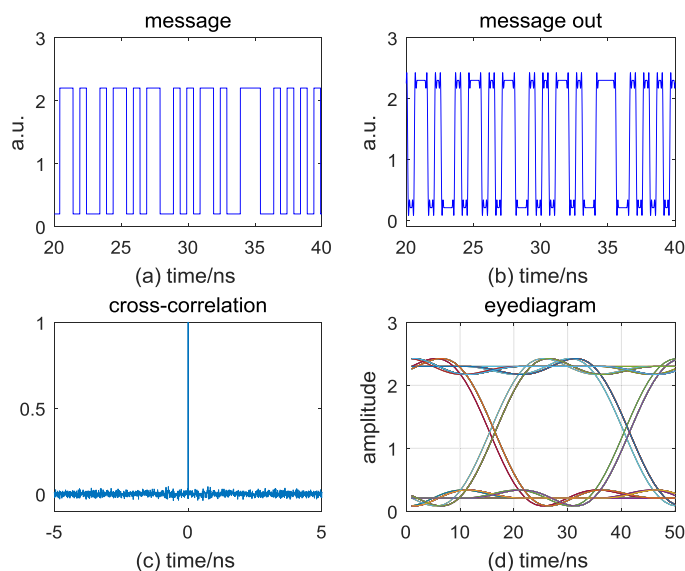


# Enhanced Bidirection Secure Communication Based on Digital Key and Chaotic Random Optical Feedback

Volume 10, Number 6, December 2018



Jianzhong Zhang  
Shuangyi Cui



DOI: 10.1109/JPHOT.2018.2874958

1943-0655 © 2018 IEEE

# Enhanced Bidirection Secure Communication Based on Digital Key and Chaotic Random Optical Feedback

Jianzhong Zhang <sup>1,2</sup> and Shuangyi Cui <sup>1,2</sup>

<sup>1</sup>Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology, Taiyuan 030024, China

<sup>2</sup>Institute of Optoelectronic Engineering, College of Physics & Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China.

DOI:10.1109/JPHOT.2018.2874958

1943-0655 © 2018 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See [http://www.ieee.org/publications\\_standards/publications/rights/index.html](http://www.ieee.org/publications_standards/publications/rights/index.html) for more information.

Manuscript received September 8, 2018; revised October 4, 2018; accepted October 5, 2018. Date of publication October 9, 2018; date of current version October 23, 2018. This work was supported in part by the National Natural Science Foundation of China under Grants 61875146, 61527819, 61671316, and 61731014, in part by the research project supported by Shanxi Scholarship Council of China under Grants 2016-036 and 2017-052 and in part by the Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi and Program for Sanjin Scholar. Corresponding author: Jianzhong Zhang (e-mail: zhangjianzhong@tyut.edu.cn).

**Abstract:** A novel bidirection secure communication scheme based on the digital key and chaotic random optical feedback is proposed and numerically verified. Digital sequence is used as a key to control random variation of external cavity optical feedback, and under the operation of this random feedback, high-dimensional chaotic light is generated with complex dynamics. It is proved that chaotic time delay signature is effectively suppressed and key space increases significantly, which enhances the security of chaotic secure communication. Meanwhile, the bidirection chaotic secure communication is successfully implemented with the message rate of 10 Gb/s. In addition, simulation results show that the proposed scheme increases system synchronization and reduces the bit-error rate of the transmitted message.

