Bidirectional high-speed chaotic communication system based on an all-optical time-delay feedback loop

Jing-Yang Liu,a Xue-Fang Zhou ,a,b,* Miao Hu,a and Qi-Liang Li a
aHangzhou Dianzi University, School of Communication Engineering, Hangzhou, China
bHangzhou Dianzi University, School of Cyberspace, Hangzhou, China

Abstract. A bidirectional high-speed chaotic optical communication scheme with physical layer encryption is proposed and studied theoretically. The external cavity optical feedback method is analyzed. An erbium-doped fiber amplifier is used to represent the all-optical delay feedback loop of the traditional external cavity; it can overcome the shortcomings of the traditional method such as lower precision and high equipment volume requirements. The bidirectional communication scheme is discussed; it sets the encryption device at the transmitter, uses the correlation between the two encryption signals to decrypt, and cancels the decryption device at the receiver, which not only simplifies the experimental equipment but also solves the problem that the receiver cannot decrypt synchronously due to the channel damage in remote communication. Further, it is easily applied in production and life. Finally, the simulation results show that the bit error rate is <10^{-5}, and the bidirectional transmission of 10-Gb/s information over an 85-km single-mode fiber is successfully realized. © 2022 Society of Photo-Optical Instrumentation Engineers (SPIE) [DOI: 10.1117/1.OE.61.7.076104]

Keywords: optical chaotic; time delay signatures; chaotic optical communication; optical feedback.

Paper 20220274G received Mar. 17, 2022; accepted for publication Jun. 22, 2022; published online Jul. 9, 2022.

1 Introduction

With the explosive growth of information exchange capacity and numbers between terminals, network information is facing an unprecedented eavesdropping crisis. Traditional security strategies such as passwords and authentication protocols at the media access control layer or higher layers have been unable to meet the needs of large capacity, high speed, and secure communication. An illegal receiver can steal information with similar mathematical algorithms, so some security risks exist. Researchers began to shift their attention to physical security technology. Until now, many encryption technologies based on physical layer have been proposed; these include optical XOR logic, optical steganography, and optical chaotic encryption.

Among them, the optical chaotic communication system has broad application prospect because of its characteristics, such as chaotic signal noise and non-long-term prediction and broadband. The chaotic light source itself is easy to build and replicate, but the chaotic signal generated by itself is extremely sensitive to the initial conditions. Small differences in the initial conditions will make the results change dramatically. Based on this, the replicability of the chaotic light source can be used to build the same chaotic dynamics at the transmitter and the receiver to encrypt and decrypt the information. The chaotic signal is extremely sensitive to the initial conditions, so the encrypted signal has strong anti-interception ability. The illegal third party can steal information only when it can completely eliminate the chaotic carrier.

Due to its potential application in secure communication, chaotic synchronization has been widely studied since 1990 when Pecora and Carroll first proposed the chaotic synchronization scheme and experimentally proved the chaotic synchronization phenomenon. In 1998, VanWiggeren and Roy demonstrated a 10-MHz back-to-back chaotic communication system with fiber lasers. In 2005, Argyris et al. carried out field experiments in Athens and realized the...
encryption transmission rate of 1 Gb/s on a 120-km optical fiber link, which opened a new era in the field of communication and ushered in a period of rapid development of chaotic secure communication. In 2010, Lavrov et al.\textsuperscript{12} successfully realized the secure transmission of 10-Gb/s differential phase-shift keying information over 100-km optical fiber. In the same year, Argyris et al.\textsuperscript{13} improved the overall transmission capacity of the system through wavelength division multiplexing (WDM) technology and achieved a transmission rate of 1.25 Gb/s under the condition that the bit error rate (BER) was below 10\textsuperscript{-12}. In 2017, Ai and Wang\textsuperscript{14} successfully transmitted 5 Gb/s carrierless amplitude/phase signal and 10-Gb/s on-off keying signal using a chaotic secure communication system based on the electro-optical time-delay feedback loop. In 2019, Wang et al.\textsuperscript{15} realized the all-optical chaotic communication of 10-Gb/s messages by enhancing the chaotic carrier bandwidth. In the past two decades, researchers have continuously been proposing new solutions to improve the communication rate and transmission distance, which have been raised to 50 Gb/s and 100 km, respectively.

