Security enhancement for OFDM-UWOC system using three-layer chaotic encryption and chaotic DFT precoding

Huan Deng (邓 欢)[1], Zihao Du (杜子豪)[1], Jianmin Xiong (熊建民)[1], Xingqi Yang (杨兴启)[1], Yan Hua (华 岩)[1], and Jing Xu (徐 敬)[1,2*]

[1] Optical Communications Laboratory, Ocean College, Zhejiang University, Zhoushan 316021, China

[2] Key Laboratory of Ocean Observation-Imaging Testbed of Zhejiang Province, Ocean College, Zhejiang University, Zhoushan 316021, China

*Corresponding author: jxu-optics@zju.edu.cn

Received April 21, 2022 | Accepted May 31, 2022 | Posted Online July 5, 2022

Security is one of the key issues in communications, but it has not attracted much attention in the field of underwater wireless optical communication (UWOC). This Letter proposes a UWOC encryption scheme with orthogonal frequency division multiplexing (OFDM) modulation, based on the three-layer chaotic encryption and chaotic discrete Fourier transform (DFT) precoding. The three-layer chaotic encryption processes are bit stream diffusion, in-phase/quadrature encryption, and time-frequency scrambling. With multi-fold data encryption, the scheme can create a keyspace of 9.7×10^{179}, effectively resisting brute force attacks and chosen-plaintext attacks. A 3 Gbit/s encrypted OFDM signal is successfully transmitted over a 7 m water channel.

Keywords: security; underwater wireless optical communication; chaotic encryption; chosen-plaintext attacks.

DOI: 10.3788/COL202220.110601

1. Introduction

To meet the increasing demand for underwater activities, such as ocean explorations and rescue missions, underwater wireless sensor networks (UWSNs)[1] are expected to be widely used in the near future. Underwater radio frequency (RF) signals are critically attenuated, and the transmission rate of underwater acoustic communication (UAC) is very low. By contrast, underwater wireless optical communication (UWOC) has the characteristics of high bandwidth and low latency, which plays a significant supplementary role in fulfilling the requirements of UWSNs.

UWOC is customarily regarded as highly secure compared with UAC since the light source is highly directional and has limited penetration distance in common waters[2,3]. Thus, UWOC has been investigated less to figure out and solve potential security issues, and its research activities mainly focus on improving data rate, transmission distance, and link alignment[4–6]. From a wireless coverage perspective, security and privacy are also important in accessing information[7].

A UWOC system does not inherently provide a secure transmission link, making it easy for attackers to capture information. In seawater, especially for long-reach transmission, the scattering effect will make the received light spot much larger than the detection area, thereby increasing the risk of signal eavesdropping[2]. Besides, eavesdroppers can place a mirror or diffraction grating[8] somewhere between the transmitter and receiver to tap light from the line-of-sight beam. To reduce the difficulty of alignment, an omni-directional light source[9] and a wide-beam laser diode (LD)[10] are also widely used in UWOC, which undoubtedly increase the probability of information leakage. Simultaneously, potential attackers may also use the non-line-of-sight channel formed by the scattered light[11,12] with increased concealment. Currently, there are not many solutions available to address UWOC security. Underwater quantum communication generally supports a low communication rate (<1 kbit/s)[13–15]. References [16,17] used phase deflection and a higher-order modulated stream to encrypt data, respectively. Chaotic encryption technology has excellent pseudo-randomness and sensitivity to initial conditions. In Ref. [18], optical discrete multi-tone (DMT) data was encrypted by digital chaos, which verified the feasibility of chaotic encryption in UWOC. The above-mentioned encryption schemes[16–18] have a low encryption dimension and a small key space, which are vulnerable to attack after statistical analysis. Furthermore, they all failed to consider the extremely threatening chosen-plaintext attacks (CPAs), and thereby they are not enough for higher safety requirements.

In this Letter, we present a security-enhanced orthogonal frequency division multiplexing (OFDM) scheme based on three-layer chaotic encryption and chaotic discrete Fourier transform (DFT) precoding in a UWOC system, which can simultaneously guarantee sufficiently high security and transmission performance. The application of multiple hyperchaotic maps and multi-fold data encryption can improve the key space and reduce the risk of the scrambling method and chaotic model being destroyed by statistical analysis. Multiple hyperchaotic maps generate masking factors, implementing bit stream diffusion encryption, in-phase/quadrature (IQ) encryption, time-frequency dimensional scrambling, and chaotic DFT precoding in OFDM. The chaotic DFT precoding matrix is generated to reduce the peak to average power ratio (PAPR) and bit error rates (BERs). The chaotic DFT precoding matrix is obtained by introducing chaotic sequences into the standard DFT matrix for phase encryption and column permutation. Hence, it is more difficult to crack than the encrypted DFT matrix in Refs. [18,19]. To verify the feasibility of the scheme, a 3 Gbit/s encrypted 16-quadrature amplitude modulation (16-QAM) OFDM signal is successfully demonstrated over a 7 m UWOC link. The encryption system is tested and analyzed to have higher security with a key space of 9.7×10^{179} and can resist brute force attacks (BFAs) and CPAs, achieving the higher confidentiality of information transmission.

