Optics Letters

32 Gb/s chaotic optical communications by deep-learning-based chaos synchronization

Junxiang Ke, Lilin Yi,* Zhao Yang, Yunpeng Yang, Qunbi Zhuge, Yaping Chen, and Weisheng Hu

State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Institute for Advanced Communication and Data Science, Shanghai Jiao Tong University, Shanghai 200240, China
**Corresponding author: lilinyi@sjtu.edu.cn*

Received 9 October 2019; revised 8 November 2019; accepted 12 November 2019; posted 12 November 2019 (Doc. ID 380030); published 27 November 2019

Chaotic optical communications were originally proposed to provide high-level physical layer security for optical communications. Limited by the difficulty of chaos synchronization, there has been little experimental demonstration of high-speed chaotic optical communications, and point to multipoint chaotic optical networking is hard to implement. Here, we propose a method to overcome the current limitations. By using a deep-learning-based scheme to learn the complex nonlinear model of the chaotic transmitter, wideband chaos synchronization can be realized in the digital domain. Therefore, the chaotic receiver can be significantly simplified while still guaranteeing security. A successful transmission of 32 Gb/s messages hidden in a wideband chaotic optical carrier was experimentally demonstrated over a 20 km fiber link. We believe the proposed deep-learning-based chaos synchronization method will enable a new direction for further development of high-speed chaotic optical communication systems and networks.

https://doi.org/10.1364/OL.44.005776

Since chaos synchronization was first proposed in 1990 [1], chaos has been widely studied in optical communications as a powerful hardware encryption method. In chaotic optical communication systems, the optical chaos is generated by the nonlinearity of optical devices, which can be either lasers [2] or modulators [2–9]. The dynamics for the modulator and the laser with feedback loop can be dated from the Ikeda ring cavity [10], and both of them have similar dynamic characterization. By using matched devices, chaotic optical communications can be realized. There have been numerous studies into chaotic optical communications, but most of them have been simulations, with only a few being experiments in high-speed chaotic optical communication [2,4,6,7] since experimental implementations of chaos synchronization are quite challenging, especially when the bandwidth is large, and the chaotic transmitter structure is complex. Many complex chaotic transmitter structures have been proposed to improve the level of security [11–13], but no chaos synchronization has been experimentally demonstrated for these structures owing to their complexity. Besides, up to date, no experimental demonstration of point to multipoint chaos synchronization has been reported, since selecting multiple well-matched transmitters and receivers will meet much more challenge. Therefore, for applications of chaotic optical communications with the features of high speed, enhanced complexity, and the capability of point to multipoint networking, chaos synchronization is the bottleneck to be addressed.

Recently, deep learning has also been widely used in optical communications for performance monitoring and linear/nonlinear equalization [9,14]. Back to 2007, an artificial neural network (ANN) with a single hidden layer was used to predict a chaotic time series [15]. As the message-to-chaos ratio is as low as 3% in Ref. [15], which cannot change the loop nonlinearity, it can be approximated as the chaos generation without message involvement, and the nonlinear model was simple and easy to learn. When the message-to-chaos ratio is big enough, the message as a random variable will change the parameter of nonlinear function, which will change the nonlinear dynamic of chaos. Therefore, whether deep learning can be used for chaos synchronization in physical high-speed chaotic optical communication systems is still an open question.

In this Letter, we propose to use deep learning to address the chaos synchronization challenge. We have experimentally demonstrated 32 Gb/s chaotic optical communications over a 20 km fiber link by using deep-learning-based chaos synchronization. After authorized training inside the chaotic transmitter, the trained ANN can be used for chaos synchronization and decryption. The system performance with different message-to-chaos ratios and bit rates was studied for back-to-back (BtB) and transmission over 20 km fiber links. We also analyzed the security of the system against deep-learning-based attacks in detail. By utilizing the learned model in different receivers, chaos synchronization has been greatly simplified, and point to multipoint chaotic optical networking can also be realized. Besides, compared with a chaotic ANN used on the transmitter side [16], the physical chaotic system is more complex and with a higher bandwidth. Therefore, we believe that the proposed deep-learning-based chaos synchronization system opens up a new avenue for chaotic optical communications.

