Secure OFDM Transmission Precoded by Chaotic Discrete Hartley Transform

Volume 10, Number 2, April 2018

Adnan A.E. Hajomer
Xuelin Yang
Weisheng Hu

DOI: 10.1109/JPHOT.2017.2734817
1943-0655 © 2017 IEEE
Secure OFDM Transmission Precoded by Chaotic Discrete Hartley Transform

Adnan A.E. Hajomer, Xuelin Yang, and Weisheng Hu

Shanghai Institute for Advanced Communication and Data Science, State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai 200240, China

DOI:10.1109/JPHOT.2017.2734817

Abstract: We propose a chaotic discrete Hartley transform (DHT) to enhance the physical-layer security and simultaneously improve the transmission performance of optical orthogonal frequency division multiplexing (OFDM) in passive optical network. The theoretical analysis and numerical simulation show that the chaotic DHT precoding matrix after independent row/column permutations can also effectively reduce the peak-to-average power ratio (PAPR) of OFDM signals, which can be generated for OFDM data encryption using digital chaos. The multifold data encryption provides a huge key space of $\sim 10^{178}$ to ensure the physical-layer confidentiality. An encrypted data transmission of 8.9 Gb/s 16-QAM optical OFDM signals is successfully demonstrated over 20 km standard single-mode fiber. Due to the effective reduction in PAPR by the chaotic DHT precoding matrix, the receiver sensitivity is improved by $\sim 1.4$ dB (BER@$10^{-3}$). Moreover, the proposed scheme has low computational complexity, which also provides high spectral efficiency since no additional sideband information is required.

Index Terms: Chaos encryption, optical orthogonal frequency division multiplexing (O-OFDM), passive optical network (PON), discrete Hartley transform (DHT).

1. Introduction

Passive optical network (PON) has been playing an important role in the broadband services driven by the advancement of internet applications [1], because it offers several potential benefits such as high capacity, low cost and energy efficiency [2]. Optical orthogonal frequency division multiplexing (O-OFDM) has been regarded as a promising candidate for next-generation PONs, since it provides unique features such as: tolerance to fiber dispersion, high spectrum efficiency and cost-effectiveness [3]. However, due to the superposition of many independent signals modulated onto individual subcarriers, OFDM signal suffers from high peak-to-average power ratio (PAPR), which is one of the most detrimental factors in OFDM transmission, as it causes power saturation and nonlinear distortion at the optical receiver, and consequently degrades transmission performance [4]. Meanwhile, the broadcasting structure of PON in downstream traffic as well as a large number of subscribers make it fragile and susceptible to be eavesdropped or attacked by illegal optical network units (ONUs) [5]. Thus, the development of secure O-OFDM transmission has become extremely essential and challenging for PONs.
Up to now, the data encryption approaches have been proposed to enhance the physical-layer security for transmission in OFDM-PON, but most of them disregarded the transmission performance improvement [6]–[9]. Several approaches such as chaotic partial transmission sequence (PTS) [10], chaotic selected mapping (SLM) [11], as well as a chaos IQ-encryption optimal frame transmission (IQ-OFT) [12] have been proposed to enhance the physical-layer security, while the O-OFDM transmission performance is improved. However, all of these techniques require a sideband information to transmit the dynamic random partition information or the candidate frame with the minimum PAPR, which reduces the spectral efficiency of transmission. An exception case without the requirement of sideband information is the encryption scheme using chaotic discrete Fourier transform spread OFDM (DFT-S-OFDM) [13], which is one of traditional precoding schemes for PAPR reduction. However, other alternative precoding schemes with lower computational complexity and higher level security have not been explored for secure OFDM transmission in OFDM-PON.