2. Principles

The concept of the proposed security-enhanced OFDM system for UWOC based on three-layer chaotic encryption and chaotic DFT precoding is shown in Fig. 1. The key-driven hyperchaotic maps are used to generate masking factors. It has been proved that signals encrypted by low-dimensional chaotic maps are not always safe[20]. Hyperchaotic maps can generate dynamic trajectories with more randomness in high-dimensional space and require more key parameters to recover. Hence, it is much more difficult for eavesdroppers to steal information from hyperchaotic encrypted signals than low-dimensional ones. At the transmitter, the input data is encrypted by bidirectional diffusion and then mapped to QAM for IQ encryption. Subsequently, the OFDM frame is further scrambled in the time-frequency dimension[21,22]. Finally, chaotic DFT precoding is employed to reduce the PAPR. The application of multi-hyperchaotic encryption can effectively hide the original information and increase the keyspace. The signal demodulation and decryption operation at the receiver is the reverse of the transmitter.

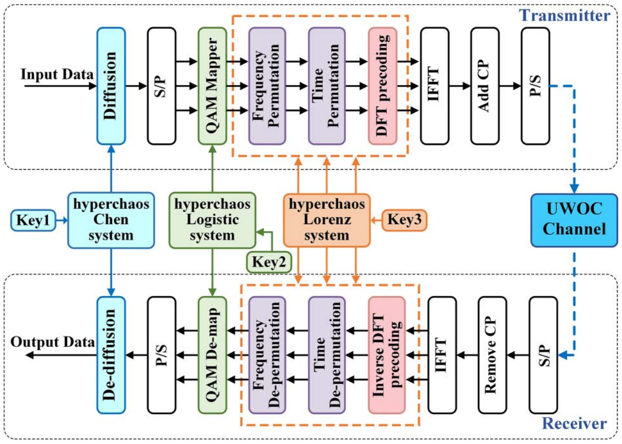

Fig. 1. Block diagram of the secure OFDM-UWOC based on three-layer chaotic encryption and chaotic DFT precoding.

2.1. Diffuse encryption

Bidirectional diffusion in cryptography makes each bit in the plaintext affect many bits in the ciphertext. Here, a four-dimensional (4D) hyperchaotic Chen system is applied to generate chaotic sequences for bidirectional diffusion[23]:

$$\begin{cases} \partial x_1/\partial t = a_1(y_1 - x_1) + u_1 \\ \partial y_1/\partial t = d_1 x_1 - x_1 z_1 + c_1 y_1 \\ \partial z_1/\partial t = x_1 y_1 - b_1 z_1 \\ \partial u_1/\partial t = y_1 z_1 + r_1 u_1 \end{cases}. \tag{1}$$

When $a_1 = 35$, $b_1 = 3$, $c_1 = 12$, $d_1 = 7$, and $0.085 \le r_1 \le 0.798$, the system is in a chaotic state. From Eq. (1), four chaotic sequences $X_1 = \{x_1(i)\}$, $Y_1 = \{y_1(i)\}$, $Z_1 = \{z_1(i)\}$, and $U_1 = \{u_1(i)\}$ can be obtained. Key1 of bidirectional diffusion is $\{r_1 = 0.16, x_1(0) = 1, y_1(0) = 2, z_1(0) = 1, u_1(0) = 1\}$. The specific diffusion process is as follows.

Step 1. Original data and chaotic sequence pre-processing. To improve the efficiency of processing data, the original bit stream is first converted into a data stream P with t ($t = 8$) bits as a unit, and the length of P is denoted as L_P. A new chaotic sequence S_1 is composed of sequences X_1 and Z_1, and the combination process is $S_1 = \{X_1(j), Z_1(j) | j = 1, 2, \ldots, L_P/2\}$. Similarly, Y_1 and U_1 form a new sequence S_2. The sequences S_1 and S_2 have the same length as P, and they are further processed as

$$\begin{cases} K_1(i) = \mathrm{mod}(\mathrm{floor}((|S_1(i)| - \mathrm{floor}(|S_1(i)|)) \times 10^{15}), 2^8) \\ K_2(i) = \mathrm{mod}(\mathrm{floor}((|S_2(i)| - \mathrm{floor}(|S_2(i)|)) \times 10^{15}), 2^8) \end{cases}. \tag{2}$$

The function $\mathrm{mod}(x, 2^8)$ returns the remainder divided by 2^8, $\mathrm{floor}(x)$ is rounding down. K_1 and K_2 sequences, both with the length of L_P, consist of integers in the range of 0 to 255.

