Security-Enhanced Electro-Optic Mutual Injection Secure Communication Scheme With Time-Delay Signature Suppressing

Wenfu Gu, Xulin Gao, Yuehua An, Anbang Wang, Yuncai Wang, Yuwen Qin, and Zhensen Gao

***Abstract*—In this article, we propose and numerically demonstrate a novel dual-phase modulated time-delay signature (TDS) concealed communication system. The proposed system addresses the fatal disadvantage of conventional electro-optic chaotic systems in that TDS is vulnerable to detection. Combined with the dispersive devices ahead, which significantly expands the complexity of the signal, the scheme perturbs the transmitted data with the mutual injection of the feedforward and feedback branches in the phase, strengthening the nonlinear effect of the system considerably. In addition, the key space of the system against illegal users' exhaustive attack within reasonable parameters reaches 10^{19}, which is 14 orders of magnitude larger than that of the classical electro-optic system. A confidential 32 G/s OOK signal was transmitted over 100 km and successfully recovered. Numerical results demonstrate that the chaotic system can tolerate minor parameter mismatches which are controllable in practice, proving that the system can be used for secure communication.**

***Index Terms*—Electro-optic modulation, optical feedback, time-delay concealment, secure communication.**

I. Introduction

NOWADAYS, the quantity of fiber optic communication data is exploding, which poses a serious threat to the security of data. Therefore, seeking an effective encryption method for message transmission is crucial. Since hardware encryption has obvious advantages at the lowest layer of the transport network, it has been recognized for providing security at the physical layer while combined with digital cryptography at the upper layer to improve the overall privacy of the transmission network [1]. Aiming to guarantee the highest privacy of information among connected users, various encryption methods have been tried in the previous decades, including quantum encryption [2], digital chaos encryption [3], and hardware-based chaos encryption [4]. Thanks to the unpredictability of chaos and its noise-like properties, hardware-based chaotic communication systems have recently emerged as strongly competitive candidates for confidential communication at the physical layer [5].

A recent field transmission experiment demonstrates that chaotic signals can be transmitted directly in existing optical communication systems without additional handling [6], which means that it is compatible with commercial networks. According to its generation method, chaos can be separated into two types. One is all-optical chaos generated by optical feedback [7], [8], [9] or optical injection [10], [11], where optical feedback uses mirrors as a feedback medium, allowing the output signal to be re-injected into the laser, scrambling its internal optical field to produce a noise-like optical signal. However, this method is limited by the laser hardware characteristics and the relaxation oscillation [12], which is difficult to synchronize. As another promising method for chaos generation, the electro-optic feedback modulation technique based on Ikeda's equation is favored by numerous researchers since it offers the advantages of higher bandwidth, easier synchronization, and lower cost [13], [14], [15]. In these types of systems, the parameters of each device are used as keys to constitute an anti-eavesdropping system, among which the TDS is crucial and its leakage can greatly compromise the confidentiality of the system. It should be noted that the TDS of the system can be identified by statistical analysis, such as the autocorrelation function (ACF) [16] and delayed mutual information (DMI) [17]. Once the TDS is available, it is sufficient to reconstruct the chaotic dynamics of the transmitter [18], threatening the security of the communication.

Consequently, effective concealing of the system's TDS and further extension of the system's key space are the main concerns of researchers. So far, a large number of schemes have been proposed and investigated, such as using varying parameters

Manuscript received 18 April 2023; revised 18 May 2023; accepted 20 May 2023. Date of publication 23 May 2023; date of current version 2 June 2023. This work was supported in part by the National Key Research and Development Program of China under Grant 2020YFB1806401, in part by the National Natural Science Foundation of China under Grants U2001601, U22A2087, 11904057, and 62004047, in part by Guangdong Basic and Applied Basic Research Foundation under Grant 2023B1515020088, and in part by Guangdong Introducing Innovative and Entrepreneurial Teams through The Pearl River Talent Recruitment Program under Grant 2019ZT08X340. *(Corresponding author: Zhensen Gao.)*

Wenfu Gu, Xulin Gao, Anbang Wang, and Yuwen Qin are with the Advanced Institute of Photonics, School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China, and also with the Guangdong Provincial Key Laboratory of Photonics Information Technology, Guangzhou 510006, China (e-mail: 2112103076@mail2.gdut.edu.cn; 2112103031@mail2.gdut.edu.cn; qinyw@gdut.edu.cn).

Yuehua An is with the School of Optoelectronic Engineering, Guangdong Polytechnic Normal University, Guangzhou 510665, China (e-mail: anyuehua@163.com).

Yuncai Wang and Zhensen Gao are with the Advanced Institute of Photonics, School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China, also with the Guangdong Provincial Key Laboratory of Photonics Information Technology, Guangzhou 510006, China, and also with the Pengcheng Laboratory, Shenzhen 518052, China (e-mail: wangyc@gdut.edu.cn; gaozhensen@gdut.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2023.3279282