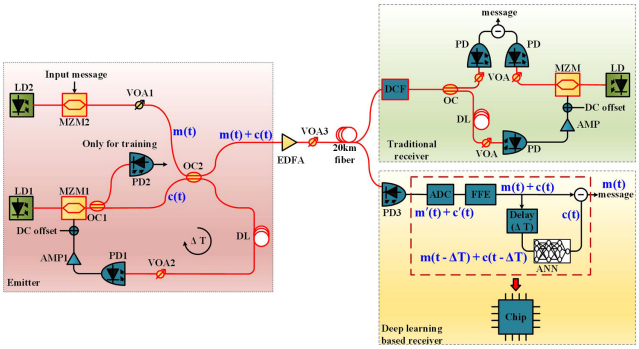

Fig. 1. Experiment setup. LD, laser diode; MZM, Mach–Zehnder modulator; VOA, variable optical attenuator; OC, optical coupler; DL, delay line; PD, photodiode; AMP, broadband radio frequency amplifier; EDFA, erbium-doped fiber amplifier; DCF, dispersion compensation fiber; ADC, analogue-to-digital conversion; FFE, feedforward equalizer; ANN, artificial neural network.

The experimental setup is shown in Fig. 1. The output light of a laser diode (LD1) with a power of 13 dBm is injected into a Mach–Zehnder modulator (MZM1) with a 3 dB bandwidth of 10 GHz and a half-wave voltage of 3.8 V. And, MZM1 is driven by an electrical amplifier (AMP1) with a 3 dB bandwidth of 30 kHz to 10 GHz and a peak-to-peak voltage of 10 V. The output light of MZM1 is divided into two parts through an optical coupler (OC1), where one part is used for training an ANN, and the other part is mixed with the message from LD2 and MZM2 through OC2. MZM2 is driven by a quadrature amplitude modulation-16 (16 QAM) message, which is generated by an 80 GS/s arbitrary waveform generator. The mixture ratio between message $m(t)$ and chaos $c(t)$ is adjusted by a variable optical attenuator (VOA1). The light mixture that is the chaos-masked message $m(t) + c(t)$ is divided into two parts, where one part is used for secure transmission, and the other part is sent back to the feedback loop for chaos generation. In this case, the message also participates in the chaos generation process, and thus improves the system complexity. After being delayed, the mixed light is converted into an electric signal by photodiode (PD1) with a 3 dB bandwidth of 10 GHz. VOA2 in the loop is used to control the feedback strength. Before being sent into the 20 km fiber link, the mixed light is amplified by an erbium-doped fiber amplifier (EDFA), and VOA3 is used to control the injection power into the fiber at 0 dBm. At the receiver side, the mixed light is received by PD3 with a 3 dB bandwidth of 10 GHz, and then the light is converted into digital signals by an analogue-to-digital converter (ADC). A 40-GS/s oscilloscope (OSC) is employed for its ADC function. A feedforward equalizer (FFE) is used to equalize the fiber dispersion, which can be expressed as $m'(t) + c'(t)$, to the BtB case $m(t) + c(t)$ for the following processing. The output of the FFE is split into two parts, where one part is processed by a delay module whose delay time ΔT is matched with the value in the chaotic transmitter. Following the delay module, a trained ANN module is used for the chaos synchronization. The message $m(t)$ can be decrypted by the subtraction of the regenerated chaos of ANN $c(t)$ and the other output of the FFE module $m(t) + c(t)$.