Step 2. Utilize K_1 to encrypt the plaintext P by the XOR operation to form the encrypted data C_1:

$$C_1(i) = C_1(i-1) \oplus P(i) \oplus K_1(i), \tag{3}$$

where "$\oplus$" is bitxor operation, and $i = 1, 2, \ldots, L_P$. When $i = 1$ is a particular case, we set $C_1(0)$ to 112 in the experiment.

Step 3. Let $C_1'(0) = C_1(L_P)$ and use Eq. (4) to get bidirectional diffusion of C_1':

$$C_1'(i) = C_1'(i-1) \oplus C_1(i) \oplus K_2(i). \tag{4}$$

Step 2 can diffuse the plaintext into the ciphertext to different degrees but fails to spread globally due to the single direction of the diffusion, and the following plaintext cannot be diffused to the preceding ciphertext. Hence, using bidirectional diffusion, each part of the binary plaintext information is fully diffused into the ciphertext to generate an utterly dynamic ciphertext.

When the plaintext is changed, the entire ciphertext will produce irregular changes, which can effectively resist the CPAs.

2.2. IQ encryption

Then, the first layer of encrypted data C_1' is converted to binary data for QAM mapping to obtain symbol sequence W. The hyperchaotic logistic mapping is used for IQ encryption and is defined as[24]

$$\begin{cases} x_{n+1} = 4\lambda_1 x_n(1 - x_n) + \gamma y_n \\ y_{n+1} = 4\lambda_2 y_n(1 - y_n) + \gamma x_n \end{cases}, \tag{5}$$

where $\gamma = 0.1$, and $\lambda_1, \lambda_2 \in [0.65, 0.9]$. The values of the generated sequences $X_2 = \{x(i)\}$ and $Y_2 = \{y(i)\}$ range from 0 to 1. Key2 of IQ encryption in the second layer is $\{\lambda_1 = 0.9, \lambda_2 = 0.9, x_2(0) = 0.01, y_2(0) = 0.12\}$. To generate IQ-encrypted sequences, the post-processing of X_2 and Y_2 to obtain the sequences R and I is described as

$$\begin{cases} R(i) = 1 - \text{round}(X_2(i)) \times 2 \\ I(i) = 1 - \text{round}(Y_2(i)) \times 2 \end{cases}, \tag{6}$$

where $R(i), I(i) \in \{-1, 1\}$, and two sequences R and I are used to encrypt the real and imaginary parts of the QAM symbol, respectively.

The encryption for the kth QAM symbol W_k in the symbol sequence can be expressed as

$$C_2(k) = \text{Re}(W_k) \cdot R(k) + j \cdot \text{Im}(W_k) \cdot I(k). \tag{7}$$

2.3. Time-frequency dimensional scrambling

After completing the IQ encryption in the second layer, the OFDM frames are scrambled in the time-frequency dimension[21,22], as shown in Fig. 2. The third layer of encryption and chaotic DFT precoding apply a hyperchaotic Lorenz system, which is defined as follows[25]:

$$\begin{cases} \partial x_3/\partial t = a_3(-x_3 + y_3) \\ \partial y_3/\partial t = c_3 x_3 - y_3 - x_3 z_3 + u_3 \\ \partial z_3/\partial t = x_3 y_3 - b_3 z_3 \\ \partial u_3/\partial t = -d_3 x_3 \end{cases}, \tag{8}$$

where $a_3 = 10$, $b_3 = 8/3$, $c_3 = 28$, and $d_3 \in [0, 21.75]$, and key3 is $\{d_3 = 5, x_3(0) = 3.5, y_3(0) = 2.2, z_3(0) = 1.7, u_3(0) = 4.6\}$. Four chaotic sequences X_3, Y_3, Z_3, and U_3 are generated by Eq. (8). X_3 is used for frequency-domain (row) permutation, and Y_3 is applied for time-domain (column) permutation. The dimension of sequences X_3 and Y_3 is $M \times L$, where M is the number of effective subcarriers, and L is the number of symbols effectively transmitted in the OFDM frame.