This paper proposes for the first time a chaotic discrete Hartley transform (DHT) to enhance the physical-layer security and jointly to improve the OFDM transmission performance. Both of the theoretical analysis and numerical simulation show that, the chaotic DHT matrix still has the same capability of reducing PAPR of OFDM signals after any row/column permutations within the standard DHT matrix. The new reconfigurable chaotic DHT matrices can be applied as alternative precoders for PAPR reduction as well as for OFDM data encryption. Since the independent row/column permutations in chaotic DHT matrix can be generated and predetermined via a hyper digital chaos, in which a huge key space is created via a multi-fold data encryption. As a result, the transmission performance is improved due to the significant reduction of PAPR by chaotic DHT precoding, which also provides the advantages of lower computational complexity. In addition, higher spectrum efficiency is achieved since no sideband information is required for chaotic DHT precoding scheme. Transmission of 8.9-Gb/s encrypted 16-quadrature amplitude modulation (16-QAM) O-OFDM signals is successfully demonstrated over 20 km standard single-mode fiber (SSMF).

2. Principle
The schematic diagram of the proposed multi-fold OFDM data encryption using chaotic DHT precoding is depicted in Fig. 1, where the multi-fold chaotic encryption are: chaotic row/column permutations of the standard DHT matrix, chaotic subcarrier allocation, and chaotic training sequence (TS) insertion for OFDM symbol time synchronization. Before data encryption, a pseudo-random binary sequence (PRBS) is mapped onto QAM symbols after serial-to-parallel (S/P) conversion. In the proposed scheme, a 4-dimensional (4D) hyper digital chaos is deployed to generate the chaotic sequences [10]

\[
\begin{align*}
\dot{x} &= \zeta(-x + y) + yz u \\
\dot{y} &= \mu(x + y) - xz u \\
\dot{z} &= \eta y - u + \psi xy u \\
\dot{u} &= -\delta u + xyz 
\end{align*}
\]
Fig. 2. Properties of chaotic TS. (a) Auto-correlation for the same initial value $x_0 = 1.528121243912453$; (b) Cross-correlation for different initial values $x_0 = 1.528121243912454$ and $x_0 = 1.528121243912453$.

where $\zeta$, $\mu$, $\eta$, $\psi$ and $\delta$ are real constants. We set $\zeta = 35$, $\mu = 10$, $\eta = 80$, $\psi = 0.5$ and $\delta = 10$ to ensure the system enters into the chaotic zones [10]. The differential equations in (1) are solved by Runge–Kutta method to obtain the chaotic sequences $\{x\}$, $\{y\}$, $\{z\}$ and $\{u\}$. To generate the chaotic vectors $B_x$, $B_y$, $B_z$ and $B_u$ with uniform distribution, each of the chaotic sequences $\{x\}$ can be digitalized and post-processed using [14],

$$B_x = \text{Sort}(x)$$

where the $\text{Sort}$ function returns the index vector $B_x$, according to the ascending order of the values in the chaotic sequence $\{x\}$. Similarly, the other chaotic vectors $B_y$, $B_z$ and $B_u$ can also be obtained.

The procedure of the proposed DHT chaotic encryption is given as follows. The first two permutation vectors $B_x$ and $B_y$ are used to exchange the row and column indexes of the standard DHT matrix respectively. Note that the length of the chaotic sequences $\{x\}$ and $\{y\}$ is $L$, where $L$ is the order of DHT matrix. Assuming the $P_{L \times L}^{(0)}$ is the standard DHT matrix,

$$P_{L \times L}^{(0)} = [\alpha^T(1), \alpha^T(2), \cdots, \alpha^T(L)]$$

where $\alpha(1), \alpha(2), \ldots, \alpha(L)$ are the row vectors and $T$ is the transpose of matrix. After row permutations predetermined on the chaotic vector $B_x$, it becomes

$$P_{L \times L}^{(1)} = [\alpha^T(B_x(1)), \alpha^T(B_x(2)), \cdots, \alpha^T(B_x(L))] = [\beta(1), \beta(2), \cdots, \beta(L)]$$

Similarly, the columns in matrix can also be exchanged depending on the chaotic vector $B_y$, the corresponding chaotic DHT matrix after both of row/column permutations is

$$P_{L \times L}^{(2)} = [\beta(B_y(1)), \beta(B_y(2)), \cdots, \beta(B_y(L))] = [\psi^T(1), \psi^T(2), \cdots, \psi^T(L)]$$

The second encryption is the subcarrier allocation, where the number of OFDM subcarriers is expanded from $L$ to $N$ after zero-padding, while the final subcarrier index is predetermined by the 3rd chaotic vector $B_z$, applied the same way as the DFT precoding scheme described in [13].