**Index Terms:** Digital key, random feedback, chaotic signals, bi-directional communication.

## 1. Introduction

Due to the characteristics of chaotic light, noise-like and wide spectrum, its application in secure communication has received extensive attention [1], [2], [3]. External cavity optical feedback enables semiconductor laser to output chaotic light, but there is a general time delay signature (TDS) caused by feedback, that is, the auto-correlation curve of chaotic laser has a significant peak at feedback delay. This TDS structure provides a possible clue for chaotic secure communication attackers [4], [5], [6]. So it is very important to eliminate the TDS, for example, some modified feedback schemes [7], [8] have been proposed and experimentally achieved with the TDS suppression. Meanwhile, for traditional optical feedback semiconductor laser, operating parameters are fixed after synchronous system establishment, which undoubtedly gives hacker opportunity to infer key parameters, thus reducing security of chaotic communication. Using laser internal parameters as communication key is not easy to change and key parameter space is limited. Therefore, solving these two key problems, i.e., eliminating TDS and increasing key space, is necessary and crucial to the security of chaotic communication. At present, some solutions have been put forward at home and abroad.

In Ref. [9], time delay modulation is achieved by controlling optical path of photoelectric chaotic generator. System chaotic synchronization and efficient information hiding are proved, but elimination of delay signature is not considered. In Ref. [10], message is modulated in chaotic carrier through electric amplifiers to enhance the security of data communication. However, system key is mainly chaotic laser parameter, where key space is small, and the TDS of chaotic carrier is not discussed. Ref. [11] proposes a method of eliminating the TDS by dual-loop rapid phase modulation. To set a certain modulation frequency, the TDS in chaotic carrier is effectively eliminated, preventing information from being bugged. However, the condition of information demodulation at receiving end is not easy to reconstruct. Ref. [12] introduces a group delay frequency modulation module in the photoelectric feedback loop, which effectively inhibits delay information and increases key space. However, the module is made up of standard cascading components, physical arrangement results are limited, and an attacker may illegally eavesdrop on information through a limited arrangement combination. Ref. [13], [14] adopt a fractional Fourier transform to post process chaotic signal, eliminating the TDS. Although in Ref. [13] joins pseudo random code sequence, since chaotic source is not modified, there exist unsafe factor so that attacker crack the system in message transmission process. In Ref. [15], a digital key is introduced into chaotic photoelectric feedback system, where time-delay information is eliminated, and the relationship between encryption algorithm and chaotic coding is established. Similarly, in Ref. [16], two photoelectric feedback loops with parallel structure are adopted, and a long pseudo-random code sequence is used as key to control feedback loops of two different delay structures. However, these systems have complex structures and too many physical devices. Ref. [17] modulates optical feedback phase with binary pseudo-random code and simulates the scenario that eavesdropper extracts information under error key condition. The results show that eavesdropper cannot obtain correct message even if he has the same chaotic source. However, chaotic signals modulated by binary pseudo-random code may still have delay signature, so it is possible that attacker eavesdrop information through auto-correlation analysis. In Ref. [18], intermittent delay photoelectric chaos system is put forward, where digital chaos is generated and encoded to control optical switch to connect different fiber delay line, leading that chaotic signals with random delay is generated and the TDS is eliminated successfully. Meanwhile, digital chaos is used as key, which makes key space increase several times. However, system scheme uses physical structures such as optical switch and fiber delay line, which may cause errors in communication, since deviation may exist in switching on different optical fibers and adjustment of delay line is not easy to control.

In order to solve these defects, we put forward a more simple and effective solution. The digital random sequence consisting of random square wave of multiple levels is used to modulate external optical feedback to realize delay random variation. For one thing, the external-cavity-induced TDS can be effectively eliminated, and for another thing, the digital random sequence used as the secret key can significantly expand the key space. In this way, the digital sequence as key is simple and prone to operation, and the inaccuracy of physical structure is overcome. The proposed scheme is further applied into bi-direction chaotic secure communication. Compared with Ref. [19], we establish a new enhanced bi-direction chaotic secure communication system with the TDS suppression and the key space increase.