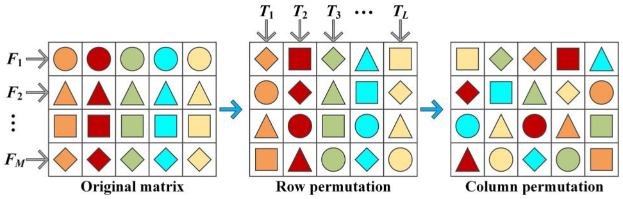

Fig. 2. Schematic diagram of time-frequency scrambling[21].

The data matrix after IQ encryption can be expressed as

$$Q_{M\times L} = \begin{bmatrix} Q_{11} & Q_{12} & \cdots & Q_{1L} \\ Q_{21} & Q_{22} & \cdots & Q_{2L} \\ \vdots & \vdots & & \vdots \\ Q_{M1} & Q_{M2} & \cdots & Q_{ML} \end{bmatrix} = \begin{bmatrix} F_1 \\ F_2 \\ \vdots \\ F_M \end{bmatrix}. \tag{9}$$

Equation (9) defines the row vectors of the data matrix as $F_1, F_2, \ldots, F_M$. Before the time-frequency permutation, the sequence X_3 is partitioned into L parts, and then each part is ranked in ascending order separately to return and record the dynamic indices. L position index sequences obtained by X_3 are used to reorder the frequency-domain data of the L OFDM symbols, respectively, to realize row scrambling operation. The frequency-domain scrambled matrix can be represented by column vectors $T_1, T_2, \ldots, T_L$. The same operation is used to process Y_3 to obtain M position index sequences and then scramble time-domain data of M subcarriers, respectively. Time-frequency permutation is similar to bit interleaving, which can reduce the BER to some extent in the case of burst noise.

2.4. Chaotic DFT precoding

In this work, chaotic DFT precoding is adopted to reduce PAPR and increase the security of UWOC additionally[18]. Chaotic DFT precoding can be realized by applying a combination of row–column phase encryption and column scrambling to the conventional DFT precoding matrix. The conventional DFT precoding matrix D can be defined as[19]

$$D_{m,l} = \frac{1}{\sqrt{M}} e^{-j2\pi(m-1)(l-1)/M}, \qquad 0 \le m, \quad l \le M - 1, \tag{10}$$

where m and l are the row and column index of the standard DFT matrix:

$$D^p_{m,l} = \frac{1}{\sqrt{M}} e^{-j2\pi(m - Z_3(l))(l-\alpha)/M}, \qquad 0 \le m, \quad l \le M - 1. \tag{11}$$

According to the above equation, the standard DFT matrix of $M \times M$ is row-phase encrypted using M different values in the sequence Z_3 generated by Eq. (8), i.e., each row is subtracted by a different value $Z_3(l)$, while the column-phase is encrypted using a constant $\alpha = 6.35$, which is from Z_3. Finally, the sequence U_3 is used to perform a column scrambling on the whole of the phase encrypted DFT matrix D^p to obtain our final chaotic encrypted DFT matrix D^{pc}. Column scrambling of the DFT matrix is equivalent to input data scrambling.

Table 1. The Computation Complexity of Encryption Schemes.

	Our Scheme	Ref. [20] (with DFT-S)	Ref. [18]
Real-valued multiplication	0	N^2	0
Complex-valued multiplication	$M^2 + N^2$	M^2	$M^2 + N^2$
Addition	$M(M-1) + N(N-1)$	$3M(M-1) + 2M \times (2M-1) + N(N-1)$	$M(M-1) + N(N-1)$

Table 2. The Computation Complexity of Chaos Systems.

	Our Chaotic Systems	7D Chaos (Ref. [20])	Chaos Maps (Ref. [18])
Addition	104	221	5
Multiplication	110	118	10
Sine function	0	4	2

Compared with other single and common chaotic mappings, the multiple hyperchaotic mappings used have more dimensions, leading to increased complexity and security of the UWOC encryption system, similar to the seven-dimensional (7D) chaotic mappings applied in Ref. [20]. However, once the encryption system is implemented in practical applications, we do not need to iterate multiple hyperchaotic systems or update the key sequence frequently until the key of the UWOC system changes. In this case, the major computation complexity would only come from the encryption at the system level[18,20], as shown in Table 1. Here, the number of effective subcarriers is set to M, the inverse fast Fourier transform (IFFT) size is N, and only one OFDM symbol is used. In contrast, if we want to change the security key frequently to enhance the security of the UWOC further, the computational complexity of the hyperchaotic mapping iterations needs to be considered, as shown in Table 2.