Finally, the 4th chaotic vector $B_u$ is adopted to generate the chaotic TS for OFDM symbol time synchronization, which is defined as a random set of $\{-1, 1\}$ [15].

$$\text{TS} = \{(\text{mod} (B_z, 2) - 0.5) \times 2\}$$

where mod ($\alpha$, $\beta$) returns the remainder of $\alpha$ divided by $\beta$. The auto- and cross-correlation (with a tiny difference in the initial values) functions of a chaotic TS are shown in Fig. 2, where the autocorrelation function is similar to the $\delta$ function which provides accurate time synchronization for OFDM symbol.

The secure keys shared between the optical line terminal (OLT) and ONUs in PONs are the initial values in digital chaos. Fig. 3 shows the sensitivity of the digitalized row/column permutation indexes applied in chaotic DHT matrix with respect to a tiny change in the initial values in hyper chaos of (1), which leads to the change in chaotic sequence, then consequently to the change in
the permutation indexes (Y-axis in Fig. 3). Since the digital chaotic sequences have high sensitivity with respect to the initial values ($\sim 1 \times 10^{-15}$, as shown in Fig. 3), exceptional random behavior can be expected using digital chaos [10]. It should be noted that, the encryption key can be sent via additional secure channel, for instance, using quantum key distribution (QKD) to share.

To evaluate the secure reliability of the proposed multi-fold chaotic DHT encryption, the total key space can be calculated. First, the permutations of row/column in chaotic DHT matrix produce a key space of $(L!)^2$. Second, the subcarrier allocation creates a key space of $N!$, where $N$ is the number of subcarriers before IFFT. Third, the chaotic TS for OFDM symbol synchronization increases the key space by a factor of $\sim 10$, because an illegal ONU has to try $(N_0 + N)/N_0$ times on average to realize correct synchronization and demodulation, where $N_0$ is the length of cyclic prefix times which is set to be 1/8 of the OFDM symbol length [10]. In total, a key space with the size of $\sim L! \times L! \times N! \times 10$ is created, which ensure the capability of the proposed chaotic DHT encryption against any exhaustive trials [16].

3. PAPR Reduction by Chaotic DHT Matrix

The standard DHT matrix is widely applied as a precoder for PAPR reduction of OFDM signals. It is necessary to analyze the capability of PAPR reduction for a reconfigurable chaotic DHT matrix after row/column permutations. By definition, a standard DHT matrix $D_{n \times n}$ is an orthogonal matrix [17]

$$DD = DD^T = D^T D = nI$$  \hspace{1cm} (7)

$$d_{km} = \sin (2\pi km/n) + \cos (2\pi km/n), \hspace{0.5cm} k, m = 1, 2, \ldots, n$$  \hspace{1cm} (8)

Assuming $Q_{n \times n}$ and $R_{n \times n}$ are the row and column permutation matrices operating on the standard DHT matrix respectively, then the chaotic DHT matrix $P_{n \times n}$ becomes

$$P = QDR \hspace{1cm} P^T = R^T D^T Q^T$$  \hspace{1cm} (9)

$$PP^T = QD (RR^T)D^T Q^T = QDID^T Q^T = QnIQ^T = nI$$  \hspace{1cm} (10)

where $RR^T = I$ and $QQ^T = I$, since they are orthogonal matrices. From (10), it is proved that, the chaotic DHT matrix still has the orthogonality, which implies that it can also be applied as an alternative precoder for OFDM transmission. The PAPR is defined as the ratio between the maximum peak-to-average power of OFDM signals,

$$PAPR = 10 \log \max[|x(t)|^2 / E(|x(t)|^2)]$$  \hspace{1cm} (11)

where $E(\cdot)$ denotes the expectation. The magnitude of PAPR can also be represented in terms of the peak factor ($\gamma$), which is the square root of PAPR [18]. To specify the PAPR reduction capability
of chaotic DHT matrix, the upper bound of peak factor is

\[ \gamma \leq 1 + \frac{2}{N} \sum_{n=1}^{N} |\rho_n|, \quad \rho_n = \sum_{l=1}^{N-n} a_l a_{l+n}, \quad n = 1, 2, \ldots, N - 1 \]  

where \( \rho_n \) are the aperiodic autocorrelation coefficients, and \( a_n \) is the QAM sequence. (12) shows that, the peak factor of OFDM signals reduces if the value of the autocorrelation coefficients of the corresponding QAM sequence decreases.