## 2. System Model and Principle

Fig. 1. illustrates the process of bi-direction chaotic secure communication between Alice and Bob in a schematic way. Digital sequence is used as key to control arbitrary wave generator (AWG) through digital signal processor (DSP), and square wave with random multiple levels is output. In practice, the concrete implementation process is as follows: digital random sequence is generated in DSP system by C/C++ program. Through the serial port or USB communication, data exchange between the DSP and AWG is further established. Thus, under the control of the DSP, the AWG can output the square wave signal consisting of random multiple levels. A variable delay module (VDM) is put between laser diode and feedback mirror (FM), and square wave sequence is applied to modulate delay module to make external cavity optical feedback highly variable so that laser

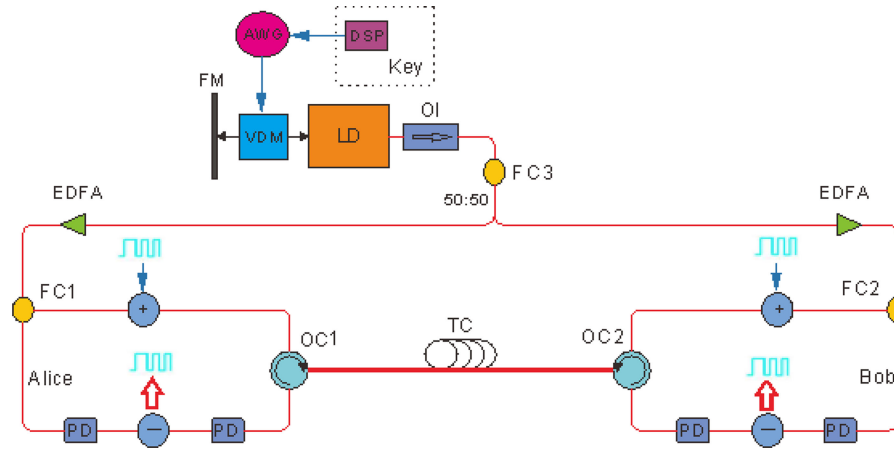


Fig. 1. Schematic diagram of enhanced bi-direction chaotic secure communication.

diode can output high-dimensional chaotic laser. The producing chaotic light is divided into 50:50 two beams through optical isolator (OI) and fiber coupler (FC3), and then enters Alice and Bob end through erbium-doped fiber amplifier (EDFA). Taking Alice's communication to Bob as an example, when chaotic light goes through fiber coupler (FC1), it is selected to only pass the upper rather than the lower path. Message is hidden in chaotic carrier, the mixed signal goes through transmission channel (TC), and then enters optical circulator (OC2) to reach Bob end. Another chaotic light passing fiber coupler (FC2) is selected only through the lower but not the upper path. In this way, the two signals pass through photoelectric detector (PD) to compare and demodulate message loaded in the mixed signal. Similarly, reverse operation can complete communication process from Bob to Alice.

The process of generating chaotic light with random feedback delay can be described as follows using the L-K equation:

$$\frac{dE(t)}{dt} = \frac{1}{2}(1 + i\alpha) \left[ G(t) - \frac{1}{\tau_p} \right] E(t) + kE(t - \tau_m(t)) \exp(-i\omega\tau_m(t)) \quad (1)$$

$$\frac{dN(t)}{dt} = \frac{I}{qV} - \frac{1}{\tau_n} N(t) - G(t) |E(t)|^2 \quad (2)$$

$$G(t) = \frac{G[N(t) - N_0]}{1 + \varepsilon |E(t)|^2} \quad (3)$$

where  $E$  and  $N$  are the slowly varying complex electrical field amplitude and the carrier density in the laser cavity.  $\omega\tau_m(t)$  is the round-trip phase shift induced by the external feedback, where  $\omega$  is the angular frequency of the free-running laser and  $\tau_m(t)$  is the external cavity round-trip time modulated by the random digital sequence.  $I$  is pump current,  $q$  is electric charge,  $V$  is laser cavity active volume,  $\tau_n$  is carrier lifetime,  $\tau_p$  is photon lifetime,  $k$  is feedback rate,  $G$  is differential gain coefficient,  $N_0$  is transparent carrier density,  $\varepsilon$  is saturated coefficient,  $\alpha$  is line width enhancement factor. All the involved laser parameters and their values used in our numerical model are from [3].