As mentioned above, there is a trade-off between security and complexity. It is worth mentioning that the UWOC encryption method in this Letter does not introduce any additional optical modules, and all of the encryption and decryption operations are performed in the digital signal processing (DSP), so the impact of the iterations of chaotic mapping is small[26,27]. Moreover, an extra layer of encryption for communication systems represents an additional security guarantee. We believe that the study of using multiple hyperchaotic mappings to encrypt UWOC systems is worthwhile.

3. Experimental Setup

The experimental setup of the proposed high-security OFDM system for UWOC based on three-layer chaotic encryption and chaotic DFT precoding is shown in Fig. 3. At the transmitter, the bit streams are encrypted and loaded into an arbitrary waveform generator (AWG, Tektronix 70002A) at a sampling rate of 3.125 GSamples/s. The voltage amplitude of the output signal is appropriately adjusted using an amplifier (AMP) and a variable electronic attenuator (ATT). Subsequently, the encrypted signal is superimposed on a bias tee (Bias-T) with a direct current (DC) of 0.3414 A, so that the drive signal operates within the linear region of the blue LD. The blue light is collimated by a collimating lens (CL) and emitted into a 7 m water tank filled with tap water. At the receiver, the blue light is incident on an avalanche photodiode (APD210) after passing through a focusing lens (FL) and a variable optical ATT (VOA). Finally, the detected encrypted signals are captured via a mixed

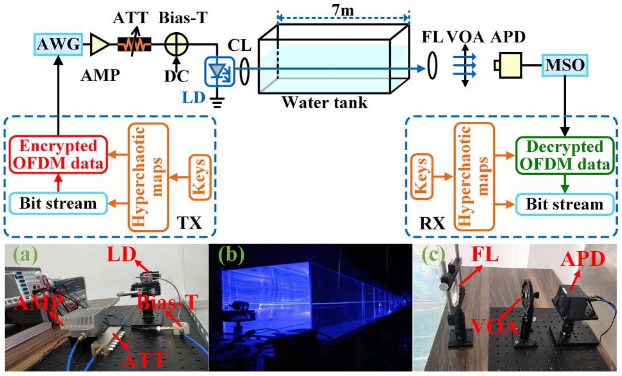

Fig. 3. Experimental setup. Insets: (a) the transmitter module, (b) the water tank, and (c) the receiving module.

Table 3. Parameters of the OFDM-UWOC System.

OFDM Parameters	Values
Modulation format	16-QAM
Number of effective subcarriers	256
Inverse fast Fourier transform (IFFT) size	1024
Number of cyclic prefix (CP)	64
Number of subcarriers for gap near DC	8
Number of OFDM symbols	520

signal oscilloscope (MSO, Tektronix MSO71254C) at a sampling rate of 25 GSamples/s and processed offline by a personal computer (PC). The final data transmission rate is about 3 Gbit/s. Table 3 shows the detailed OFDM parameters of the UWOC system.

4. Performance and Safety Analysis

The PAPR and BER are utilized to evaluate the performance of our encryption scheme. Besides, image transmission is a typical digital communication application, so we tested the encryption scheme with image data to visualize the encryption performance. The complementary cumulative distribution functions (CCDFs) of PAPRs for the original and encrypted data are shown in Fig. 4.

The PAPR decreases along with the auto-correlation coefficient of the input data reduction before the N-IFFT operation[19]. Figure 4 shows that the chaotic DFT matrix can significantly reduce the PAPR of the original image and the three-layer encrypted data. Compared with the original image using the standard DFT method, the chaotic DFT scheme obtains a PAPR reduction of about 1.7 dB (CCDF: 1×10^{-3}) owing to multiple scrambling operations. The PAPR performance of the image data after three-layer chaotic encryption is very close to that of the pseudo-random bit sequence (PRBS), where the order of PRBS is 26. Due to the relatively low auto-correlation of encrypted data, both the chaotic DFT and standard DFT matrix can achieve a PAPR reduction of about 2.6 dB (CCDF: 1×10^{-3}). In Fig. 5(b), the BERs of the three-layer encrypted data using standard DFT and chaotic DFT are almost the same.

It can be further verified that our scheme can be used in UWOC with high confidentiality and solid BER performance. Figure 5 shows BER curves and constellation diagrams of the original image and the encrypted data. The legal receiver can correctly recover the data using the correct private key. In contrast, illegal receivers always obtain a BER of about 0.5 and cannot decrypt the message, even if they obtain most of the correct key, with only a slight difference of 10^{-15} from $y_1(0)$ of key1. In the case of BFAs, the attacker receives an annulary distributed constellation since the chaotic DFT has the effect of phase encryption, as in Fig. 5(a), which perceives the encryption operation in the UWOC link. In general, the attacker utilizes all possible methods to restore the normal constellation diagram. However, the proposed UWOC system is still highly secure with multiple chaotic encryptions because they cannot easily detect the encryption operations in the bit stream, QAM, and time-frequency domain.