In the above-chaotic communication systems, the generation of chaos can be classified according to the nonlinear dynamic characteristics of different devices, including a semiconductor laser, Mach–Zehnder interferometer (MZI), and Mach–Zehnder modulator (MZM). The external optical cavity feedback method is the most common chaotic generation scheme based on semiconductor lasers. But in the traditional method, there are shortcomings such as too large equipment volume requirements and inability to accurately control the length and angle of the external cavity.

Based on this, we improve the traditional optical external cavity feedback method and propose an all-optical bidirectional chaotic communication system. Using erbium-doped fiber amplifier (EDFA) and single-mode fiber to replace the traditional external cavity, the optical path of the external cavity can be accurately controlled by changing the length of the erbium-doped fiber, and the volume of the equipment can be reduced. Then a bidirectional transmission communication scheme, which can successfully recover the information sent by the other end in the local area, is presented, and the decryption equipment at both ends is cancelled, greatly simplifying the experimental equipment. Finally, the simulation results show that the BER is < 10\textsuperscript{-5}, and the bidirectional transmission of 10 Gb/s information over an 85-km fiber can be realized. The performance of the communication system with time delay signatures (TDS) mismatch at the transmitters is studied, which proves that the system has certain anti-interception ability.

2 Theoretical Model

In the traditional external cavity optical feedback method (as shown in Fig. 1), the air cavity between the mirror and the laser is the external optical cavity. The mirror reflects the light generated by the laser back to the active layer of the laser, disrupting the interaction between photons and carriers\textsuperscript{8} and producing a dynamically unstable chaotic sequence. In this method, the round-trip time of the light on the external cavity is the delay time of the chaotic sequence. However, accurately controlling the length and angle of the air cavity is difficult, and the resulting delay time mismatch reduces the encryption and decryption performance of the system. In addition, to meet a certain feedback time, the length of the optical cavity needs to be continuously increased to make the equipment larger. For example, if the delay time of 103 ns is to be achieved, the length of the optical external cavity should reach 15.45 m [length of optical cavity = 3 \times 10^8 \text{ (m/s)} \times \text{delay time(s)}/2].

![Fig. 1 Traditional external cavity optical feedback method.](image)
Therefore, the traditional external cavity optical feedback method is improved here. An EDFA is used to replace the external cavity, and the EDFA and a single-mode fiber act as an external feedback cavity. The delay time can be controlled by changing the length of the erbium-doped fiber, which overcomes the disadvantages of the traditional scheme.

In addition, because our scheme is based on all-optical feedback, compared with the scheme based on an MZI or MZM, it avoids the use of broadband photodetectors and related electronic devices, simplifies the experimental structure of the chaotic communication system, and reduces the hardware cost. In the real transmission environment, there is a great possibility of device mismatch due to non-human reasons. A simple system structure can effectively reduce the system performance degradation caused by device mismatch.

To improve the traditional external cavity optical feedback method, a bidirectional chaotic communication system based on an all-optical time-delay feedback loop is proposed and shown in Fig. 2. The all-optical time-delay feedback loop is used to generate chaotic signals and is composed of a tunable delay line (TDL), an EDFA, and a Bessel band-pass filter. The TDL is matched with EDFA to flexibly adjust the optical path of the feedback loop. The Bessel filter causes the frequency-based phase shift to produce nonlinear signal distortion and minimizes the phase nonlinearity of the passband. The light wave generated by continue wave (CW) Laser2 generates a chaotic signal after repeated iterations in the feedback loop. MZM1 modulates the binary information to be encrypted, and the modulated signal is amplified and coupled with the chaotic carrier to complete the encryption operation. The encrypted information is divided into two channels by the beam splitter; one is left locally, and the other one enters the transmission channel through the circulator and is transmitted to the other end. Therefore, the receivers at both ends can receive the synchronous power error \( P_1(t) - P_2(t) \) of the two encrypted information. After taking the absolute value of the error and comparing it with the local information, the message sent by the other end can be recovered. In other words, bidirectional secure communication is realized.