### 3. Generation of Chaotic Signals

Under the operation of the optical feedback modulated by random digital sequence, the laser diode can generate the chaotic light signal. Suppose that  $y = [y(1), y(2), \dots, y(i), \dots, y(N)]$  is a random digital sequence, where  $y(i)$  can be arbitrary real number in the interval  $[-1, 1]$ . Here, we assume  $N = 20$ ,  $y(i) \in \{-1, -0.5, 0, 0.5, 1\}$ . Fig. 2(a) displays the random digital sequence. Fig. 2(b) shows the corresponding external cavity feedback delay  $\tau_m(t)$ . Fig. 2(c) and Fig. 2(d) illustrate chaotic

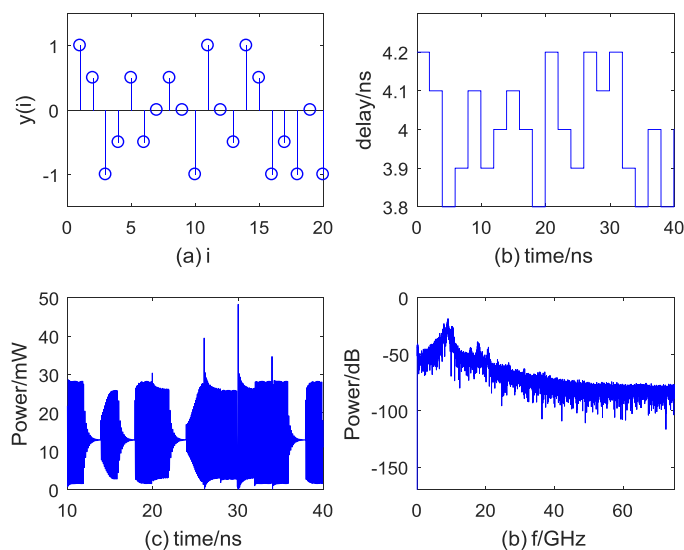


Fig. 2. (a) Digital sequence; (b) feedback delay; (c) chaotic intensity time series; (d) frequency spectrum.

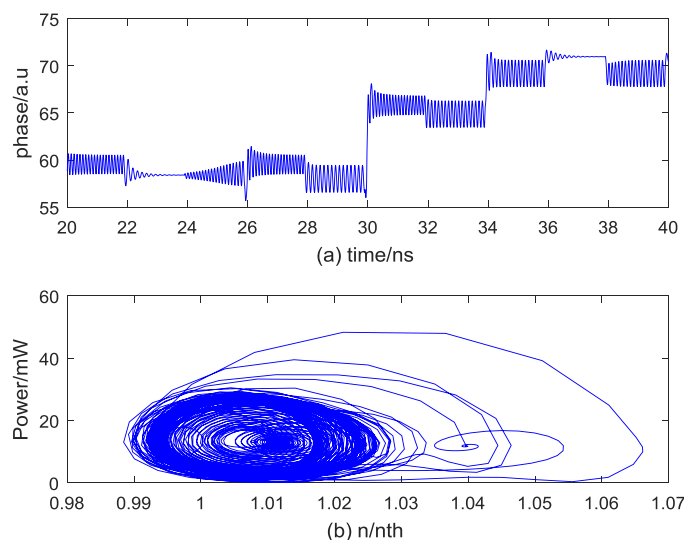


Fig. 3. (a) Phase information of chaotic signals; (b) phase diagram of chaotic signals.

intensity time series and frequency spectrum, respectively. The digital sequence is applied to make external cavity feedback delay change randomly so as to output high-dimensional chaotic light. In order to fully illustrate the characteristics of the generated chaotic light, phase information and phase diagrams of chaotic light signals are further studied, as shown in Fig. 3. From intensity time series and phase information, phase diagram and frequency spectrum, it can be clearly reflected that chaotic signals have higher unpredictability and complex dynamic trajectory.