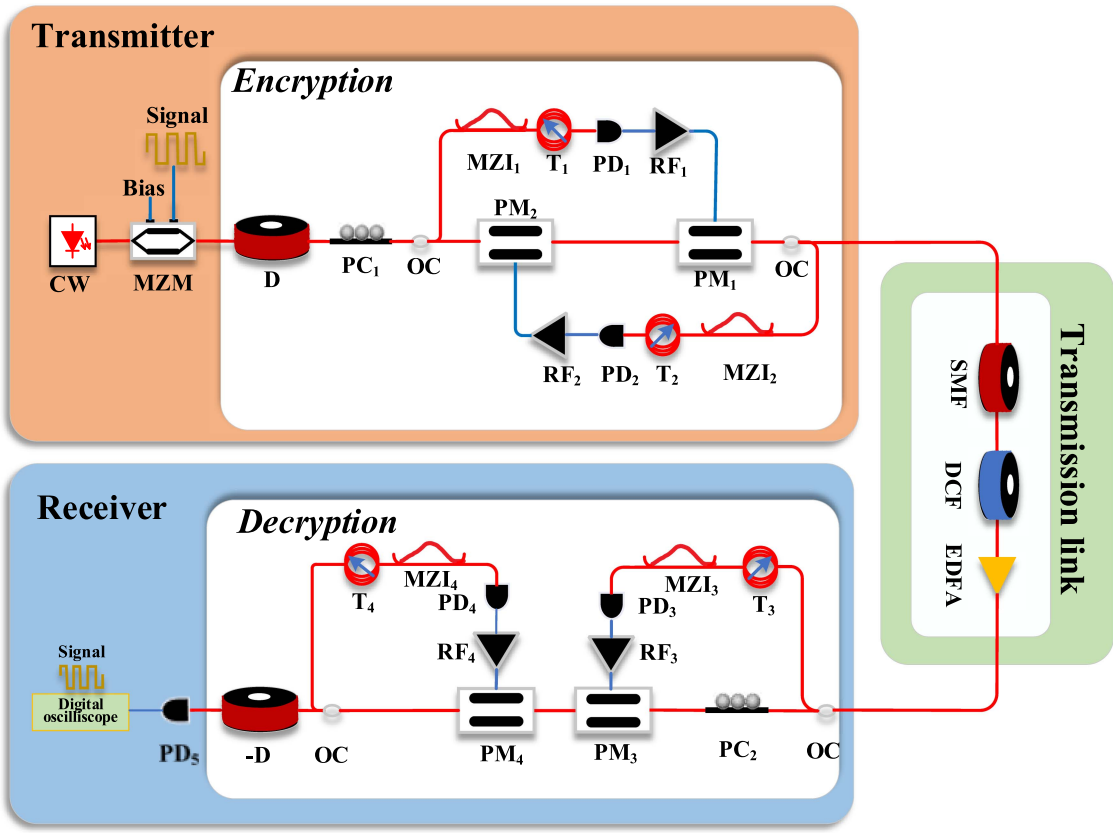

Fig. 1. Schematic diagram of the proposed system. CW, continuous-wave laser diode; MZM, Mach-Zehnder modulator; PC, polarization controller; D, dispersion; SMF, single-mode fiber; OC, optical coupler; PM, phase modulator; PD, photodetector; RF, radio-frequency amplifier; EDFA, erbium-doped fiber amplifier.

[19], [20], [21], [22], [23], utilizing external signals to scramble the signal [24], [25], performing nonlinear processing of the signal with the assistance of computers [26], [27], [28], and using multiple feedbacks to generate complex chaotic signals [29], [30]. However, these methods require additional devices including pseudo-random binary sequence (PRBS) generators, digital signal processing modules, and advanced key distribution between transmitter and receiver or external processing of the signal, which is detrimental to system integration. Meanwhile, high-quality synchronization needs to be achieved before using an open-loop structure decryption system, which encounters a certain difficulty to realize under the disturbance of external factors. Recently, Wang et al. ingeniously combined VCSELs with chaos to propose a secure communication system that generates feedback signals of different frequencies under varying optical modules to achieve TDS concealment [31]. Gao et al. proposed a system coupling several different feedback signals, whose single output can conceal the TDS. Yet it's notable that this system has more than one outlet, and the TDS can be obtained if the statistical analysis is performed between each output [29]. More recently, we have put forth a system founded on dual-loop electro-optic self-feedback phase encryption [32], aimed at eliminating TDS. Nevertheless, there remains a requirement for enhancements to the scheme's key space and transmission distance to attain superior performance.

In this paper, we propose and demonstrate a chaotic secure communication system based on dispersion with dual-phase electro-optic modulation to realize TDS concealment. The mutual coupling modulation of feedforward and feedback, along with the scrambling effect of dispersion in front, makes the signal behave as noise-like. The additional loops and dispersion greatly increase the key space which is 14 orders of magnitude larger than that of the classical EO system. The perturbation of the signal at the relevant time delays by the mutually coupled system is noticeable, thus engendering TDS suppression. After transmitting over 100 km on the SMF, decryption performance, parameter sensitivity and security analysis are illustrated. The numerical results show that the system is efficient and reliable within reasonable parameters, and a slight parameter mismatch has little impact on decryption, in which the security and robustness can simultaneously be considered, providing an effective strategy for future secure communication systems.

II. Schematic Structure and Mathematical Analysis

Fig. 1 depicts a schematic diagram for the secure communication scheme with TDS concealment which is divided into the transmitter, transmission link, and receiver. At the transmitter, a Mach-Zehnder modulator (MZM) seeded by a continuous wave semiconductor (CW) laser with a linewidth of 100 kHz is

responsible for modulating the original signal $m(t)$, where the center frequency is set as 1553.60 nm, the driving signal $m(t)$ is the OOK signal with the rate of 32 Gb/s. The MZM enables mapping electrical signals to carriers by altering the bias voltage.

Then, the signal is encrypted through the devices composed of dispersion and PM. Here, the dispersion value of 640 ps/nm is used to stretch the signal, detailed justifications for dispersion value selection are given in the next section. The introduced dispersion effect causes the signal stretching to be reflected as a distortion of the waves, leading to a noise-like characteristic. The undulating noise-like signal is used as the optical input to the PM, and the electrically driven signal is the time-delayed signal through T and δT. More specifically, the noise-like signal is split into two parts by a 50:50 coupler, with one part injected into the optical input of PM_1 and the other part into a branch consisting of time delay T_1, a Mach-Zehnder interferometer (MZI_1) with differential delay δT_1, a photodetector (PD_1) and a radio frequency amplifier (RF_1), then the output of PM_1 is split into two parts by a 50:50 with one part is fed back into PM_2 as its driving signal to modulate the signal again, the time delay parameters of this branch are T_2 and δT_2, which are different from the previous branch. In both branches, the MZI is responsible for converting the phase signal into the intensity signal, and the PD converts the optical signal into an electrical signal, which is finally amplified by the RF as the electrical drive signal of each PM. The other part is sent to the transmission link for long-distance transmission.

After encryption, the noise-like signal is transmitted through the transmission link which consists of SMF, dispersion compensating fiber (DCF) and erbium-doped fiber amplifier (EDFA). To compensate for the dispersion generated by the SMF, an 11.26 km DCF with a dispersion coefficient of -142 ps/nm is utilized, and an EDFA is employed as a compensator for attenuation, ensuring that power levels detected by the receiver are consistent with those of the transmitter.