Referring to the theory model of chaotic dynamics presented by Volkovskii and Rulkov, the system equations and the rate equation of the standard three-level laser are firstly derived:

\[
\frac{dq}{dt} = \left[ V_a B N - \left( \frac{1}{\tau_c} \right) \right] q, (1)
\]

\[
\frac{dN}{dt} = W_p (N_t - N) - 2BqN - \frac{N_t + N}{\tau_2}, (2)
\]

where \( q \) is the total number of photons, \( N \) is the number of particle inversions, \( N_t \) is the total number of particles, \( \tau_2 \) is the lifetime of high-energy particles, \( \tau_c \) is the lifetime of photons, and \( W_p \) represents the pump. Then, the normalization process is carried out to obtain...
It can be seen from Fig. 3, in the case of no information carrying, that the signal generated by the transmitter shows chaotic behavior and the high and low amplitude pulses follow each other. The phenomenon happening behind pulsating chaos is the occurrence of the population inversion state for a specific time and then the instant release of energy in the form of a chaotic pulse. As the energy stored during population inversion is not fully consumed in a single cycle, the remaining energy acts as a starting point for the next buildup of the new pulse; hence the amplitude of every chaotic pulse becomes different, so it generally shows noise-like characteristics and can effectively conceal the information. Thus, the third party cannot steal the information at any point between the transmitter and the receiver, which improves the security of the communication system.

Subsequently, we input two groups of zero-returned binary information \( m_1 \) and \( m_2 \) into the system. The introduction of information will disturb the synchronization state of the two transmitters, making the output waveform of both ends constantly switch between synchronous and asynchronous states. The introduction of information will destroy the information. Thus, the third party cannot steal the information at any point between the transmitter and the receiver, which improves the security of the communication system.

\[ \frac{d(2Bq\tau_2)}{d(t/\tau_2)} = \left[ \frac{V_aBN\tau_2 - \tau_2}{\tau_e} \right] 2Bq\tau_2, \quad (3) \]

\[ \frac{d(N/N_i)}{d(t/\tau_2)} = -(1 + \tau_2W_p + 2\tau_2Bq) \frac{N}{N_i} + \tau_2W_p - 1, \quad (4) \]

Let \( I = 2Bq\tau_2, \tau = t/\tau_2, D = N/N_i, \) and \( I_p = W_p\tau_2, \) and use \( g \) to denote \( \tau_2V_aBN, \) and \( k \) to denote \( \tau_2/\tau_e. \) The simplified formula is as follows:

\[ \dot{I}(\tau) = [gD(\tau) - k]I(\tau), \quad (5) \]

\[ \dot{D}(\tau) = -[I_p + 1 + I(\tau)]D(\tau) + I_p - 1, \quad (6) \]

Then, the delay times \( \tau_i' \) are introduced into the formula, and considering that the system has two transmitters, the following equations are obtained. The differential equations formed by Eqs. (7) and (8) are the system equations of the all-optical bidirectional chaotic communication system:

\[ \dot{I}_i(\tau) = g_iD_i(\tau)I_i(\tau) - k_iI_i(\tau - \tau_i'), \quad (7) \]

\[ \dot{D}_i(\tau) = -[I_p + 1 + I_i(\tau)]D_i(\tau) + I_p - 1, \quad (8) \]

The actual meaning of \( g \) and \( k \) are the loss coefficient and gain coefficient of the system feedback loop, respectively. The values of \( g \) and \( k \) are affected by the pumping intensity and the length and radius of the erbium-doped fiber, and \( i = 1, 2 \) are the subindices of different transmitters. In the bidirectional communication system, performing a difference operation for the synchronized chaotic signals generated at both ends, the decryption operation can be performed. Therefore, the encrypted bidirectional information transmission can be realized only when the hardware parameters of the two transmitters are perfectly matched.

The system performance was analyzed in the Optisystem software. Taking Transmitter1 as an example, the parameter values are selected. To make the simulation process have a more practical reference value, the transmitting power of CW Laser1 is set as \(-70 \) dBm, which is easy to achieve in practice, and the center frequency of the generated light wave is 1550 nm. However, the transmission power of CW Laser2 should not be too large or too small. If it is too large, the information cannot be completely covered by chaotic signals, and if it is too small, useful information will be annihilated during long-distance transmission. Here, the value of CW Laser2 is set as \(-10 \) dBm, and an amplifier with a gain of 30 dB is used to amplify the modulated light wave. In the all-optical time-delay feedback loop, the delay time of the total loop is set as 103 ns. To realize encrypted bidirectional information transmission, chaotic signals on both sides must be synchronized, so Transmitter2 adopts the same parameters as Transmitter1, which will not be described here.