#### 4. Elimination of the TDS

To ensure the security of transmission information, it is critical to eliminate the TDS. In this paper, the auto-correlation function (ACF) and delayed mutual information (DMI) technology is adopted to study the extraction of delay signature, since other methods are sensitive to noise [15]. In order to better show whether the TDS is eliminated, we fixed the coordinate axis in interval [0ns, 8ns]

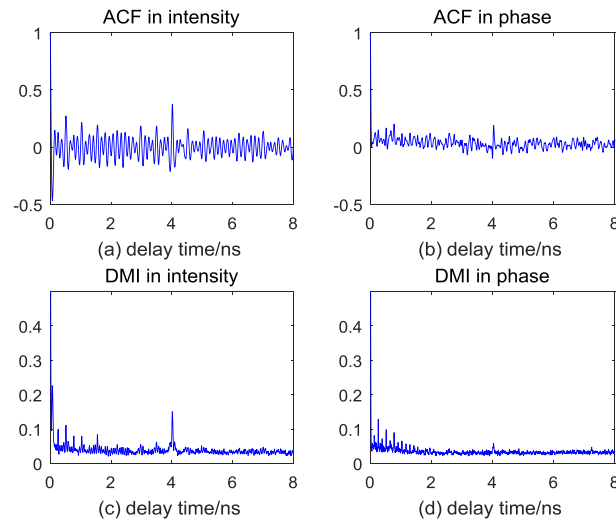


Fig. 4. (a) ACF and (c) DMI of chaotic intensity before the random digital sequence is added, respectively; (b) ACF and (d) DMI of chaotic phase before the random digital sequence is added, respectively.

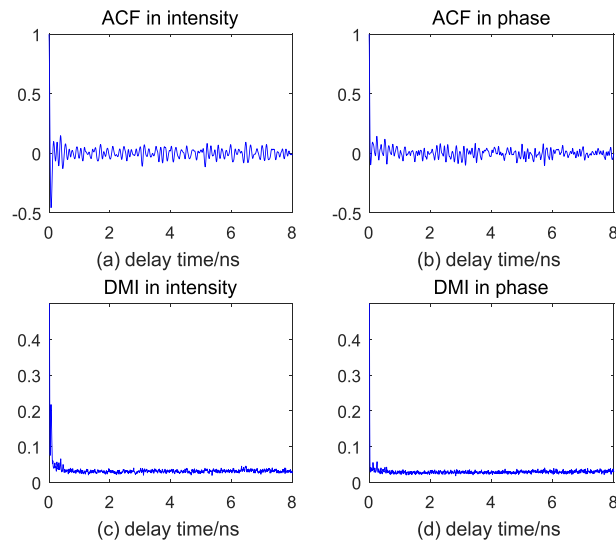


Fig. 5. Identification of time delay signature elimination. (a) ACF and (c) DMI of chaotic intensity after the random digital sequence is added, respectively; (b) ACF and (d) DMI of chaotic phase after the random digital sequence is added, respectively.

for observation and analysis. For demonstrating of the TDS elimination, we compare the ACF and DMI curves of chaotic light signals before and after the random digital sequences are modulated, as shown in Fig. 4 and Fig. 5, respectively. Fig. 4(a) and (c) show the ACF and DMI graphs of chaotic intensity signal without the random digital sequence modulation, respectively. Fig. 4(b) and (d) illustrate the ACF and DMI graphs of chaotic phase signal without the random digital sequence modulation, respectively. It can be clearly seen that there is an obvious TDS at the external cavity feedback delay of 4 ns. From Fig. 5, we can see that the TDS is effectively eliminated by introducing the random digital sequence modulation.

