Security-Enhanced Chaotic Optical Communication Based on External Temporal Self-Feedback Hardware Encryption and Decryption

Zhensen Gao, Biao Su, Sile Wu, Lei Liao, Zhaohui Li, Yuncai Wang, and Yuwen Qin

***Abstract*— Chaotic optical communication based on conventional external cavity semiconductor laser is a very promising solution for physical layer secure communication. However, the intrinsic time delay signature (TDS) associated with the external cavity length and the potential direct linear filtering (DLF) or synchronization utilization attack greatly threaten the system security. In this work, we propose and numerically demonstrate a novel scheme for TDS suppression and security enhancement of chaotic optical communication based on external temporal self-feedback hardware encryption and decryption. In this scheme, the confidential chaotic modulated signal is temporally scrambled in the time domain by two optical dispersion components and an electro-optic self-feedback phase modulation loop between them, which simultaneously conceal the TDS and enhance the security against malicious attacks. Proof-of-principle demonstration for a security enhanced chaotic optical communication system with error free transmission is successfully achieved. The proposed scheme may provide a promising way for pure-hardware based physical secure chaotic optical communication systems.**

***Index Terms*—Optical communications, optical encryption, chaos, semiconductor lasers.**

I. Introduction

CHAOTIC communication has received extensive attention because of its advantages for physical layer security over the past decades. Due to the noise-like temporal feature of chaos, it is very promising to use chaos as a means of encryption for secure optical communication. As early as 1990, Pecora and Carroll proposed a chaotic synchronization system [1], which has led to a shift in the gaze towards the protection of data exchange for optical communications to chaos, in search of more secure methods of communication. Until 2005, Argyris et al. experimentally verified the feasibility of chaotic secure optical communication in a commercial optical network in Athens [2]. The success of this experiment reinforced various innovative investigations on chaotic optical communication [3]. Wang et al. later demonstrated a chaotic communication system with an all-optical distributed feedback chaotic laser [4]. Wu et al. demonstrated a bidirectional chaotic communication system employing all-optical chaos for message encryption and decryption [5]. Lavrov et al. demonstrated an electro-optic phase chaos based chaotic communication system [6]. More recently, Ke et al. successfully demonstrated high speed chaotic optical communication utilizing a Mach-Zehnder modulator based electro-optic feedback chaotic transmitter [7].

In a typical chaotic optical communication system, the chaotic transmitter is the key optical component that generates a noise-like and broadband chaotic optical carrier for signal concealment. External-cavity semiconductor laser (ECSL) is a very popular and simple approach for chaotic transmitter, which generates a chaotic optical carrier by employing an external feedback cavity such as fiber mirrors or fiber Bragg grating, etc [8], [9]. However, since the reflected feedback light is a linear replica of the output light, the generated chaos will have a certain periodicity that represents the length of the external feedback cavity, leading to the time delay signature (TDS) problem in an ECSL. By employing autocorrelation function (ACF), delayed mutual information (DMI) and power spectrum analysis of the ECSL generated chaos, it is very easy to obtain the TDS and extract the external cavity length of the ECSL, thus leading to security risk of cracking the chaotic communication system [10]–[11]–[12]. Previously, a lot of innovative solutions for the TDS suppression have been reported [13]–[14]–[15]–[16]–[17]–[18]–[19], including the use of complex external feedback cavity such as chirped fiber Bragg grating (CFBG) [20], double cavity with two feedback mirrors [21], fiber random grating induced distributed feedback [22], phase modulated feedback [23], parallel ring-resonator feedback [24], using external optical injection [25], or performing external modulation with an extra driving signal [26]. In the traditional approaches, it is noted

Manuscript received 14 July 2022; revised 4 August 2022; accepted 10 August 2022. Date of publication 15 August 2022; date of current version 22 August 2022. This work was supported in part by the National Key R&D Program of China under Grant 2020YFB1806401, in part by the National Natural Science Foundation of China under Grants U2001601, 11904057, and 62004047, in part by the Basic and applied basic research project of Guangzhou Basic Research Program under Grant 202102020506, in part by the Research and Development Plan in Key Areas of Guangdong Province under Grant 2018B010114002, and in part by the Guangdong Introducing Innovative and Enterpreneurial Teams of The Pearl River Talent Recruitment Program under Grant 2019ZT08X340. *(Corresponding author: Yuncai Wang.)*

Zhensen Gao, Biao Su, Sile Wu, Lei Liao, Yuncai Wang, and Yuwen Qin are with the Advanced Institute of Photonics, School of Information Engineering, Guangdong University of Technology, 510006 Guangzhou, China, and also with the Guangdong Provincial Key Laboratory of Photonics Information Technology, 510006 Guangzhou, China (e-mail: gaozhensen@gdut.edu.cn; 2112103090@mail2.gdut.edu.cn; 2112003102@mail2.gdut.edu.cn; 2112003064@mail2.gdut.edu.cn; wangyc@gdut.edu.cn; qinyw@gdut.edu.cn).