### 3 Results

It can be seen from Fig. 3, in the case of no information carrying, that the signal generated by the transmitter shows chaotic behavior and the high and low amplitude pulses follow each other. The phenomenon happening behind pulsating chaos is the occurrence of the population inversion state for a specific time and then the instant release of energy in the form of a chaotic pulse. As the energy stored during population inversion is not fully consumed in a single cycle, the remaining energy acts as a starting point for the next buildup of the new pulse; hence the amplitude of every chaotic pulse becomes different, so it generally shows noise-like characteristics and can effectively conceal the information. Thus, the third party cannot steal the information at any point between the transmitter and the receiver, which improves the security of the communication system.

Subsequently, we input two groups of zero-returned binary information \( m_1 \) and \( m_2 \) into the system. The introduction of information will disturb the synchronization state of the two transmitters, making the output waveform of both ends constantly switch between synchronous and asynchronous states.
asynchronous. Only when the same symbols are transmitted at both ends at the same time can the output waveforms be kept synchronized. If the two ends transmit different symbols, the waveforms at both ends show an asynchronous state. Encrypted information is transmitted to the other end through the channel and subtracted from the local encrypted information to obtain the synchronous power error $P_1(t) - P_2(t)$ of the two waveforms. After taking the absolute value of the error, the encrypted information can be recovered by performing the XOR operation with the local information. The specific steps of decryption are shown in Table 1. The time-domain diagram obtained during the simulation process is shown in Fig. 4, which is consistent with the theoretical value in Table 1, confirming that the system has the capability of bidirectional transmission.

Under the condition of ensuring that the system can achieve bidirectional transmission, the relationship between transmission distance and BER is further studied. The information transmission rate at both ends is set at 1 Gb/s to obtain the curve of distance and BER as shown in Fig. 5(a). With the increase of transmission distance, the BER continues to increase. When the transmission distance is increased to 100 km, $\log_{10}(\text{BER}) = -6.7269$, the BER meets the minimum communication requirement of $< 10^{-5}$. However, when the transmission distance continues to increase to 120 km, the BER is lower than $10^{-5}$ due to the introduction of too many interference signals during the transmission process of encrypted information. In this case, the eye diagram is shown in Fig. 5(d). Compared with Figs. 5(b) and 5(c), when the transmission distance increases to 120 km, there is chaos and no obvious “eye” shape in the eye diagram, so the information cannot be decrypted effectively. Therefore, when information is transmitted at a rate of 1 Gb/s, the maximum transmission distance that can be achieved is 100 km.

As usual, the information transmission rates commonly used in optical fiber communication are 10 and 40 Gb/s, which are much higher than the 1 Gb/s set in the above simulation process. The relationship between the transmission speed and the BER is studied to make the simulation more practical. To reserve space for the increase of the BER accompanied by the rate growth, the transmission distance is set as 85 km in combination with the data in Fig. 5. We get the curve of

### Table 1 Digital demonstration of decryption steps. (The italic values correspond to the red line in Fig. 4. The bold values correspond to the blue line in Fig. 4).

| $m_1(t)$         | 0100100111011101 |
|------------------|------------------|
| $m_2(t)$         | 0111100010110010 |
| $|P_1(t) - P_2(t)|$ | 0011000101101111 |
| $m_1(t) \oplus |P_1(t) - P_2(t)|$ | 0111100010110010 |
| $m_2(t) \oplus |P_1(t) - P_2(t)|$ | 0100100111011101 |
transmission speed and BER as shown in Fig. 6(a) after multiple simulations. When the transmission speed is 10 Gb/s, the minimum requirement of the communication BER is met. Therefore, under the condition that the BER is $<10^{-5}$, the bidirectional information transmission of 10 Gb/s on an 85-km optical fiber is successfully realized. The eye diagrams at different transmission rates are show in Figs. 6(b), 6(c), and 6(d). With the increase of the speed, the

Fig. 4 (a) Information $m_1(t)$; (b) information $m_2(t)$; (c) the absolute value of the synchronization power error received by Receiver1; (d) the absolute value of the synchronization power error received by Receiver2; (e) information recovered by Receiver1; and (f) information recovered by Receiver2.

Fig. 5 (a) Relationship between distance and BER at 1 Gb/s; (b) eye diagram at 50 km; (c) eye diagram at 100 km; and (d) eye diagram at 120 km.
height of the eye opening gradually decreases. When the transmission rate is increased to 13 Gb/s, the quality of the eye diagram is seriously affected, and it is almost impossible to accurately recover the encrypted information.

