| 0.0281 | 0.0427         | 0.0061         | 0.0014         | 0.0011         |

In order to compare the comprehensive performance of each dividing rule, \( k_1 \) and \( k_2 \) are set to 100 and 0.05 with the reason that their products have same range order magnitude. The comprehensive values as shown in Table 3, which indicates that cell \((5^3)\) is the optimum dividing rule \((Q_w = 4.830)\) combining good time delay and BER performance. In this case, it is obvious that the weighted comprehensive performance order is cell \((5^3)\) > cell \((4^3)\) > cell \((10^3)\) > 3DBC > cell \((20^3)\).

### Table 3. The comprehensive performance of 3DBC and 3DBCC with cell \((20^3,10^3,5^3,4^3)\)

|                   | 3DBC | cell \((20^3)\) | cell \((10^3)\) | cell \((5^3)\) | cell \((4^3)\) |
|-------------------|------|----------------|----------------|----------------|----------------|
| Processing time (T)| 0.0579 | 0.0870         | 0.0140         | 0.0047         | 0.0040         |
| PAPR value \(V_{PAPR}\) | 87.9437 | 86.8089       | 88.5077       | 87.2000       | 89.5030       |
| Value \(Q_w\)  | 10.187 | 13.040         | 5.825          | 4.830          | 4.875          |

Figure 7 illustrates the measured BER performances of 3DBC, cell \((20^3)\), cell \((10^3)\), cell \((5^3)\), cell \((4^3)\) based legal optical network unit (ONU) and an illegal ONU for encryption signals. From the FEC limit, it is easy to conclude that cell \((20^3)\) has the best BER performance. It approximately improves 1dB compared with that of cell \((4^3)\). These results indicate that \( V_{PAPR} \) can directly pre-estimate the BER performance for an OFDM-PON system, which meets theory very well. And for an illegal ONU, no matter what encryption dividing rule is employed, the BER of the received signal is almost 0.5. This shows these encryption rules have a high security.

![Graph showing BER vs. received optical power](image)

Fig. 7. Measured results of the received OFDM signals versus different encryptions.

Transforming these symbols into the cube cells is conveniently confused by a 3DBC-based method and the other encryption methods such as 3D cat mapping. If any of 3 dimensions is very short, it is rapidly turned by randomly scrambling. It then causes that the
confusion is not optimum. However, our method has a good confusion performance using the normalized 3DBC compared with the other methods such as 3D cat mapping. In the experiment, the bit stream is randomly generated and different bit streams generate different CCDF curves of PAPR. No matter what bit stream is generated, a weighted optimum value $Q_w$ can be then obtained via this method.

4. Summary

In order to reduce processing time delay, improve BER and enhance physical layer security of OFDM-PON, we have proposed and experimentally demonstrated a chaos encryption method using 3DBC and 3DBCC. In this experiment, $4.8 \times 10^3$ 16-QAM symbols have been transformed into the matrixes with $120 \times 20 \times 20$ symbols and different side length-based cells. A physical layer secure OFDM-PON system with 22.06-Gb/s signal has been successfully demonstrated over a 25.4-km SSMF. From the experimental results, we can find:

a) Owing to the addition of one more extra degree of freedom, 3DBC has a more complicated trajectory than that of 2DBC.

b) The $V_{\text{PAPR}}$ of CCDF curves can pre-estimate the BER for different CCDF curves of PAPR.

c) The processing time decreases with the matrix side length decreasing. And 3DBCC can reduce the encryption and decryption processing time delay and improve the BER.

d) A new defined value ($Q_w$) can estimate the weighted overall system performance.

Funding

National Natural Science Foundation of China (NSFC) (61571092); Program for Joint Research of UESTC and Salton Tech (2018STKY001); 111 Project (B14039).