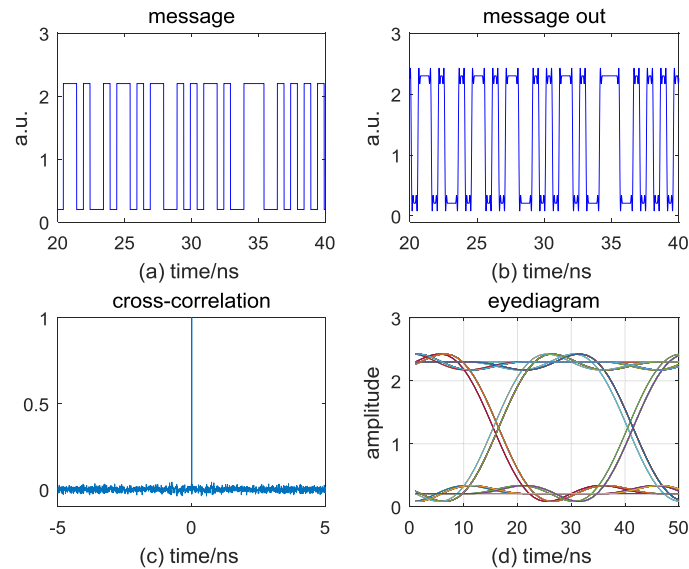


Fig. 6. (a) Original message to be transmitted with the rate of 10 Gb/s; (b) demodulated message; (c) cross-correlation diagram of chaotic signals between Alice and Bob ends; (d) eye diagram of the demodulated message.

## 5. Modulation and Demodulation of Message

The message modulation scheme is based on the chaos masking (CMS), where the message  $M(t)$  is added to the chaotic carrier  $E(t)$  generated by the digital-sequence-modulated external feedback. Here we implement this as:

$$E'(t) = E(t) + m\sqrt{P} \times M(t) \quad (4)$$

Where  $P$  is the average power of the chaotic light from the digital-sequence-modulated external feedback laser diode and  $m$  is the modulation index.

Taking Alice's communication to Bob as an example, the chaotic carrier with the loaded message is transmitted to Bob end, and then the original message is compared and demodulated. A pseudo-random code sequence with the rate of 10 Gb/s is used as the original message at Alice end, as shown in Fig. 6(a). The demodulated message at Bob end after filtering is depicted in Fig. 6(b). Fig. 6(c) represents cross-correlation of chaotic signals between Alice and Bob ends, and Fig. 6(d) shows eye diagram of the demodulated message. It is indicated from Fig. 6 that the original message can be loaded and demodulated successfully, which is also illustrated that the proposed scheme has good synchronization of chaotic secure communication.

In practice, the message transfer between Alice and Bob is achieved through transmission channel. To consider the actual situation of chaotic secure communication, we further investigate the tolerance of the proposed scheme to noise and amplitude distortions of the signal in the transmission channel [20]. The noise simulated is an additive zero-mean Gaussian white noise. Fig. 7 shows the dependence of bit-error rate (BER) of the recovered message on the signal-to-noise ratio (SNR). It can be seen that as the SNR increases, the BER decreases. The insets (a) and (b) in Fig. 7 further depict the eye diagrams of the demodulated messages for the corresponding SNRs of 60 dB and 80 dB, respectively, as a comparison. The former is closed, and conversely the latter is clearly open. This means that the message cannot be properly demodulated when the SNR is lower than 60 dB. The main reason is that the channel noise causes damage of the chaotic carrier and the hidden message, which leads to chaotic synchronization mismatch at receiving end.