Zhaohui Li is with the School of Electrical and Information Technology, Sun Yat-Sen University, Guangzhou 510006, China (e-mail: lzhh88@mail.sysu.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2022.3198527

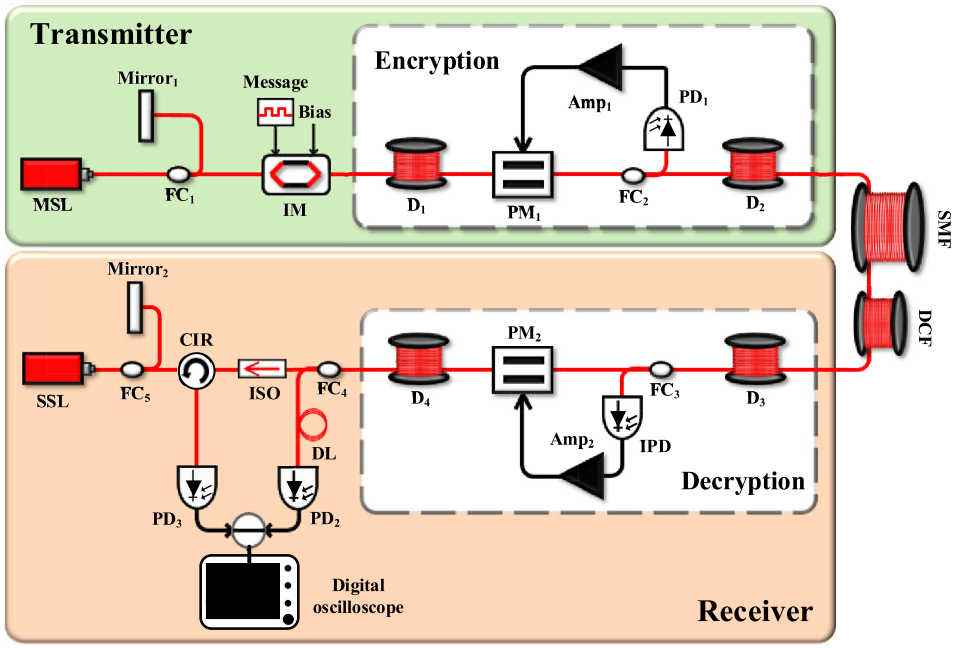

Fig. 1. Schematic of the proposed security enhanced chaotic optical system. MSL, master semiconductor laser; SSL, slave semiconductor laser; FC, fiber coupler; IM, intensity modulator; PM, phase modulator; PD, photo-detector; Amp, radio-frequency amplifier; SMF, single mode fiber; DCF, dispersion compensation fiber; IPD, inverted photo-detector; ISO, optical isolator; DL, optical delay line; CIR, circulator.

that the general idea of suppressing the TDS is to break the inherent time delay characteristics of the feedback chaotic signal in the external cavity by changing the external cavity structure of the chaotic laser, randomly modulating the feedback signal inside the cavity, or adding hardware modules inside the cavity of the chaotic transmitter. Since the reflected feedback signal inside the cavity is no longer a simple replica of the chaotic signal output from the laser, the temporal periodicity and the corresponding TDS can be greatly suppressed. Nevertheless, such methods potentially suffer from the problems of high implementation complexity, reduced robustness and stability of chaotic synchronization, which directly limit the applications for chaotic communication systems. It is essential to explore novel innovative solution for TDS suppression with high quality synchronization and robustness for ECSL to be applied in chaotic communication systems.

Besides the TDS issue, the traditional chaotic communication systems also face several other potential security threats. It has been revealed that when the optical chaos is used as a carrier of the message to transmit information at a relatively low transmission rate, direct liner filtering (DLF) attack can be used to intercept part of the confidential information via setting the cut-off frequency of a low-pass filter equaling to the transmission bit rate [27]. An alternative attacking method is synchronization utilization attack [28], which firstly separates the chaotic modulated signal from the public transmission link and then injects it into a non-perfectly matched attack receiver to perform synchronization with the captured transmitted chaotic signal. Due to the injection locking mechanism, this illegal attack laser is also possible to intercept the message by subtracting the generated synchronization signal with the received signal separated from the common link [29], [30]. Therefore, it is desirable to enhance the security of chaotic communication systems to resist the above-mentioned security attacks.