At the receiver, two inverse closed-loop phase modulation loops with exact parameter matching are built to remove the encryption effect introduced at the transmitter using identical parameters. The signal received from the transmission link is split into two parts by a 50:50 coupler, one part is injected into PM_3 as a carrier, and the other part is converted into an electrical signal opposite to RF_1 after passing through T_3 and δT_3, while T_3 and δT_3 must be strictly the same as T_2 and δT_2. The same modulation is performed on PM_4, whose time delay parameters are the same as T_1 and δT_1. After demodulation in virtue of PM_3 and PM_4, the phase components attributed to the signal at the transmitter are all eliminated. Lastly, the original signal can be recovered by compensating for the dispersion D in the transmitter with inverse dispersion ($-$D) value. During the demodulation, the order between PM_3 and PM_4 cannot be changed, or else the correct message will not be obtained even if the parameters match.

At the transmitter, a standard 32 Gb/s OOK signal $m(t)$ is used to drive the intensity modulator, and the electric field expression at the output of the modulator can be expressed as:

$$E_0(t) = \sqrt{P_0} m(t) \exp(j\omega_0 t + \varphi_0) \tag{1}$$

Where ω_0 represents the angular frequency $\varphi_0 = p/2$; P_0 represents the optical power, which is set at 3 dBm here.

$E_0(t)$ will then be scattered, the frequency domain equation for dispersion is as follows:

$$D(\omega) = \exp\left[-2\pi \mathrm{j} \int \sigma_{\mathrm{d}}(\omega) d\omega\right] \tag{2}$$

where σ_d represents the group time delay introduced by dispersion; the noise-like signal after being stretched by dispersion is below:

$$c(t) = ifft^{-1}\left\{fft\left[E_0(t)\right] \cdot D(\omega)\right\} \tag{3}$$

where $fft[\cdot]$ is the fast Fourier transform and $ifft[\cdot]$ is the inverse fast Fourier transform.

Following the dispersion, the signal will be electro-optic phase modulated by the PM. As we know, the dynamical equations of the electro-optic chaotic system, also called the Ikeda equation [33], can be described as follows:

$$x(t) + \tau \frac{d}{dt} x(t) + \frac{1}{\theta} \int_{t_0}^{t} x(t) dt = \beta \cos^2[x(t-T) + \phi] \tag{4}$$

Here $x(t) = pV(t)/(2V_p), V(t)$ is the input physical input voltage for the PM; V_π is the bias half-wave voltage of the PM; $\tau = 1/(2\pi f_H)$ and $\theta = 1/(2\pi f_L)$ are the high cutoff time and low cutoff time of the bandpass filter formed by the feedback loop, which is controlled by the -3 dB cutoff bandwidth of the PD (30 KHz$-$10 GHz); $\beta = PgA\pi/(2V_\pi)$ is the feedback intensity of the circuit; *P* is the optical power entering the PM; *g* represents the amplification gain; *A* is the attenuation of the whole feedback loop; *T* is the delay time.

The chaotic system based on Ikeda's equations has a hyperchaotic system with high-dimensional attractors, and the dynamical equations of our proposed mutually injected chaotic system can be expressed as follows:

$$\begin{cases} a_1 = c_1(t - T_1) - c_1(t - T_1 - \delta T_1) + \phi_1 \\ b_1 = c_2(t - T_2) - c_2(t - T_2 - \delta T_2) + \phi_2 \\ c_1 + \tau \frac{dc_1}{dt} + \frac{1}{\theta} \int_{t_0}^{t} c_1(\xi) d\xi = \beta_1 \left[\cos^2(a_1)\right] \\ c_2 + \tau \frac{dc_2}{dt} + \frac{1}{\theta} \int_{t_0}^{t} c_2(\xi) d\xi = \beta_2 \left[\cos^2(b_1)\right] \end{cases} \tag{5}$$

where $c_1(t)$ and $c_2(t)$ represent the equations at RF_i (i = 1, 2), ϕ_1 and ϕ_2 are the static offset phases of MZI_1 and MZI_2, δT_1 and δT_2 are the differential time delays of MZI_1 and MZI_2, respectively. To receive the confidential signal, all components including the optical delay line, MZI, PD, and RF driver, must be identical to the transmitter.

III. Numerical Simulation Variables and Security Analysis

A. System Parameters Analysis

As an important encryption component, dispersion is indispensable in the whole encryption session. The original signal will effectively behave as a noise-like signal after dispersion encryption, forming the first layer of encryption. Therefore, it is crucial to investigate the impact of dispersion values for different rates. The BER for the stretched OOK signal reflects whether the

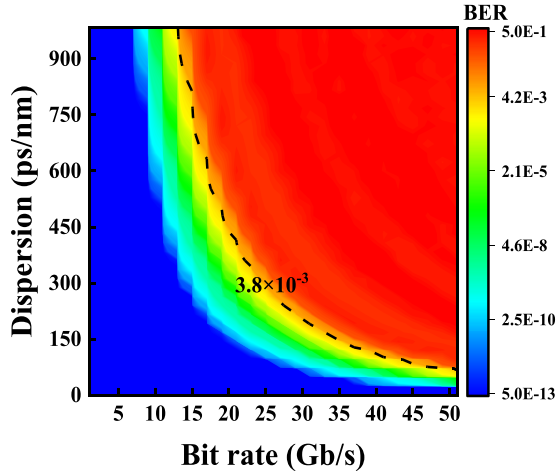

Fig. 2. The relationship between different signal bit rates and minimum cryptographic dispersion.