References

1. S. Jain, F. Effenberger, A. Szabo, Z. Feng, A. Forucci, W. Guo, Y. Luo, R. Mapes, Y. Zhang, and V. O’Byrne, “World’s first XG-PON field trial,” J. Lightwave Technol. 29(4), 524–528 (2011).
2. F. J. Effenberger, “The XG-PON system: Cost effective 10 Gb/s access,” J. Lightwave Technol. 29(4), 403–409 (2011).
3. J. Chen, L. Wosinska, C. M. Machuca, and M. Jaeger, “Cost vs. reliability performance study of fiber access network architectures,” IEEE Commun. Mag. 48(2), 56–65 (2010).
4. C. Chen, C. Zhang, D. Liu, K. Qiu, and S. Liu, “Tunable optical frequency comb enabled scalable and cost-effective multiuser orthogonal frequency-division multiple access passive optical network with source-free optical network units,” Opt. Lett. 37(19), 3954–3956 (2012).
5. A. Argyris, D. Syvridis, L. Larter, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, “Chaos-based communications at high bit rates using commercial fibre-optic links,” Nature 438(7066), 343–346 (2005).
6. T. Kodama, N. Nakagawa, N. Kataoka, W. Wada, G. Cincotti, X. Wang, T. Miyazaki, and K. Kitayama, “Secure 2.5 Gbit/s, 16-ary OCDM block-ciphering with XOR using a single multi-port en/decoder,” J. Lightwave Technol. 28(1), 181–187 (2010).
7. H. Kaushal and G. Kaddoum, “Applications of lasers for tactical military operations,” IEEE Access 5, 20736–20753 (2017).
8. G. Kaddoum, “Wireless chaos-based communication systems: A comprehensive survey,” IEEE Access 4, 2621–2648 (2016).
9. M. Cheng, L. Deng, X. Gao, H. Li, M. Tang, S. N. Fu, P. Shum, and D. Liu, “Security-enhanced OFDM-PON using hybrid chaotic system,” IEEE Photonics Technol. Lett. 27(3), 326–329 (2015).
10. L. Deng, M. Cheng, X. Wang, H. Li, M. Tang, S. Fu, P. Shum, and D. Liu, “Secure OFDM-PON system based on chaos and fractional Fourier transform techniques,” J. Lightwave Technol. 32(15), 2629–2635 (2014).
11. B. Liu, L. Zhang, X. J. Xin, and N. Liu, “Piecewise chaotic permutation method for physical layer security in OFDM-PON,” IEEE Photonics Technol. Lett. 28(21), 2359–2362 (2016).
12. 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 Photonics Technol. Lett. 26(19), 1964–1967 (2014).
13. W. Zhang, C. F. Zhang, C. Chen, W. Jin, and K. Qiu, “Joint PAPR reduction and physical layer security enhancement in OFDMA-PON,” IEEE Photonics Technol. Lett. 28(9), 998–1001 (2016).
14. W. Zhang, C. F. Zhang, C. Chen, and K. Qiu, “Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement,” J. Lightwave Technol. 35(9), 1524–1530 (2017).
15. C. F. Zhang, W. Zhang, C. Chen, X. J. He, and K. Qiu, “Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding,” J. Lightwave Technol. 36(9), 1706–1712 (2018).
16. C. F. Zhang, W. Zhang, X. J. He, C. Chen, H. J. Zhang, and K. Qiu, “Physically secured optical OFDM-PON by employing chaotic pseudorandom RF subcarriers,” IEEE Photon. J. 9(5), Art. No. 7204408 (2017).
17. W. Zhang, C. F. Zhang, C. Chen, H. J. Zhang, W. Jin, and K. Qiu, “Hybrid chaotic confusion and diffusion for physical layer security in OFDM-PON,” IEEE Photon. J. 9(2), Art. No. 7201010 (2017).
18. Z. Shen, X. Yang, H. He, and W. S. Hu, “Secure transmission of optical DFT-S-OFDM data encrypted by digital chaos,” IEEE Photon. J. 8(3), Art. No. 7904609 (2016).
19. A. A. E. Hajomer, X. Yang, and W. S. Hu, “Secure OFDM transmission precoded by chaotic discrete Hartley transform,” IEEE Photon. J. 10(2), Art. No. 7901209 (2018).
20. M. H. Bi, S. S. Fu, X. F. Zhou, X. L. Yang, S. L. Xiao, and W. S. Hu, “Chaotic nonlinear encryption scheme for CPAs resistance and PAPR reduction in OFDM-PON,” IEEE Photonics Technol. Lett. 29(24), 2147–2150 (2017).
21. M. H. Bi, S. S. Fu, X. F. Zhou, L. Zhang, G. W. Yang, X. L. Yang, S. L. Xiao, and W. S. Hu, “A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON,” IEEE Photon. J. 9(1), Art. NO. 7901510 (2017).
22. C. Zhang, Y. Yan, T. Wu, X. Zhang, G. Wen, and K. Qiu, “Phase masking and time-frequency chaotic encryption for DFMA-PON,” IEEE Photonics J. 10(4), 7203009 (2018).
23. W. Zhang, C. F. Zhang, C. Chen, H. J. Zhang, and K. Qiu, “Brownian motion encryption for physical-layer security improvement in CO-OFDM-PON,” IEEE Photonics Technol. Lett. 29(12), 1023–1026 (2017).
24. X.-L. Chai, Z.-H. Gan, K. Yuan, Y. Lu, and Y.-R. Chen, “An image encryption scheme based on three-dimensional Brownian motion and chaotic system,” Chin. Phys. B 26(2), 99–113 (2017).
25. X. Chai, “An image encryption algorithm based on bit level Brownian motion and new chaotic systems,” Multimedia Tools Appl. 76(1), 1159–1175 (2017).
26. J. Armstrong, “OFDM for optical communication,” J. Lightwave Technol. 27(3), 189–204 (2009).