The randomness of chaotic systems and their high sensitivity to initial conditions are the basis of our encryption algorithm.

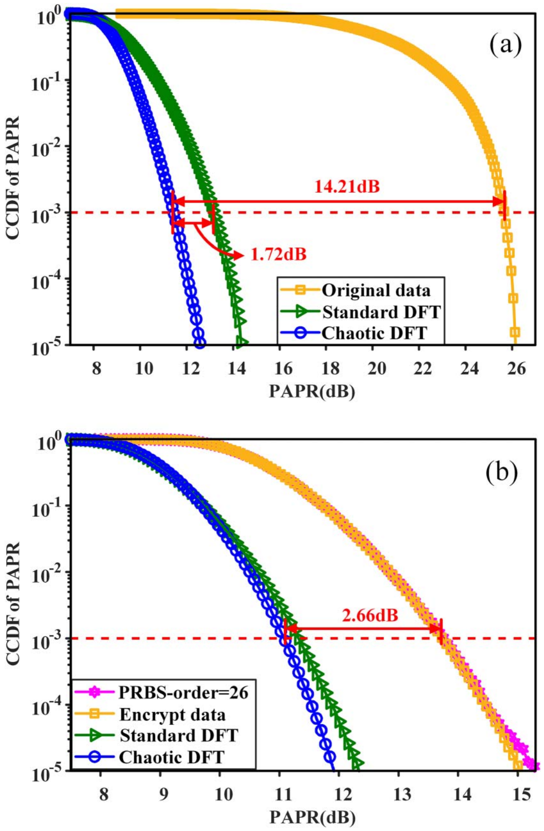

Fig. 4. Performance of PAPR for (a) original image data and (b) three-layer encrypted data under different conditions.

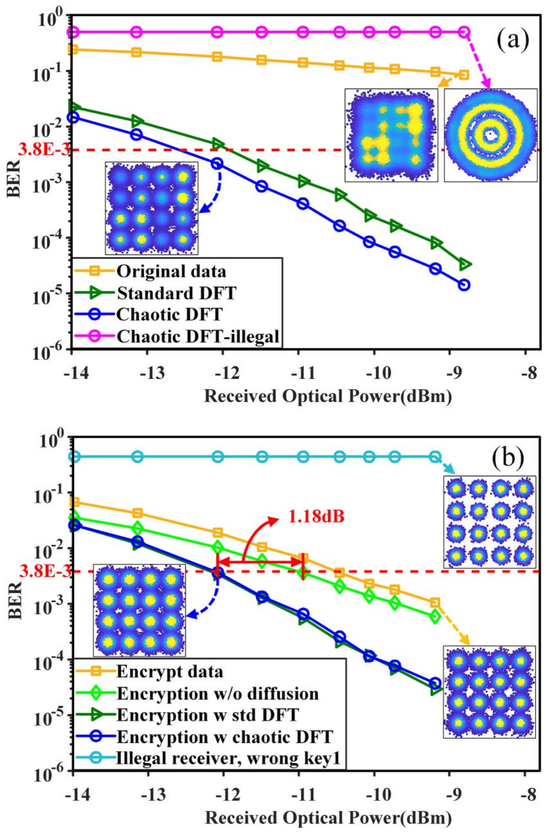

Fig. 5. BER curves of normal and illegal receiver for (a) original image data and (b) three-layer encrypted data.

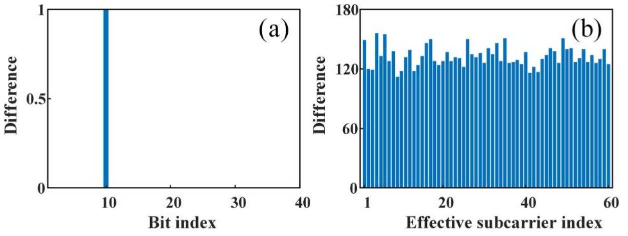

Fig. 6. (a) Change 1 bit in plaintexts. (b) The difference of ciphertext change on the first 60 OFDM subcarriers.