The ANN used in our experiment is a fully connected neural network, and the hyper parameters of ANN need to be tuned carefully; different hyperparameter combinations of ANN need to be tried to find the best performance. The hyperparameters of ANN include the number of layers and the number of neurons in each layer, and the ANN in our experiment consisted of one input layer with 71 neurons, two hidden layers with 71 and 41 neurons, and one output layer with 1 neuron. In addition, the hyperparameters of ANN need to be slightly tuned to achieve the best performance in the experiment when the parameters of the transmitter are changed. The activation function is $\max(0, x)$. The input of the ANN is the mixed message and chaos after they have experienced the loop delay, which can be expressed as $m(t - \Delta T) + c(t - \Delta T)$, corresponding to the output waveform of the chaotic transmitter. The desired output of the ANN is the chaotic waveform $c(t)$ at the output of PD2. The loss function is the mean square error. And backpropagation (BP) algorithm is used to train the ANN.

For comparison, a traditional chaotic optical receiver is also provided in Fig. 1. A dispersion compensation fiber (DCF) is required to compensate the fiber dispersion before the chaos synchronization. The loop delay time and the parameters of the MZM, AMP, and PDs must be well-matched with those in the chaotic transmitter for the chaos synchronization and the decoding of the chaos-masked message. Compared with the traditional chaotic optical receiver, the proposed deep-learning-based chaotic receiver is significantly simplified, and all the digital signal processing functions can be integrated into a digital chip. All the deep-learning-based chaotic receivers can achieve consistent synchronization performance for point to multipoint networking, which is almost impossible to be achieved by traditional hardware-based chaotic receivers. A well-matched hardware depends on the fine screening component, which cannot always be guaranteed. Except for the simplicity, the main benefit of the deep-learning-based chaotic receiver is the performance consistency, which is essential for practical applications.

First, we present our study on the performance of the chaos synchronization using the deep learning in the BtB case. The chaotic time series collected from PD2 is shown in Fig. 2(a), and the chaotic time series generated by the trained ANN is shown in Fig. 2(b). The synchronization plot of the two time series is shown in Fig. 2(c). The correlation coefficient is used to evaluate the performance of the chaos synchronization; it is defined as [17]

$$C = \frac{\langle (x[n] - \langle x[n] \rangle)(y[n] - \langle y[n] \rangle) \rangle}{\sqrt{\langle [x[n] - \langle x[n] \rangle]^2 \rangle \langle [y[n] - \langle y[n] \rangle]^2 \rangle}}, \quad (1)$$

where $x[n]$ denotes the chaotic time series collected from PD2, $y[n]$ denotes the chaotic time series generated by the ANN, and $\langle \cdot \rangle$ denotes the average operation. The calculated correlation coefficient C is as high as 97.57%, which is even better than 96.44% of the well-matched chaotic receiver [4]. In previous work, for some well-selecting components, the correlation coefficient may be as high as 99% [2], but this perfect synchronization is very dependent on the component manufacturing and, therefore, cannot always be guaranteed, as discussed before. In this experiment, we cannot find matched components to realize 10 GHz chaos synchronization with a correlation coefficient higher than 97.57%, but we can realize 10 GHz chaos synchronization by ANN, which is much simpler than the hardware-based synchronization. Therefore, the synchronization performance for the traditional hardware-based chaotic receiver is not demonstrated to avoid unfair comparison. Besides, in the deep learning-based chaotic receiver FFE can be