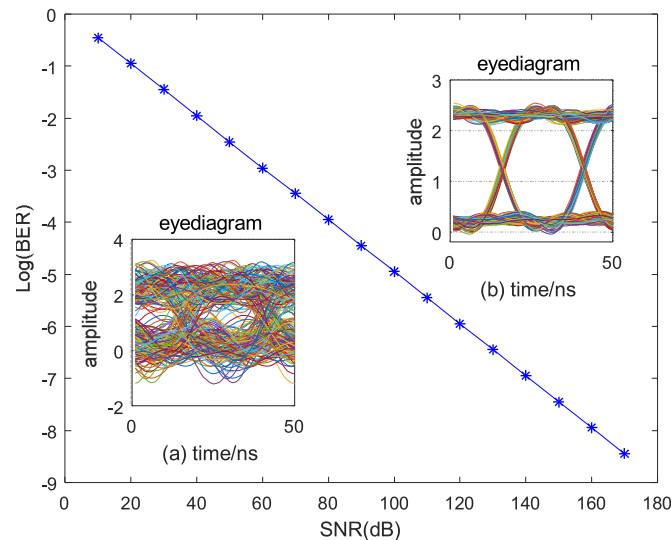


Fig. 7. Relationship between BER and SNR. (a) signal eye diagram corresponding to SNR of 60 dB; (b) signal eye diagram corresponding to SNR of 80 dB.

## 6. Analysis of the Key Space Increase

According to the chaotic synchronization theory, the key to implementing secure communication between Alice and Bob ends lies in that both communication parties have the same hardware with the same structure parameters. In the proposed scheme, the random digital sequence is introduced to modulate the external feedback delay. On the one hand, the utilization of the random digital sequence can eliminate the TDS to prevent this hardware parameter from being extracted by the attacker. On the other hand, the random digital sequence as the secret key can further enhance the key space. As stated previously, the random digital sequence is composed of a series of square wave signals with the sequence length of  $N$  and random multiple levels of  $x$ . In our simulation,  $N = 20$  and  $x = 5$  are taken. Therefore, an additional huge key space of  $5^{20}$  can be achieved.

## 7. Conclusion

In summary, a novel bi-direction chaotic secure communication scheme is demonstrated by the numerical simulation, where the random digital sequence as the secret key is utilized to modulate the external feedback delay. It has been proved that the utilization of the digital sequence cannot only eliminate the TDS but also enlarge the key space significantly. Under the operation of this random feedback, high-dimensional chaotic laser as chaotic carrier is generated. The message with the rate of 10 Gb/s is added in the chaotic carrier by the chaos masking for the bi-direction communication. The results demonstrate that the original message is successfully demodulated at the receiving end. Besides, the tolerance of the proposed scheme to noise in the transmission channel is further analyzed. The proposed scheme provides a better theoretical basis for practical operation of chaotic secure communication.

## Acknowledgment

The authors would like to express their sincere thanks to the editors for their valuable revisions and suggestions on this paper.