Multiple hyperchaotic mappings can create a larger key space and increase the difficulty for attackers to crack. According to the Institute of Electrical and Electronics Engineers (IEEE) floating-point standard[28], the computational precision of a 64 bit double-precision number is approximately 10^{-15}. Thus, the key space of the whole encryption system can be approximately calculated as $(0.798 - 0.085) \times 10^{15} \times (10^{15})^4 \times [(0.9 - 0.65) \times 10^{15}]^2 \times 21.75 \times 10^{15} \times (10^{15})^4 = 9.6923 \times 10^{179}$. It takes at least 9.08×10^{155} years to obtain the correct key by exhaustive enumeration with the 3.386×10^4 TFlop/s computation speed of the Tianhe-2 supercomputer[18]. The key space of our encryption method is large enough to resist BFAs.

It is worth noting that two-layer encryption without diffusion has a better BER performance than three-layer encryption in Fig. 5(b). Owing to the XOR operation in the diffusion, which associates the front and back plaintexts, noise accumulation will happen when the ciphertext is decrypted. However, diffusion encryption can generate dynamic ciphertexts to resist the most threatening and aggressive CPAs, so the performance penalty is acceptable. In this paper, to obtain higher information security and ensure transmission performance, chaotic DFT precoding is adopted to compensate for the loss, even improving the reception sensitivity by about 1 dB.

To verify the anti-CPA ability of our encryption system, we give the variations of the ciphertext when changing 1 bit of the plaintext, as shown in Fig. 6. The 10th bit of the original binary plaintext has been changed in Fig. 6(a). Figure 6(b) indicates great difference between the new ciphertext obtained after the corresponding plaintext change and the original one in the same OFDM subcarrier, implying that the plaintext information has been sufficiently spread out to nearly all the data during the ciphertext generation process in the OFDM-based UWOC system. For clarity, Fig. 6(b) only shows the difference of ciphertext change on the first 60 OFDM subcarriers. Consequently, the proposed encryption system can mix up the relationship between the original data and the ciphertext to resist CPAs.

5. Conclusion

In this Letter, we have proposed a security-enhanced OFDM scheme for UWOC using three-layer chaotic encryption and chaotic DFT precoding. Although there is a trade-off between security and system complexity, the experiment in this paper validates the transmission performance and feasibility of this scheme, which is also an additional way to achieve UWOC secure transmission. The three-layer encryption operations of OFDM symbols are diffusion, IQ encryption, and time-frequency scrambling in turn. Finally, chaotic DFT precoding compensates for BER deterioration, and the key space reaches 9.7×10^{179}. Our encryption system can resist BFAs, statistical attacks, and CPAs, which has great potential for UWOC systems in the future with higher security requirements.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (NSFC) (No. 61971378), Strategic Priority Research Program of the Chinese Academy of Sciences (No. XDA22030208), and Zhoushan-Zhejiang University Joint Research Project (No. 2019C81081).

References

1. A. Khasawneh, M. S. Bin Abd Latiff, O. Kaiwartya, and H. Chizari, “Next forwarding node selection in underwater wireless sensor networks (UWSNs): techniques and challenges,” Information **8**, 3 (2016).
2. M. Kong, J. Wang, Y. Chen, T. Ali, R. Sarwar, Y. Qiu, S. Wang, J. Han, and J. Xu, “Security weaknesses of underwater wireless optical communication,” Opt. Express **25**, 21509 (2017).
3. S. Jiang, “On securing underwater acoustic networks: a survey,” IEEE Commun. Surv. Tutor. **21**, 729 (2019).
4. Y. Huang, C. Tsai, Y. Chi, D. Huang, and G. Lin, “Filtered multicarrier OFDM encoding on blue laser diode for 14.8-Gbps seawater transmission,” J. Light. Technol. **36**, 1739 (2018).
5. J. Wang, C. Lu, S. Li, and Z. Xu, “100 m/500 Mbps underwater optical wireless communication using an NRZ-OOK modulated 520 nm laser diode,” Opt. Express **27**, 12171 (2019).
6. J. Lin, Z. Du, C. Yu, W. Ge, W. Lü, H. Deng, C. Zhang, X. Chen, Z. Zhang, and J. Xu, “Machine-vision-based acquisition, pointing, and tracking system for underwater wireless optical communications,” Chin. Opt. Lett. **19**, 050604 (2021).
7. M. Gao, C. Li, and Z. Xu, “Performance enhancement of LED-based indoor OFDM-VLC system using digital chaotic scheme,” Opt. Commun. **439**, 21 (2019).
8. D. Shaboy, D. Rockban, and A. Handelman, “Tapping underwater wireless optical communication in pure water and natural dead-sea ultra-high-salinity water by diffraction grating,” Opt. Express **26**, 29700 (2018).
9. G. Baiden, Y. Bissiri, and A. Masoti, “Paving the way for a future underwater omni-directional wireless optical communication systems,” Ocean Eng. **36**, 633 (2009).
10. X. Sun, M. Kong, O. A. Alkhazragi, K. Telegenov, M. Ouhssain, M. Sait, Y. Guo, B. H. Jones, J. S. Shamma, T. K. Ng, and B. S. Ooi, “Field demonstrations of wide-beam optical communications through water-air interface,” IEEE Access **8**, 160480 (2020).
11. X. Sun, W. Cai, O. Alkhazragi, E.-N. Ooi, H. He, A. Chaaban, C. Shen, H. M. Oubei, M. Z. M. Khan, T. K. Ng, M.-S. Alouini, and B. S. Ooi, “375-nm ultraviolet-laser based non-line-of-sight underwater optical communication,” Opt. Express **26**, 12870 (2018).
12. X. Sun, M. Kong, O. Alkhazragi, C. Shen, E. N. Ooi, X. Zhang, U. Buttner, T. K. Ng, and B. S. Ooi, “Non-line-of-sight methodology for high-speed wireless optical communication in highly turbid water,” Opt. Commun. **461**, 125264 (2020).
13. Y. Chen, W. G. Shen, Z. M. Li, C. Q. Hu, Z. Q. Yan, Z. Q. Jiao, J. Gao, M. M. Cao, K. Sun, and X. M. Jin, “Underwater transmission of high-dimensional twisted photons over 55 meters,” PhotoniX **1**, 5 (2020).
14. S. Zhao, W. Li, Y. Shen, Y. H. Yu, X. H. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu, “Experimental investigation of