The capability of PAPR reduction via chaotic DHT precoding can be verified through the autocorrelation coefficients defined in (12), as shown in Fig. 4, where 64 OFDM symbols of 16-QAM are applied. Compared with the un-precoded original OFDM signals, the autocorrelation curves have shown lower sidelobe for the cases of the chaotic and standard DHT precoding. Moreover, the sidelobe shape is exact the same for both of the standard and chaotic DHT matrices.

The complementary commutative distribution functions (CCDFs) of PAPR are plotted in Fig. 5 for the cases of chaotic DHT precoding, standard DHT precoding and un-precoded original OFDM signals (1000 OFDM symbols). The PAPR reduction is \( \sim 1.8 \text{ dB (CCDF@10}^{-2}\) for either the standard or chaotic DHT precoding, if compared to the un-precoded original OFDM signals. In addition, the CCDF curves are exact the same for the standard and chaotic DHT, which again verifies our previous theoretical analysis.

In summary, the chaotic DHT matrix can be applied to improve the transmission performance via effective PAPR reduction, and simultaneously to enhance the physical-layer security of OFDM
4. Experimental Results and Discussion

The experimental setup of the secure OFDM transmission with chaotic DHT precoding is shown in Fig. 6, where intensity modulation and direct detection were applied in the experiments. At OLT, the IFFT size was 256, in which 64 subcarriers were used for data transmission, while the rest 64 subcarriers were filled by the complex conjugate of the corresponding 64 subcarriers to satisfy the requirement of Hermitian symmetry for direct detection. It should be noted that, the proposed encryption scheme does not limit the number of applied subcarriers, more than 64 subcarriers can be used in order to maximize the data rate. After the parallel-to-serial (P/S) conversion, a cyclic prefix of 1/8 length of OFDM symbol was added into each OFDM symbol. The effective net data rate was 8.9 Gb/s (10 Gs/s × 4 × 64/256/(1 + 1/8)) and the electrical bandwidth was 2.5 GHz (10 GHz/256 × 64). A chaotic TS was inserted for OFDM symbol synchronization. The encrypted O-OFDM signals were generated via an arbitrary waveform generator (AWG, Tektronix AWG7122C). A continuous-wave (CW) laser of the central wavelength at 1550 nm and the linewidth of 100 kHz was used as the optical carrier. A 10 GHz Mach-Zehnder Modulator (MZM, $V_{\pi} = 4$ V) with a fixed bias voltage at its quadrature point was used to convert electrical signals into optical. The double sideband O-OFDM signals with a launch power of $-7$ dBm were transmitted over 20 km standard single-mode fiber (SSMF). At ONU, the signals were received via a photodiode of 10 GHz bandwidth and recorded by a 20 Gs/s real-time oscilloscope for offline processing.

The transmission performance of the chaotic DHT precoded O-OFDM signals was evaluated by the bit error rate (BER) measurements of 128 OFDM symbols, for the cases of the back-to-back (B2B) and transmission after 20 km SSMF, as shown in Fig. 7. The BER was improved $\sim 1.4$ dB (BER@$10^{-3}$) in receiver sensitivity after using chaotic DHT precoding, if compared with the un-precoded OFDM signals. This improvement can be attributed to the precoding gain from the chaotic DHT, since BER was also improved even for the case of B2B. Since the bandwidth of OFDM signal was relatively narrow, the effect of the chromatic dispersion is negligible for the case of 20 km SSMF. Furthermore, it’s obviously that the BER performance for the original and chaotic DHT is exactly same, which could be attributed to the effective PAPR reduction using chaotic and non-chaotic DHT.