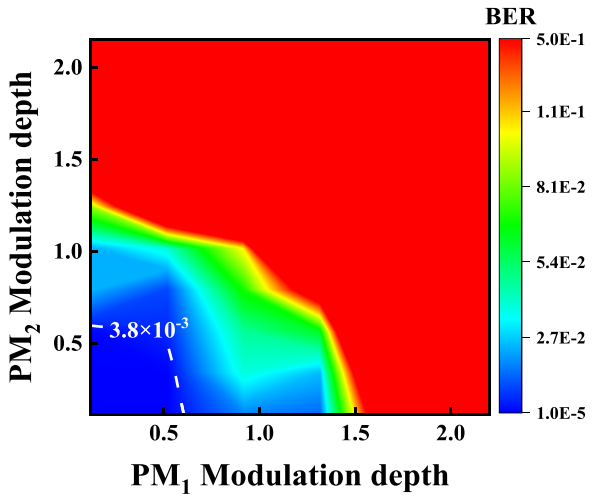

Fig. 3. The relationship between PM modulation depth and EVE's BER.

signal is encrypted or not. We use the hardware-decision forward error correction (HD-FEC) limit of 3.8×10^{-3} to estimate the encryption performance, in other words, when the BER is precisely above the limit, the minimum encryption dispersion is met. As shown in Fig. 2, the minimum dispersion required for time domain stretching is significantly different for various rates. In the case of our system, the value is about ∼250 ps/nm. The dispersion value in the subsequent sections is fixed at 640 ps/nm, which is intended to match the actual range of the device on the one hand and to attain better BER on the other hand, since the higher the dispersion value set, the worse the BER obtained.

To guarantee that each phase modulator works in the encryption state, the relationship between the modulation depth β and the degree of encryption is investigated. Similarly, the most intuitive BER data is to reflect the level of encryption as shown in Fig. 3, the modulator gradually works as the β of PM_1 and PM_2 increases, at which point the BER of the EVE rises rapidly without phase recovery. As can be seen from the scale in the figure, if the β of the two modulators is greater than 0.55, the BER of the EVE will be higher than the HD-FEC threshold of 3.8×10^{-3}. Therefore, the minimum β recommended for both PMs is greater than 0.6.

TABLE I
PARAMETER VALUES USED IN OUR SYSTEM

Symbol	Description	Value
ω_0	The center frequency of continuous wave laser	193.1 THz
τ	The high cutoff frequency of the equivalent bandpass filter	15.9 ps
θ	The low cutoff frequency of the equivalent bandpass filter	5.3 μs
D	The dispersion component	640 ps/nm
d	Dispersion coefficient of DCF	-142 ps/nm
β_1	The modulation depth of PM_1	0.89
β_2	The modulation depth of PM_2	0.95
T_1	The optical time-delay1	12 ns
T_2	The optical time-delay2	9 ns
δT_1	The differential delay of MZI_1	500 ps
δT_2	The differential delay of MZI_2	300 ps
L	The length of SMF	100 km
R	The bitrate of the message	32 Gb/s

The corresponding values of the simulation variables used in our system are shown in Table I.

B. TDS Concealment

Having investigated the system parameters, attention is now turned to time-delay concealment. Typically, the EVE cracks the intercepted signal by statistical analysis and then reconstructs the receiver with the relevant parameters to obtain the original information. Therefore, the confidentiality of the system also depends on the effective elimination of the TDS. There are two main statistical methods for capturing the time delay: ACF and DMI, which are defined as follows:

$$ACF(s) = \frac{\langle [x(t+s) - \langle x(t) \rangle] [x(t) - \langle x(t) \rangle] \rangle}{\sqrt{\langle (x(t) - \langle x(t) \rangle)^2 \rangle \langle (x(t+s) - \langle x(t) \rangle)^2 \rangle}} \quad (6)$$

where $< \cdot >$ stands for the mean value within the brackets

$$DMI(s) = \sum_{x(t),x(t+s)} \rho(x(t), x(t+s)) \log \frac{\rho(x(t), x(t+s))}{p(x(t))\rho(x(t+s))} \quad (7)$$

where $\rho(x(t))$ represents the probability function of $x(t)$, while $\rho(x(t), x(t+s))$ is the joint probability function, and s is the time delay of each branch.

To demonstrate the efficacy of our system in eliminating Time Delay Signature (TDS), Fig. 4 provides a comparison of the ACF (a) and DMI (b) of the classical electro-optic feedback system [34] versus our proposed system simultaneously. Cryptographic signals analyzed through statistical methods of ACF and DMI show a clear peak exposure (black line) at 9 ns and 12 ns for the classical electro-optic system, which is the relevant time delay set in the system, EVE can break the system through this delay and other parameters to capture the original information easily.

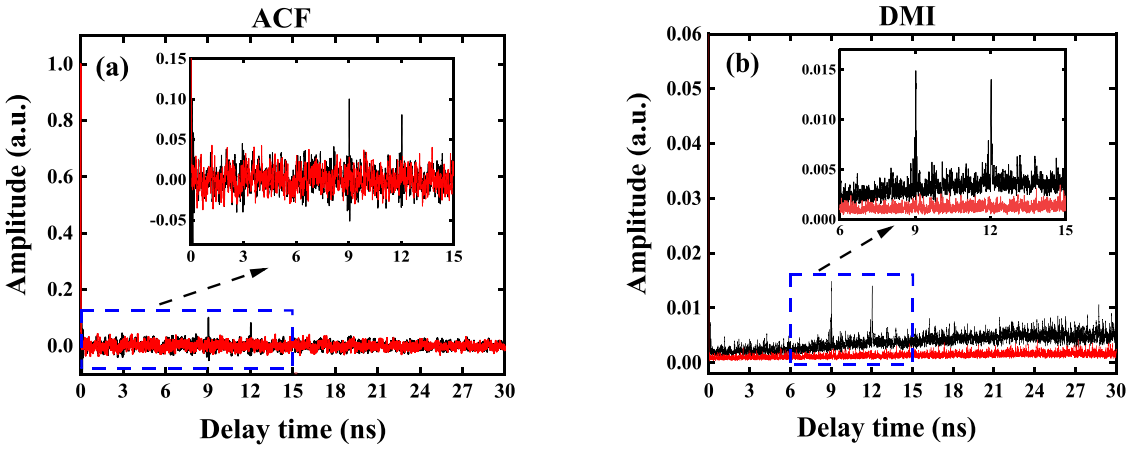

Fig. 4. The statistical analysis of the classical system (black line) and our proposed system (red line) with ACF (a) and DMI (b) (the small figure is partial enlargement).