Next, the performance of the system when the two transmitters are TDS mismatched is further analyzed. We continue to maintain the transmission distance of 85 km and the transmission rate of 10 Gb/s by adjusting the delay time of the TDL at either end, and we obtain the curve graph of TDS mismatched degree and the normalized BER in Fig. 7. It can be seen from Fig. 7, due to the mismatch of TDS, the BER of the recovered information increases sharply, resulting in a great discount on the quality of the information. The greater the degree of mismatch is, the less successful recovery of the information is. In other words, the system has a certain ability to resist interception. As long as the third party cannot reconstruct the completely correct chaotic dynamics system, the information will not be able to be stolen, ensuring the security of the communication.

4 Conclusions

This paper proposed an all-optical bidirectional chaotic communication system that overcomes the problems of poor security and low transmission efficiency in the traditional secure communication system. In this scheme, an all-optical time-delay feedback loop was designed using EDFA to improve the traditional external optical cavity method; it produced chaotic waveforms successfully and solved the problem of high equipment requirements in the traditional scheme, making it easy to apply on a large scale. It provides a new idea for the research of subsequent chaotic generation schemes. The improved chaotic generation scheme can also be applied to the
fields of random number generation, broadband signal generation, chaotic lidar, optical time domain reflectometer, and image encryption.

On this basis, a bidirectional transmission scheme was proposed to improve the efficiency of information transmission. Under the condition that BER is $10^{-5}$, the bidirectional information transmission rate of 10 Gb/s on an 85-km optical fiber was finally achieved successfully. The anti-interception ability of the system was also verified by studying the mismatch degree of TDS at the transmitters, which proved the security of the system. This scheme can be applied to many situations that need confidential communication, such as the transmission of electrocardiography or electromyography containing patient privacy information in remote health monitoring system, and to the encryption transmission of images, audio, and videos in network transmission to prevent malicious theft and destruction of information by others.

Until now, researchers have proposed many schemes to improve the performance of the system, but the system structure is complex and difficult to implement, and the overall information transmission rate remains at about 10 Gb/s. Table 2 lists the performance structures of some existing schemes, which are compared with our scheme.

From the perspective of basic structure, the schemes proposed in Refs. 13 and 20 are fundamentally different from other schemes. The chaotic communication systems in Refs. 13 and 20 are implemented on photonic integrated circuits (PICs), while the chaotic light sources in other references are composed of discrete devices. The PIC-based chaotic light source has the advantages of small size and stable performance. However, compared with the chaotic light source composed of discrete devices, there are also disadvantages such as complex process, low yield, and high cost.

From the perspective of data encryption, the references in the table cover three information encryption methods of optical chaotic secure communication: chaotic masking method, phase modulation method, and amplitude modulation method. Compared with the chaotic masking method realized directly by a coupler or adder, the latter two require broadband photodetectors and related electronic devices. Therefore, in our work, we chose the chaotic masking method with a simple structure and easy realization.

In addition, although the proposed scheme can realize bidirectional communication and resist information interception, there is still room for improvement. For example, Ref. 13 combines chaotic communication with the dense wavelength division multiplexing technology to improve the transmission efficiency of the system. In Ref. 6, amplified spontaneous emission noise is
innovatively used as a complex entropy source, which enhances the complexity of the system. These excellent schemes have given us great inspiration, and we will continue to focus on improving the transmission efficiency and security performance of chaotic communication systems in subsequent research.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 60170505) and Zhejiang Province Key Research and Development Program (Grant No. 2019C01G1121168).

References

1. B. Wu, B. J. Shastri, and P. R. Prucnal, “Secure communication in fiber-optic networks,” in Emerging Trends in ICT Security, B. Akhgar and H. R. Arabnia, Eds., pp. 173–183, Morgan Kaufmann (2014).
2. E. Wohlgemuth et al., “Photonic-layer encryption and steganography over IM/DD communication system,” Opt. Express 26(25), 32691–32703 (2018).
3. Z. Li and G. Li, “Ultrahigh-speed reconfigurable logic gates based on four-wave mixing in a semiconductor optical amplifier,” IEEE Photonics Technol. Lett. 18(12), 1341–1343 (2006).
4. Y. Liu et al., “All-optical logic gates based on two-dimensional low-refractive-index nonlinear photonic crystal slabs,” Opt. Express 19(3), 1945–1953 (2011).
5. N. Jiang et al., “Physical secure optical communication based on private chaotic spectral phase encryption/decryption,” Opt. Lett. 44(7), 1536–1539 (2019).
6. Y. Fu et al., “High-speed optical secure communication with an external noise source and an internal time-delayed feedback loop,” Photonics Res. 7(11), 1306–1313 (2019).
7. Q. Li et al., “Numerical investigations of synchronization and communication based on an electro-optic phase chaos system with concealment of time delay,” Appl. Opt. 58(7), 1715–1722 (2019).
8. L. Yan, “Chaotic laser parallel series synchronization and its repeater applications in secure communication,” Acta Opt. Sin. 68(17), 170502 (2019).
9. L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems,” Phys. Rev. Lett. 64(8), 821–824 (1990).