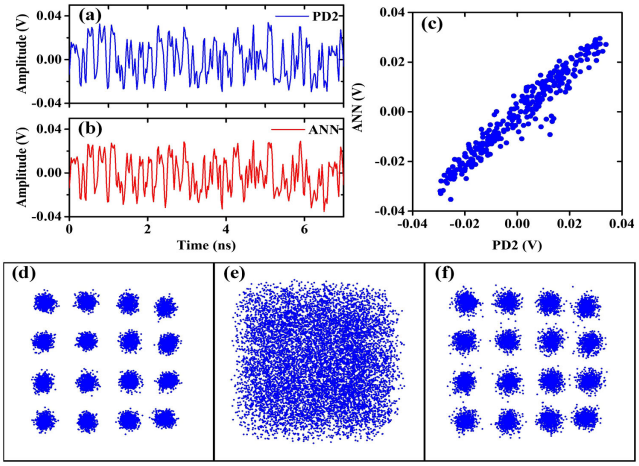

Fig. 2. Chaos synchronization and constellations of the original, encrypted, and decrypted 16 QAM signal in a BtB situation. (a) Chaotic time series collected from PD2 by the OSC. (b) Chaotic time series generated by the ANN. (c) Chaotic synchronization plot of the chaotic time series collected from PD2 and generated by the ANN. (d) Constellation of the original 16 QAM signal. (e) Constellation of the chaos-masked 16 QAM signal. (f) Constellation of the 16 QAM signal decrypted by the ANN.

used for dispersion compensation in the digital domain, which also simplifies the fiber link. For the traditional hardware-based synchronization method, DCF has to be used in the fiber link to compensate the dispersion before synchronization.

After the chaos synchronization is realized by the trained ANN, the 16 QAM message can be recovered by subtracting the ANN-generated chaos from the chaos-masked message. The constellation of the digital coherent demodulated 16 QAM message is shown in Fig. 2(f). Digital coherent demodulation is also performed on the encrypted message for a fair comparison: the constellation of that demodulated encrypted 16 QAM message is shown in Fig. 2(e), and it can be seen that the constellation is completely noisy. The decrypted 16 QAM message is worse than the original one, as shown in Fig. 2(d), because the synchronization error is converted into noise, which degrades the signal-to-noise ratio.

We also studied the bit error rate (BER) performance with different bit rates and different mask coefficients for the BtB and 20 km fiber transmission cases. As shown in Fig. 3, the mask coefficient is defined as the ratio of the peak-to-peak values between the 16 QAM message and the chaotic waveform. For the 20 km fiber transmission case, a FFE module with 21 taps is needed to compensate the fiber dispersion. Both 20 Gb/s and 32 Gb/s 16QAM messages masked by a 10 GHz wide chaotic waveform were studied. The BER curves for the encrypted message and the decrypted message in the BtB and 20 km fiber transmission cases for the 20 Gb/s 16 QAM message are shown in Fig. 3(a). The BER of the encrypted message in the BtB situation is higher than 1×10^{-1}, guaranteeing the security. The green line represents the BER performance of the decrypted message in the BtB situation, where the BER decreases as the mask coefficient increases, and the BER is well below 3.8×10^{-3}, which is the hard decision forward error correction threshold, indicating that the message can be effectively extracted. The purple line shows the BER performance of the decrypted message after 20 km fiber transmission. Compared

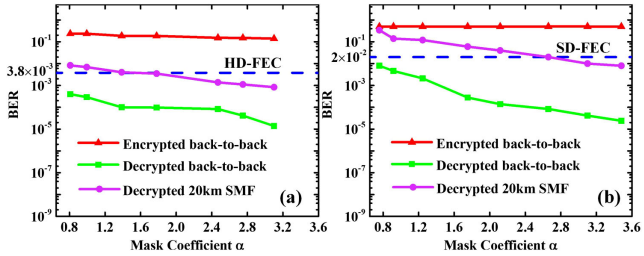

Fig. 3. BER performance. (a) BER performance of the encrypted signal (red triangles), the decrypted signal (green squares) in the BtB case, and the decrypted signal (purple circles) after 20 km fiber transmission with different mask coefficients for a 20 Gb/s 16 QAM signal. (b) BER performance of the encrypted signal (red triangles), the decrypted signal (green squares) in the BtB case, and the decrypted signal (purple circles) after 20 km fiber transmission with different mask coefficients for a 32 Gb/s 16 QAM signal.