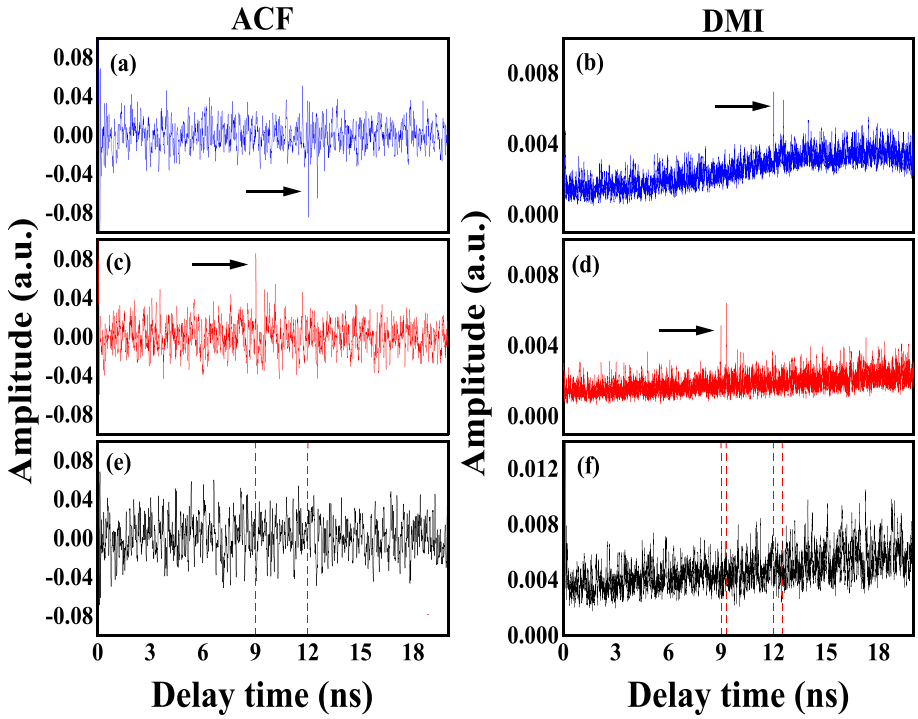

Fig. 5. ACF (left column) and DMI (right column) curves for individual and interactive interactions. ACF curve at T_1 only (a); ACF curve at T_2 only (c); ACF curve with T_1 and T_2 (e); DMI curve at T_1 only (b); DMI curve at T_1 only (d); DMI curve at T_1 only (f).

On the contrary, after the encryption of our proposed system, the peak of the corresponding TDS is notably eliminated, which illustrates the effectiveness of our architecture (red line), furthermore, greatly improves the security performance of the system.

For a better understanding of the effectiveness of the system for TDS concealment, a discussion of the critical contributions of the two branches in TDS concealment is carried out next. As shown in Fig. 5, the curve of ACF is shown on the left column, and the corresponding curve of DMI is shown on the right column. When $\beta_2 = 0$, in other words, the branch where T_2 is placed is not involved in encryption, as shown in (a) (b), the time delay peaks can be detected at $T_1, T_1 + \delta T_1$. When $\beta_1 = 0$, namely the branch where T1 is not participating in the modulation, as depicted in (c) (d), distinct peaks above the nearby can be detected at $T_2, T_2 + \delta T_2$ as well. On the contrary, with two branches working together, as in Fig. 5(e) and (f), the ACF and DMI functions can't recognize the peaks at $T_1, T_2, T_1 + \delta T_1, T_2 + \delta T_2$. That is to say, it's the interactive effect of the two branches that can virtually solve the problem of TDS leakage, and without any of the introduction of the two loops to modulate the signal, the successful elimination of the TDS can't be achieved although the parameters are reasonably

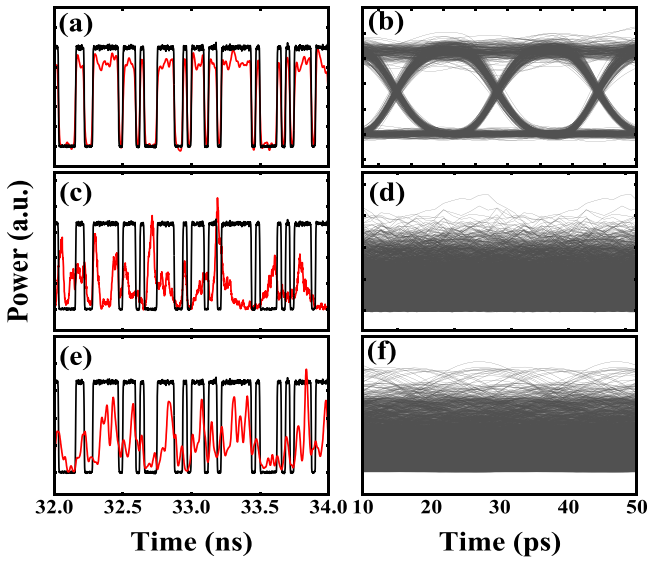

Fig. 6. Original signal (black line) vs. decrypted waveform (red line) and eye diagram; (a) original waveform vs. correctly decrypted waveform; (b) correctly decrypted eye diagram; (c) directly decrypted waveform on transmission link vs. original waveform; (d) directly decrypted eye diagram; (e) waveform of EVE with mismatched parameters vs. original waveform; (f) eye diagram of EVE with mismatched parameters.