In this paper, a novel security-enhanced chaotic optical communication scheme is proposed, which is realized by introducing external temporal self-feedback hardware encryption outside the ECSL. A pair of optical dispersion components and an electro-optic feedback phase modulation loop between them is constructed as a hardware encryption module to encrypt the transmitted chaotic modulated signal, so as to greatly enhance the security of confidential information whilst effectively suppressing the TDS. The cross-correlation coefficient of the chaotic signals before and after the hardware encryption is only $\sim$0.06, which is powerful to resist against eavesdroppers employing the DLF attack and the synchronization utilization attack. Successful demonstration of security enhancement for a chaotic optical communication system with the external hardware encryption and decryption is achieved. The proposed scheme can be fully compatible with commercial fiber-optic components and operated in a pluggable manner, exhibiting great potential for future physical layer security optical communication systems.

II. Principle and System Architecture

Fig. 1 illustrates the operating principle and system architecture of the proposed secure-enhanced chaotic optical communication system. At the transmitter side, a master semiconductor laser (MSL) with an external feedback mirror is used to form an ECSL and generate an optical chaos, which is output from a fiber coupler (FC_1) and employed as the original chaotic carrier (C). The roundtrip delay time of the external feedback mirror is denoted as τ_1. A Mach-Zehnder (MZM) optical intensity

modulator (IM) is used to modulate a 2.5 Gbit/s non-return-to-zero (NRZ) confidential message (*m*) onto the chaotic carrier, producing a chaotic modulated signal (carrier+message: *C*+*m*). The confidential signal to be transmitted is then directed into the proposed external temporal self-feedback hardware encryption module, which consists of two optical dispersion components and an electro-optic self-feedback loop based on a phase modulator in between them to perform temporal scrambling of the chaotic confidential signal. In the hardware encryption module, the first dispersive element (D_1) is to stretch the intensity-modulated chaotic signal in the time domain due to the chromatic dispersion. Conventional chirped fiber Bragg grating or dispersive fiber can be used as the dispersion element. Then, the temporal stretched chaotic signal is injected into an electro-optic phase modulator (PM_1) based self-feedback loop, which firstly phase modulate the injected signal by the PM_1 and then divide it into two portions by a fiber coupler (FC_2). One portion is directly used for secure transmission, while the other portion is converted into an electrical signal by a photo-detector (PD_1). The electrical signal is further amplified by a radio-frequency amplifier (Amp_1) and delayed by a delay time of τ_2 before feeding back to drive the PM_1, so that the stretched chaotic signal is self-phase modulated by its time delayed signal and further transformed to an intensity scrambled noise-like signal due to phase to intensity conversion by passing through another dispersion element with a dispersion value of D_2. Therefore, the original chaotic modulated signal is redistributed in the time domain and the TDS of the external cavity can be greatly suppressed. The values of dispersion components, the round-trip time delay in the feedback loop and phase modulation depth contribute to the hardware encryption parameters together. For a malicious eavesdropper without the whole matched hardware module or just using a part of the hardware module for decryption, she can only get an intensity scrambled noise-like signal, which sufficiently guarantees the security of confidential chaotic signals at the physical layer.

Mathematically, the electrical field of the intensity modulated chaotic signal $E_0(t)$ can be expressed as follows:

$$E_0(t) = \sqrt{p_0} m(t) \exp(j\omega_0 t + \theta) \tag{1}$$

Where P_0 is the output optical power of the MSL, $m(t)$ is the confidential data to be transmitted, $\omega_0 = 2\pi f_0$ is the original angle frequency, θ is the constant phase shift. The introduction of the D_1 will cause the chaotic modulated signal to be stretched in the time domain. The transfer function of the D_1 can be described in the frequency domain as:

$$H_{D1}(\omega) = \exp\left[j\frac{B_1}{2}(\omega - \omega_0)^2\right] \tag{2}$$

Where B_1 is the dispersion coefficient of D_1. The output of D_1 can be represented by

$$E_{D1}(t) = F^{-1}\left[F(E_0(t)) \cdot H_{D1}(\omega)\right] \tag{3}$$

Where $F(\cdot)$ stands for Fourier transform, $F^{-1}(\cdot)$ stands for Fourier inverse transform. After the phase encryption, the output signal E_{pm} can be expressed as:

$$E_{pm}(t) = E_{D1}(t) exp[i\varphi(t)] \tag{4}$$

$$\varphi(t) = K_{PM1} N\left[|E(t - \Delta t_x)|^2\right] \cdot \pi \tag{5}$$

Where $\varphi(t)$ is the phase shift introduced by the phase modulator, K_{PM1} is the modulation depth of the phase modulator, $N[|E(t-\Delta t_x)|^2] \cdot \pi$ is the normalized electrical driving signal, Δt_x represents the time delay of the driving signal which is caused by the associated the fiber loop and O-E conversions. Similarly, the transfer function of the second dispersion component (D_2) can be described as:

$$H_{D2}(\omega) = \exp\left[j\frac{B_2}{2}(\omega - \omega_0)^2\right] \tag{6}$$