with the BER in the BtB case, the BER becomes worse because the impairments in the 20 km fiber transmission cannot be completely compensated by the FFE module. When we increased the bit rate of the 16 QAM message to 32 Gb/s [BER performance shown in Fig. 3(b)], the variation of the BER with the mask coefficient is similar as for the case in Fig. 3(a). However, the 32 Gb/s 16 QAM message is more sensitive to the dispersion. Therefore, the BER performance of the 32 Gb/s 16 QAM message was worse than the BER performance of the 20 Gb/s message, and a soft decision forward error correction, which is associated with a higher cost, is needed for channel coding. Since in intensity modulation direct-detection system dispersion is a serious distortion factor, an FFE with 21 taps is not sufficient to completely compensate the fiber dispersion, and increasing the taps of FFE still cannot improve the performance, this results in a discrepancy between the compensated waveform and the BtB waveform. Therefore, the ANN trained on the BtB case is not optimized for the transmission case, and the system performance will be degraded after fiber transmission, but it is not easy to train ANN on the 20 km fiber case in experiment because of the large time delay between the transmitter and receiver. If optical coherent detection or DCF is used, the fiber dispersion can be completely compensated, and the performance can be improved.

We have demonstrated that an ANN can replace a traditional chaotic optical receiver for chaos synchronization and decryption. We will then discuss if it is possible to use an ANN for eavesdroppers to attack the chaos system. We consider three well-known attacks: brute-force attack, free cypher text attack, and plaintext attack. First of all, it is almost impossible to brute-force the chaos system using the ANN since there are infinite node combinations for an ANN and the parameter space for a given ANN is also infinite in principle. In this work, the number of parameters in the ANN is 8106, and the digital value range of each parameter is no limitation. Besides, except for the parameters of the ANN, the time delay has to be known for correct decryption as the traditional hardware chaotic receiver, which contributes additional key space if the time delay signature can be concealed [11]. Therefore, we consider the structure is safe against the ANN-based brute-force attack. Then, we consider if it is possible to train the ANN using the detected chaotic time series from the transmission line when the message is turned off, the so-called free cypher text attack.

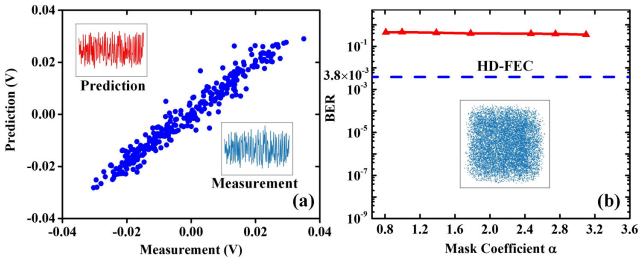

Fig. 4. Synchronization performance using the ANN trained without a message. (a) Chaotic synchronization plot of the chaotic time series measured from the chaotic transmitter and predicted by the ANN trained without a 16 QAM signal. (b) BER performance and constellation of the 16 QAM signal using the ANN trained without a message.

In Fig. 4, we prove that the trained ANN from the chaotic time series without message involvement cannot be used to decrypt the chaos-masked message, guaranteeing the safety against the free cypher text attack. Figure 4(a) shows that the predicted chaotic time series from the trained ANN can be well-matched with the measured chaotic time series from the chaotic transmitter. But using the trained ANN to crack the chaos-masked message failed for all the different mixture ratios between the message and the chaos, as shown in Fig. 4(b). In addition, we tried to change the hyperparameters of ANN in experiment, and the message still could not be decrypted. This is because the nonlinear models of the chaotic transmitter with and without message involvement are completely different. Note that the small mask coefficient, corresponding to small mixture ratio between the message and the chaos, will result in a security issue, which is the case in Ref. [15]. In our experiment, the message will significantly influence the chaos dynamic when the mask coefficient is bigger than 0.8. Finally, we consider the plaintext attack. In this case, the eavesdroppers may use the known plaintext and the achieved chaos-masked message to train the ANN. To correctly train the ANN, $m(t)$ should be known, corresponding to the output waveform of the transmitter. However, for different coding schemes, modulation formats, bit rates of the data, and different modulation responses of the modulator, the output waveform for a given plaintext could be completely different, so only knowing the plaintext without knowing the corresponding waveform is not sufficient to correctly train the ANN. Therefore, the plaintext attack cannot work if the attacker cannot physically access the transmitter. However, according to more conventional attacks [18], more work needs to be done for security enhancing in chaos communication.