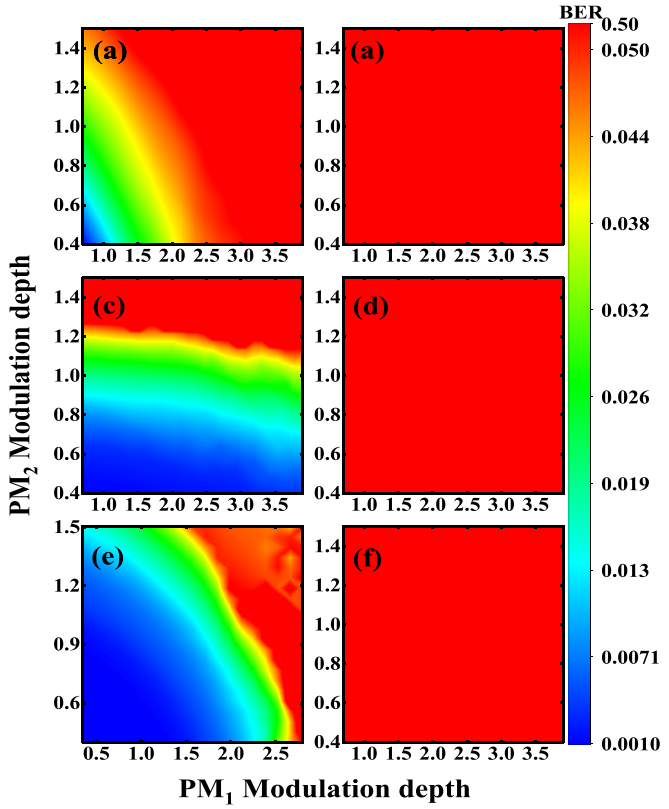

Fig. 7. Eavesdropper BER; (a) compensated dispersion D in the transmission link; (b) without compensation of dispersion D in the transmission link; (c) compensated dispersion D after PM_3; (d) without compensation of dispersion D after PM_3; (e) without compensation of dispersion D and with PM_4 only; (f) compensated dispersion D and with PM_4 only.

set. This means that its TDS cannot be captured by general statistical analysis, which greatly enhances the security of the system. Remarkably, the effective concealment of the TDS can be explained by the fact that the high-speed chaotic signal interactions enhance the signal nonlinearity, resulting in each delay signal being effectively concealed by another.

IV. Chaotic Communication and Results Analysis

A. Communication Performance

In this section, we will discuss the communication performance of the system after the effective concealment of TDS.

Fig. 6 shows the different scenarios of transmission with 32 Gb/s OOK signals transmitted over 100 km. With the parameters of the receiver matching with those of the transmitter, the decrypted waveform (red line) is recorded in compound with the original waveform (black line) in Fig. 6(a), and its eye diagram is depicted in (b), from which can be seen that the recovered waveform after decryption is basically the same as the original waveform, and the eye diagram is completely opened. In contrast, the acquired waveform is out of order altogether and the eye diagram is fully closed for EVEs that intercept signals directly on the transmission link (Fig. 6(c) and (d)) or after collecting part of the hardware parameters (Fig. 6(e) and (f)), indicating that the security of our proposed system can be effectively guaranteed.

To further explain the security of our proposed system, several points on the link are targeted to simulate a practical EVE to capture the signal. Unlike the previous waveforms and eye diagrams, the BER of the detected signal is used in Fig. 7 to represent the leakage of confidential data. The illegal interception of the encrypted signal is first performed in the transmission link with the dispersion precisely compensated as the BER illustrated in (a), while (b) presents the situation without dispersion compensation. Moreover, (c) and (d) describes the BER obtained by detecting the signal after PM_3 with and without dispersion compensation, which means that the path parameter of PM_4 is invalidated. On the contrary, (e) and (f) depict the BER obtained in the case where only PM_4 is decrypting the signal. From the diagrams, we can conclude that the BER of the EVE can reach the order of 10^{-1} when the β is small, indicating the PM is not effective, yet it is already well above 3.8×10^{-3}. Slightly increasing the β will cause the BER to rise and approach 0.5 rapidly. Without accurate dispersion matching with the transmitter, the BER will always keep at around 0.5, no matter how it changes, meaning that the decrypted signal is thoroughly cluttered. The above 4 scenarios prove that our system has reliable anti-eavesdropping performance.

B. Effect of Parameter Mismatch

Having discussed the security performance, we turn to the sensitivity of the system toward parameter mismatch. In practical systems, minor parameter mismatches are inevitable, therefore a discussion of the key parameters of the system can help us to have a more comprehensive knowledge of the system.

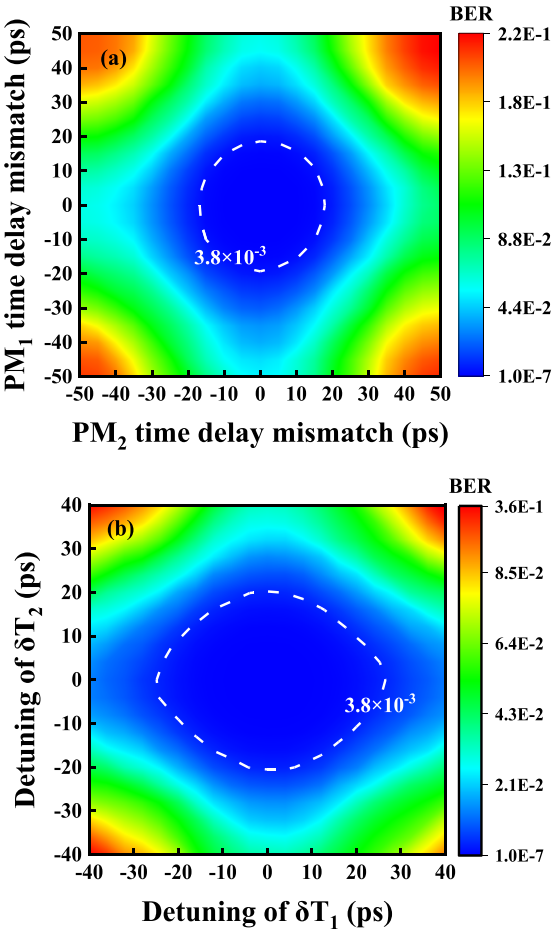

Fig. 8. (a) The delay mismatch VS legitimate decryption BER; (b) variation of BER with T_1 and T_2 mismatches ($\beta_1 = 0.89$ & $\beta_2 = 0.95$).