Table 2  Comparison of this work with other work.

| Ref. | Basic structure | Data encryption method | Transmission type | Maximum transmission distance | Maximum transmission speed (Gb/s) |
|------|----------------|------------------------|------------------|-------------------------------|----------------------------------|
| 6    | An external noise source and an internal time-delay feedback loop | Amplitude modulation method | Unidirection | 100 km | 10 |
| 12   | An electro-optic delay feedback loop | Phase modulation method | Unidirection | 70 km | 10 |
| 13   | A PIC | Chaos masking method | Unidirection | 116 km | 1.25 |
| 20   | A PIC | Amplitude modulation method | Unidirection | 100 km | 2.5 |
| 21   | An electro-optic delay feedback loop | Phase modulation method | Unidirection Back-to-back (SNR = 20 dB) | 3 |
| This work | An all-optical time-delay feedback loop | Chaos masking method | Bidirection | 85 km | 10 |
10. G. D. VanWiggeren and R. Roy, “Communication with chaotic lasers,” *Science* **279**(5354), 1198–1200 (1998).
11. A. Argyris et al., “Chaos-based communications at high bit rates using commercial fibre-optic links,” *Nature* **438**(7066), 343–346 (2005).
12. R. Lavrov, M. Jacquot, and L. Larger, “Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications,” *J. Quantum Electron.* **46**(10), 1430–1435 (2010).
13. A. Argyris et al., “Transmission effects in wavelength division multiplexed chaotic optical communication systems,” *J. Lightwave Technol.* **28**(21), 3107–3114 (2010).
14. J. Z. Ai and L. L. Wang, “Secure communications of CAP-4 and OOK signals over MMF based on electro-optic chaos,” *Opt. Lett.* **42**(18), 3662–3666 (2017).
15. L. Wang et al., “Experiment on 10-Gb/s message transmission using an all-optical chaotic secure communication system,” *Opt. Commun.* **453**, 124350 (2019).
16. A. R. Volkovskii and N. Rulkov, “Synchronous chaotic response of a nonlinear oscillator system as a principle for the detection of the information component of chaos,” *Tech. Phys. Lett.* **19**(6), 97–99 (1993).
17. R. Shahzadi et al., “Secure EEG signal transmission for remote health monitoring using optical chaos,” *IEEE Access* **7**, 57769–57778 (2019).
18. C. H. Cheng et al., “3D pulsed chaos lidar system,” *Opt. Express* **26**(9), 12230–12241 (2018).
19. X. Dong et al., “Combined attenuation and high resolution fault measurements using chaos-OTDR,” *IEEE Photonics J.* **7**(6), 6804006 (2015).
20. A. Argyris et al., “Chaos-on-a-chip secures data transmission in optical fiber links,” *Opt. Express* **18**(5), 5188–5198 (2010).
21. J. Oden et al., “Multi-Gbit/s optical phase chaos communications using a time-delayed optoelectronic oscillator with a three-wave interferometer nonlinearity,” *Chaos: Interdiscipl. J. Nonlinear Sci.* **27**(11), 114311–114311 (2017).

**Jing-Yang Liu** received her BS degree from the School of Communication Engineering from HangZhou DianZi University, HangZhou, Zhejiang, China, in 2020. She is currently pursuing her MSc degree at the School of Communication Engineering of Hangzhou Dianzi University. Her research interest mainly focuses on optical chaotic communication.

**Xue-Fang Zhou** received her BS and MS degrees in optical engineering from Wuhan University of Science and Technology, Wuhan, Hubei, in 2000 and 2003. From 2014 to 2015, she was a visiting scholar with the Optics Laboratory, School of Electric Engineering, University of Arizona. Since 2003, she has been an assistant professor with communication engineering at Hangzhou Dianzi University. Her current research interests include optical fiber laser, optical fiber sensing technology, and optical communication systems. Biographies of the other authors are not available.