To analyze the high secure sensitivity of the encryption scheme using chaotic DHT precoding, the BERs are given with respect to the mismatched row/column indexes in chaotic DHT matrices, for either a wrong $B_x$ (in Fig. 8(a)) or $B_y$ (in Fig. 8(b)). As shown in Fig. 8, only one pair of wrong column/row indexes in the chaotic DHT matrix will make the BER higher than the FEC threshold, where the received optical power is set at $-19$ dBm. It implies that, the original data cannot be correctly recovered by the illegal attackers via any exhaustive attacks, owing to the high sensitivity of the initial values in hyper chaos.
The robustness of the multi-fold encryption of the proposed encryption scheme can also be evaluated via the number of key space. First, the chaotic DHT matrix created a key space of $64! \times 64! \approx 10^{178}$, where 64 is the dimension of DHT matrix. Second, the subcarrier allocation provided a key space of $128! \approx 10^{215}$. Finally, the chaotic TS further increased the key space by a factor of $\sim 10$. In total, the key space of $\sim 10^{394}$ was achieved by the chaotic DHT encryption scheme in the experiment. Thus, to obtain the correct key through exhaustive brute-force trials by the available fastest computing speed ($\sim 2.5 \times 10^{13}$ Hz) [10], the computation time will be $\sim 10^{372}$ years.

For the comparison of the chaotic DHT with DFT precoding schemes, the chaotic DHT has two advantages. First, as shown in Table 1, the DHT precoding lowers the multiplication complexity by a factor of two if compared with DFT, since DHT matrix has only real elements. Second, in terms of computation complexity, the DHT precoding is more efficient than the DFT.

### Table 1

<table>
<thead>
<tr>
<th></th>
<th>DHT</th>
<th>PFT [11]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Real Multiplications</strong></td>
<td>$2L^2$</td>
<td>$4L^2$</td>
</tr>
<tr>
<td><strong>Complex Addition</strong></td>
<td>$L(L-1)$</td>
<td>$L(L-1)$</td>
</tr>
</tbody>
</table>

Fig. 7. BERs of the encrypted O-OFDM transmission using chaotic DHT precoding.

Fig. 8. BERs versus the (a). row and (b). column index mismatches in chaotic DHT matrix.
of key space, the independent row/column permutations in the chaotic DHT provides a huge key space of \((L!)^2\), which is much higher than that of \((L/0.01)^2\) for the case of chaotic DFT [13], where 0.01 is the sensitivity of the chaotic reconfigurable parameters that results in significant degradation in BER.

In addition, if compared with the previous similar chaotic encryption schemes such as PTS [10], SLM [11] and IQ-OFT [12], the proposed chaotic DHT scheme provides a higher spectral efficiency, since it does not require any sideband information. Table 2 shows the corresponding sideband information that has to be transmitted for these alternative approaches, in terms of the number of bits per OFDM symbol. The number of bits required for each OFDM symbol also increases with respect to the number of sub-blocks and the phase sequences. Consequently, better PAPR performance in these schemes leads to stronger degradation in the spectral efficiency in transmission.

### Table 2
Sideband Information Requirement for the Chaotic Secure Schemes

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits/OFDM symbol</td>
<td>NONE</td>
<td>([V\log_2 W])</td>
<td>([\log_2 W])</td>
<td>([\log_2 W])</td>
</tr>
</tbody>
</table>

\(V\) is number of sub blocks, \(W\) is the number of the phase factors. \(|x|\) denotes the greatest integer less than \(x\).

5. Conclusion

We have proposed and demonstrated a data encryption scheme for OFDM transmission using chaotic DHT precoding, which enhances the physical-layer security with a huge key space and jointly improves the transmission performance by effective PAPR reduction. The high-level security is achieved via the multi-fold chaotic encryption in OFDM signals including: the chaotic DHT via two independent row/column permutations, chaotic subcarrier allocation as well as chaotic TS insertion, which creates a total key space of \(\sim 10^{394}\). An 8.9-Gb/s encrypted OFDM transmission precoded by the chaotic DHT has been successfully demonstrated, where the receiver sensitivity is improved by \(\sim 1.4\) dB (BER@10\(^{-3}\)). In addition, the chaotic DHT precoding scheme has the advantages of low computation complexity and high spectral efficiency. It could be a promising security solution for next-generation OFDM-PON.

References