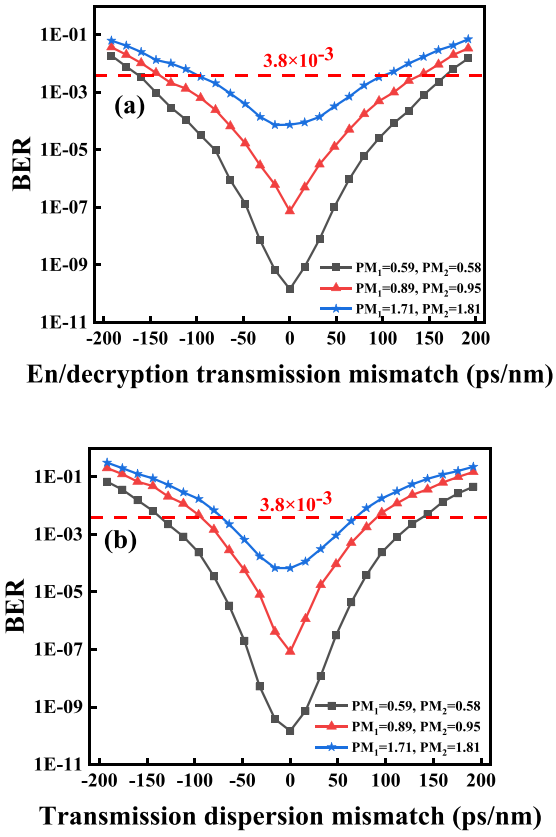

Fig. 9. BER effect of dispersion mismatch at varying modulation depths; (a) en/decryption dispersion mismatch; (b) Transmission dispersion mismatch.

As a crucial parameter, the time delay mismatch is first discussed and demonstrated. Fig. 8(a) represents the BER of decrypted signal with the increase of time delay detuning, where β_1 is fixed at 0.89 and β_2 is 0.95. A slight delay mismatch between transceivers is acceptable, but once the delay of T_3 and T_4 is different from that of the transmitter, detuning beyond about ± 20 ps, the decryption BER will be higher than the threshold of HD-FEC, implicating that the information received is unreliable.

Differential delay mismatch of MZI also has a significant impact on the system which is necessary to discuss. Under the same conditions as Fig. 8(a), the relevant data are measured as shown in Fig. 8(b), which indicates that the mismatch of δT_2 is about ± 20 ps, 40 ps in total, while the mismatch tolerance of δT_1 is ± 5 ps larger than that of δT_2.

The analysis of the delay parameters above shows that the particular acquisition of time delay for decryption is essential. For illegal users, the attempt of extraction without a certain key is extremely difficult, while for legitimate users, the time delay can be easily matched thanks to the accuracy of commercial tunable delay lines that can reach the femtosecond level. Since the TDS of this system is completely concealed, the time delay can be used as a crucial key.

With a long-distance transmission of over 100 km, the effects of fiber including dispersion and attenuation will cause unpredictable degradation at the receiver. Therefore, the dispersion mismatch on the receiver must be investigated in the following section. The BER for en/decryption dispersion mismatch (a) and transmission dispersion mismatch (b) are illustrated in Fig. 9, the maximum mismatch tolerance of en/decryption dispersion (a) is about ± 160 ps/nm at $\beta_1 = 0.59$ & $\beta_2 = 0.5$, with the increase of β, the sensitivity of the system to the parameters will also increase, and the maximum tolerance to the decryption dispersion will drop to about ± 96 ps/nm at $\beta_1 = 1.71$ & $\beta_2 = 1.81$. Similarly, the same trend can be observed for the transmission dispersion mismatch, in which the maximum tolerance to dispersion diminishes from ± 140 ps/nm to ± 64 ps/nm for the same conditions. This phenomenon can be explained by the fact that long-distance transmission links introduce more nonlinearities to the signal resulting in a greater sensitivity to mismatches.

At last, we estimated and calculated the expansion of the key space by performing the method as same as that in [35], A delay of several hundred nanoseconds can be easily set in our system without an external device, and for the differential time of MZI, the setting space of several hundred picoseconds can be achieved. The setting range of delay time and the differential time of MZI can be denoted by T_R and the cracking accuracy down to 1 ps that the illegal user can achieve will be expressed by T_E, so the key space of delay time and differential time is around $(T_R/T_E) \times (T_R/T_E)_{\delta T} = 10^5 \times 10^3$.

As another key, the amount of dispersion is also vulnerable to brute force cracking by the illegal user. In the laboratory, dispersion values can reach the order of several thousand ps/nm, and the minimum cracking accuracy is 1 ps/nm, so the key space that dispersion can provide is $(D_R/D_E) = 10^3$. Through the above analysis, we can calculate the total key space of the proposed system as $(D_R/D_E) \times [(T_R/T_E)_T \times (T_R/T_E)_{\delta T}]^2 = (10^3) \times (10^5 \times 10^3)^2 = 10^{19} = 2^{63}$. Therefore, the key space is 14 orders of magnitude higher than the classical EO system whose key space is calculated merely by $(T_R/T_E)_T$.

V. Conclusion

In conclusion, an electro-optic chaotic encryption scheme with dual-phase modulation is proposed. Numerical results show that TDS can be eliminated when the two branches are modulated in conjunction which greatly enhances the security of the system, on this basis, the encrypted 32 G/s OOK signal was successfully transmitted over 100 km. The combination of dispersion and mutual injection of the encryption devices introduces more tunable parameters, making the key space of the proposed system up to 2^{63}, about 14 orders of magnitude larger than the classical EO system [34]. The impact on the decryption effect when the system hardware parameters are not properly matched is discussed in detail, the delay mismatch tolerance is approximately ± 20 ps indicated by the tolerance range of BER, and the maximum mismatch tolerance of dispersion is roughly ± 160 ps/nm. Considering the great superiority of this dispersion spreading and mutual injection modulation method in guaranteeing communication security and enhancing the key space, it can be more widely used in the future.

References

[1] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[2] F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, "Experimental long-distance quantum secure direct communication," *Sci. Bull.*, vol. 62, no. 22, pp. 1519–1524, 2017.

[3] L. Zhang, B. Liu, and X. Xin, "Secure optical generalized filter bank multi-carrier system based on cubic constellation masked method," *Opt. Lett.*, vol. 40, no. 12, pp. 2711–2714, 2015.

[4] R. M. Nguimdo, R. Lavrov, P. Colet, M. Jacquot, Y. K. Chembo, and L. Larger, "Effect of fiber dispersion on broadband chaos communications implemented by electro-optic nonlinear delay phase dynamics," *J. Lightw. Technol.*, vol. 28, no. 18, pp. 2688–2696, Sep. 2010.

[5] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nature Photon.*, vol. 9, no. 3, pp. 151–162, 2015.

[6] A. Argyris et al., "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, 2005.

[7] R. Lang and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," *IEEE J. Quantum Electron.*, vol. QE-16, no. 3, pp. 347–355, Mar. 1980.