In conclusion, by using deep learning to learn the complex nonlinear model of a chaotic transmitter, wideband chaos synchronization was realized; thanks to chaos synchronization being realized in the digital domain, a digital equalizer rather than an optical dispersion compensator can be used to compensate the dispersion. Therefore, the chaotic receiver can be simplified significantly. Secure transmissions of 20 Gb/s and 32 Gb/s 16 QAM messages over 20 km fiber have been experimentally demonstrated. The BER performance in BtB and 20 km fiber transmission cases has been studied. The proposed deep-learning-based chaos synchronization has the same level of security as traditional synchronization schemes, but the implementation difficulty is significantly reduced, which is essential for practical applications. By embedding the trained neural network into different digital chips, point to multipoint chaotic optical networking can also be realized, and the method can also be used in the chaos system based on lasers with optical feedback. Therefore, we believe deep-learning-based chaos synchronization can open up a new direction of chaotic optical communications and may lead to deeper insight into other chaos-based applications, such as chaos key distribution.

Funding. National Key R&D Program of China (2018YFB1800904).

Disclosures. The authors declare no conflicts of interest.

REFERENCES

1. L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
2. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, Nature **438**, 343 (2005).
3. R. Lavrov, M. Jacquot, and L. Larger, IEEE J. Quantum Electron. **46**, 1430 (2010).
4. J. Ke, L. Yi, G. Xia, and W. Hu, Opt. Lett. **43**, 1323 (2018).
5. J. Goedgebuer, L. Larger, and H. Porte, Phys. Rev. Lett. **80**, 2249 (1998).
6. J. Z. Ai, L. L. Wang, and J. Wang, Opt. Lett. **42**, 3662 (2017).
7. J. Oden, R. Lavrov, Y. K. Chembo, and L. Larger, Chaos **27**, 114311 (2017).
8. J. P. Goedgebuer, P. Levy, L. Larger, C. C. Chen, and W. T. Rhodes, IEEE J. Quantum Electron. **38**, 1178 (2002).
9. J. Ke, L. Yi, and W. Hu, IEEE Photon. Technol. Lett. **31**, 1104 (2019).
10. K. Ikeda, Opt. Commun. **30**, 257 (1979).
11. T. T. Hou, L. L. Yi, X. L. Yang, J. X. Ke, Y. Hu, Q. Yang, P. Zhou, and W. S. Hu, Opt. Express **24**, 23439 (2016).
12. N. Jiang, C. Wang, C. P. Xue, G. L. Li, S. Q. Lin, and K. Qiu, Opt. Express **25**, 14359 (2017).
13. A. B. Wang, Y. B. Yang, B. J. Wang, B. B. Zhang, L. Li, and Y. C. Wang, Opt. Express **21**, 8701 (2013).
14. F. Musumeci, C. Rottondi, A. Nag, I. Macaluso, D. Zibar, M. Ruffini, and M. Tornatore, IEEE Commun. Surv. Tutorials **21**, 1383 (2019).
15. S. Ortin, L. Pesquera, J. M. Gutierrez, A. Valle, and A. Cofino, AIP Conf. Proc. **887**, 1 (2007).
16. J. Zhang and S. Wang, *IEEE Asia-Pacific Conference on Circuits and Systems. Electronic Communication Systems* (2000), p. 371.
17. Y. C. Kouomou, P. Colet, N. Gastaud, and L. Large, Phys. Rev. E **69**, 056226 (2004).
18. F. Anstett, G. Millerioux, and G. Bloch, IEEE Trans. Circuit Syst. I **53**, 2673 (2006).