---

## References

- [1] A. Argyris *et al.*, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, pp. 343–346, Nov. 17, 2005.
- [2] A. Bogris, K. E. Chlouverakis, A. Argyris, and D. Syvridis, "Subcarrier modulation in all-optical chaotic communication systems," *Opt. Lett.*, vol. 32, pp. 2134–2136, 2007.
- [3] J.-Z. Zhang, A.-B. Wang, J.-F. Wang, and Y.-C. Wang, "Wavelength division multiplexing of chaotic secure and fiber-optic communications," *Opt. Exp.*, vol. 17, pp. 6357–6367, 2009.
- [4] V. S. Udaltsov, L. Larger, J.-P. Goedgebuer, A. Locquet, and D. S. Citrin, "Time delay identification in chaotic cryptosystems ruled by delay-differential equations," *J. Opt. Technol.*, vol. 72, pp. 373–377, 2005.
- [5] D. Rontani, A. Locquet, M. Sciamanna, D. S. Citrin, and S. Ortin, "Time-delay identification in a chaotic semiconductor laser with optical feedback: A dynamical point of view," *IEEE J. Quantum Electron.*, vol. 45, no. 7, pp. 879–1891, Jul. 2009.
- [6] R. M. Nguimdo, G. Verschaffelt, J. Danckaert, and G. Van der Sande, "Loss of time-delay signature in chaotic semiconductor ring lasers," *Opt. Lett.*, vol. 37, pp. 2541–2543, Jul. 1, 2012.
- [7] Y. P. Xu, M. J. Zhang, L. Zhang, P. Lu, S. Mihailov, and X. Y. Bao, "Time-delay signature suppression in a chaotic semiconductor laser by fiber random grating induced random distributed feedback," *Opt. Lett.*, vol. 42, pp. 4107–4110, 2017.
- [8] J. Z. Zhang, M. W. Li, A. B. Wang, M. J. Zhang, Y. N. Ji, and Y. C. Wang, "Time-delay-signature-suppressed broadband chaos generated by scattering feedback and optical injection," *Appl. Opt.*, vol. 57, pp. 6314–6317, 2018.
- [9] M. W. Lee, L. Larger, and J. Goedgebuer, "Transmission system using chaotic delays between lightwaves," *IEEE J. Quantum Electron.*, vol. 39, no. 7, pp. 931–935, Jul. 2003.
- [10] G. Aromataris and V. Annovazzi-Lodi, "Enhancing privacy of chaotic communications by double masking," *IEEE J. Quantum Electron.*, vol. 49, no. 11, pp. 955–959, Nov. 2013.
- [11] C. Xue *et al.*, "Security-enhanced chaos communication with time-delay signature suppression and phase encryption," *Opt. Lett.*, vol. 41, pp. 3690–3, Aug. 15, 2016.
- [12] T. T. Hou *et al.*, "Maximizing the security of chaotic optical communications," *Opt. Exp.*, vol. 24, pp. 23439–23449, Oct. 3, 2016.
- [13] M. Cheng, L. Deng, H. Li, and D. Liu, "Enhanced secure strategy for electro-optic chaotic systems with delayed dynamics by using fractional Fourier transformation," *Opt. Exp.*, vol. 22, pp. 5241–51, Mar. 10, 2014.
- [14] J. J. Suárez-Vargas, B. A. Márquez, and J. A. González, "Highly complex optical signal generation using electro-optical systems with non-linear, non-invertible transmission functions," *Appl. Phys. Lett.*, vol. 101, 2012, Art. no. 071115.
- [15] R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, "Digital key for chaos communication performing time delay concealment," *Phys. Rev. Lett.*, vol. 107, Jul. 15, 2011, Art. no. 034103.
- [16] R. M. Nguimdo and P. Colet, "Electro-optic phase chaos systems with an internal variable and a digital key," *Opt. Exp.*, vol. 20, pp. 25333–25344, Nov. 5, 2012.
- [17] A. Bogris, P. Rizomiliotis, K. E. Chlouverakis, A. Argyris, and D. Syvridis, "Feedback phase in optically generated chaos: A secret key for cryptographic applications," *IEEE J. Quantum Electron.*, vol. 44, no. 2, pp. 119–124, Feb. 2008.
- [18] X. Gao, F. Xie, and H. Hu, "Enhancing the security of electro-optic delayed chaotic system with intermittent time-delay modulation and digital chaos," *Opt. Commun.*, vol. 352, pp. 77–83, 2015.
- [19] J.-G. Wu, Z.-M. Wu, Y.-R. Liu, L. Fan, X. Tang, and G.-Q. Xia, "Simulation of bidirectional long-distance chaos communication performance in a novel fiber-optic chaos synchronization system," *J. Lightw. Technol.*, vol. 31, no. 3, pp. 461–467, Feb. 2013.
- [20] A. S. Karavaev, D. D. Kulminskiy, V. I. Ponomarenko, and M. D. Prokhorov, "An experimental communication scheme based on chaotic time-delay system with switched delay," *Int. J. Bifurcation Chaos*, vol. 25, 2015, Art. no. 1550134.