quantum key distribution over water channel," Appl. Opt. **58**, 3902 (2019).

15. L. Ji, J. Gao, A.-L. Yang, Z. Feng, X.-F. Lin, Z.-G. Li, and X.-M. Jin, "Towards quantum communications in free-space seawater," Opt. Express **25**, 19795 (2017).
16. J. Zhang, G. Gao, and B. Wang, "Spectrum spreading and encryption of underwater optical OFDM communication," in *Asia Communications and Photonics Conference/International Conference on Information Photonics and Optical Communications (ACP/IPOC)* (2020), paper M4A.284.
17. Y. Shang, W. Mao, M. Han, C. Xu, and G. Gao, "Underwater wireless optical communication with high modulation level based stream cipher," in *Asia Communications and Photonics Conference (ACP)* (2018), paper Su2A.247.
18. J. Du, Y. Wang, C. Fei, R. Chen, G. Zhang, X. Hong, and S. He, "Experimental demonstration of 50-m/5-Gbps underwater optical wireless communication with low-complexity chaotic encryption," Opt. Express **29**, 783 (2021).
19. Z. Shen, X. Yang, H. He, and W. Hu, "Secure transmission of optical DFT-S-OFDM data encrypted by digital chaos," IEEE Photon. J. **8**, 7904609 (2016).
20. Z. Hu and C. K. Chan, "A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON," J. Light. Technol. **36**, 3373 (2018).
21. M. Bi, X. Fu, X. Zhou, L. Zhang, G. Yang, X. L. Yang, S. Xiao, and W. Hu, "A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON," IEEE Photon. J. **9**, 7901510 (2017).
22. B. Liu, L. Zhang, X. Xin, and Y. Wang, "Physical layer security in OFDM-PON based on dimension-transformed chaotic permutation," IEEE Photon. Technol. Lett. **26**, 127 (2014).
23. T. Wu, C. Zhang, H. Wei, and K. Qiu, "PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM," Opt. Express **27**, 27946 (2019).
24. D. Chen, D. Qing, and D. Wang, "AES key expansion algorithm based on 2D logistic mapping," in *Fifth International Workshop on Chaos-fractals Theories and Applications* (2012), p. 207.
25. G.-Y. Wang, Y. Zheng, and J.-B. Liu, "A hyperchaotic Lorenz attractor and its circuit implementation," Acta. Phys. Sin. **56**, 3113 (2007).
26. Z. Hu, P. Song, and C. K. Chan, "Chaotic non-orthogonal matrix-based encryption for secure OFDM-PONs," IEEE Photon. Technol. Lett. **33**, 1127 (2021).
27. R. Tang, B. Liu, Y. Mao, R. Ullah, J. Ren, X. Xu, J. Zhao, M. Li, S. Chen, and Y. Han, "High security OFDM-PON based on an iterative cascading chaotic model and 4-D joint encryption," Opt. Commun. **495**, 127055 (2021).
28. IEEE, "Standard for binary floating-point arithmetic," IEEE Std. 754 (1985).