[8] N. Jiang, A. Zhao, S. Liu, C. Xue, and K. Qiu, "Chaos synchronization and communication in closed-loop semiconductor lasers subject to common chaotic phase-modulated feedback," *Opt. Exp.*, vol. 26, no. 25, pp. 32404–32416, 2018.

[9] P. Jiang, P. Zhou, N. Li, P. Mu, and X. Li, "Optically injected nanolasers for time-delay signature suppression and communications," *Opt. Exp.*, vol. 28, no. 18, pp. 26421–26435, 2020.

[10] T. Yamamoto et al., "Common-chaotic-signal induced synchronization in semiconductor lasers," *Opt. Exp.*, vol. 15, no. 7, pp. 3974–3980, 2007.

[11] A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, "Generation of synchronized wideband complex signals and its application in secure optical communication," *Opt. Exp.*, vol. 28, no. 16, pp. 23363–23373, 2020.

[12] D. Wang et al., "Time delay signature elimination of chaos in a semiconductor laser by dispersive feedback from a chirped FBG," *Opt. Exp.*, vol. 25, no. 10, pp. 10911–10924, 2017.

[13] R. Lavrov, M. Jacquot, and L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications," *IEEE J. Quantum Electron.*, vol. 46, no. 10, pp. 1430–1435, Oct. 2010.

[14] Y. Fu et al., "High-speed optical secure communication with an external noise source and an internal time-delayed feedback loop," *Photon. Res.*, vol. 7, no. 11, pp. 1306–1313, 2019.

[15] G. Zou, H. Wang, and Y. Ji, "Electro-optic chaos system with time delay signature concealment based on XOR operation and multi-bit PRBS," *Opt. Exp.*, vol. 29, no. 5, pp. 7327–7341, 2021.

[16] V. S. Udaltsov, J. P. Goedgebuer, L. Larger, J. B. Cuenot, P. Levy, and W. T. Rhodes, "Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations," *Phys. Lett. A*, vol. 308, no. 1, pp. 54–60, 2003.

[17] 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, no. 5, pp. 373–377, 2005.

[18] M. D. Prokhorov, V. I. Ponomarenko, A. S. Karavaev, and B. P. Bezruchko, "Reconstruction of time-delayed feedback systems from time series," *Physica D-Nonlinear Phenomena*, vol. 203, no. 3/4, pp. 209–223, 2005.

[19] D. Rontani, M. Sciamanna, A. Locquet, and D. S. Citrin, "Multiplexed encryption using chaotic systems with multiple stochastic-delayed feedbacks," *Phys. Rev. E*, vol. 80, no. 6, 2009, Art. no. 066209.

[20] H. Hu, W. Su, L. Liu, and Z. Yu, "Electro-optic intensity chaotic system with varying parameters," *Phys. Lett. A*, vol. 378, no. 3, pp. 184–190, 2014.

[21] H. Hu, S. Shi, and F. Xie, "Electro-optic intensity chaotic system with an extra optical feedback," *Opt. Commun.*, vol. 402, pp. 140–146, 2017.

[22] L. Liu, S. Miao, M. Cheng, and X. Gao, "Two-dimensional coupled electro-optic delayed feedback system with varying parameters," *J. Mod. Opt.*, vol. 64, no. 6, pp. 547–554, 2017.

[23] Y. Lv, N. Jiang, D. Liu, C. Xue, and K. Qiu, "Energy-efficient scheme based on sub-band grouping and allocating for digital filter multiple access adopted PON," *IEEE Photon. J*, vol. 9, no. 3, Jun. 2017, Art. no. 7904009.

[24] R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, "Digital key for chaos communication performing time delay concealment," *Phys. Rev. Lett.*, vol. 107, no. 3, 2011, Art. no. 034103.

[25] R. M. Nguimdo and P. Colet, "Electro-optic phase chaos systems with an internal variable and a digital key," *Opt. Exp.*, vol. 20, no. 23, pp. 25333–25344, 2012.

[26] 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.

[27] Y. Huang, H. Hu, F. Xie, and J. Zheng, "An innovative electro-optical chaotic system using electrical mutual injection with nonlinear transmission function," *IEEE Photon. J*, vol. 10, no. 1, Feb. 2018, Art. no. 7900112.

[28] Z. Yang, J. Ke, Q. Zhuge, W. Hu, and L. Yi, "Coherent chaotic optical communication of 30 Gb/s over 340-km fiber transmission via deep learning," *Opt. Lett.*, vol. 47, no. 11, pp. 2650–2653, 2022.

[29] X. Gao, M. Cheng, L. Deng, L. Liu, H. Hu, and D. Liu, "A novel chaotic system with suppressed time-delay signature based on multiple electro-optic nonlinear loops," *Nonlinear Dyn.*, vol. 82, no. 1/2, pp. 611–617, 2015.

[30] X. Zhu et al., "An optically coupled electro-optic chaos system with suppressed time-delay signature," *IEEE Photon. J.*, vol. 9, no. 3, Jun. 2017, Art. no. 6601009.

[31] H. Wang, T. Lu, and Y. Ji, "Key space enhancement of a chaos secure communication based on VCSELs with a common phase-modulated electro-optic feedback," *Opt. Exp.*, vol. 28, no. 16, pp. 23961–23977, 2020.

[32] B. Tang et al., "Time-delay signature concealment in a security-enhanced optical system with dual-loop electro-optic self- feedback phase encryption," *IEEE Photon. J*, vol. 15, no. 1, Feb. 2023, Art. no. 7200508.

[33] K. Ikeda and K. Matsumoto, "High-dimensional chaotic behavior in systems with time-delayed feedback," *Physica D*, vol. 29, no. 1, pp. 223–235, 1987.

[34] Y. C. Kouomou, P. Colet, L. Larger, and N. Gastaud, "Chaotic breathers in delayed electro-optical systems," *Phys. Rev. Lett.*, vol. 95, no. 20, 2005, Art. no. 203903.

[35] J. Bai, H. Wang, and Y. Ji, "Time-delay signature concealing electro-optic chaotic system with multiply feedback nonlinear loops," *Opt. Exp.*, vol. 29, no. 2, pp. 706–718, 2021.