Where B_2 is the dispersion coefficient of D_2. The final encrypted signal $E_{D2}(t)$ in the time domain after D_2 can be expressed as:

$$E_{D2}(t) = F^{-1}\left[F(E_{pm}(t)) \cdot H_{D2}(\omega)\right] \tag{7}$$

The encrypted chaotic confidential signal is then directed into a fiber transmission link, which consists of a span of single mode fiber (SMF) and corresponding dispersion compensation fiber (DCF). At the receiver side, a legitimate user firstly needs to employ a dispersion component (D_3) with opposite dispersion value of D_2 to remove the dispersion effect of D_2. Then, the signal is similarly split into two portions by a fiber coupler (FC_3), where one portion is injected into PM_2 for phase decryption, and the rest of the signal is time delayed by τ_3 with an identical delay time of τ_2 as the transmitter and converted to an electrical signal by an inverted photo-detector (IPD), which subsequently outputs an inverted signal from its differential output port to drive the PM_2. By properly controlling the modulation depth of PM_2 and the delay time inside the self-feedback loop, the imposed phase signature on the encrypted chaotic signal would be erased by decryption loop, leaving only the time stretched chaotic signal. Another dispersion components (D_4) with an opposite dispersion value of D_1 is used for compensating and decrypting the encrypted signals to recover the original chaotic modulated signal.

Finally, the decrypted chaotic modulated signal is divided into two portions by the FC_4, where a portion of the signal is unidirectionally injected into the SSL with the identical structure as the MSL to generate the synchronous chaotic carrier signal, while the other portion is directed into an optical delay line (DL) to compensate for the delay time with the other path. The two optical signals from different paths are converted to electrical signals, and then electrical subtraction is performed to extract the original confidential message (*m*) for eventual bit error rate analysis. To verify the principle and investigate the system performance, a simulation system is established by using the commercial optical system simulator VPI Transmission Maker 11.1, which employs the well-known embedded fourth-order Runge-Kutta algorithm to solve the differential equations. The VPI simulation time window is set as 100 ns and the sample mode bandwidth is the default value of 1280 GHz which corresponds to a time step size of 0.78125 ps, resulting a total data

TABLE I
VALUES OF PARAMETERS USED IN THE SIMULATION SYSTEM

Parameter	Description	Value
f_0	Center frequency of ECSL	193.1 THz
M_D	Modulation depth of PM_1	2.8
M	Modulation depth of IM	0.19
τ_p	Photon lifetime of ECSL active region	2 ps
τ_n	Carrier lifetime of ECSL active region	2 ns
R	Bit rate of the confidential message	2.5 Gbit/s
D_1	Chromatic dispersion value of D_1	1000 ps/nm
D_2	Chromatic dispersion value of D_2	1000 ps/nm
B	Chromatic dispersion coefficient	16.75×10^{-6} s/m^2
τ_1	External cavity feedback time delay of ECSL	5 ns
τ_2	Feedback time delay of self-feedback loop	8 ns
L	Length of transmission SMF	50 km

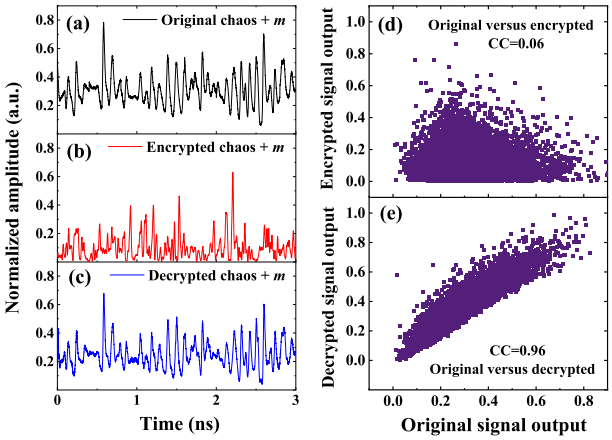

Fig. 2. (a)∼(c) are the temporal waveforms of the original chaotic modulated signal, encrypted and decrypted chaotic modulated signals; (d)∼(e) are the corresponding correlation plots between the original chaotic modulated signal and the encrypted as well as decrypted signals.

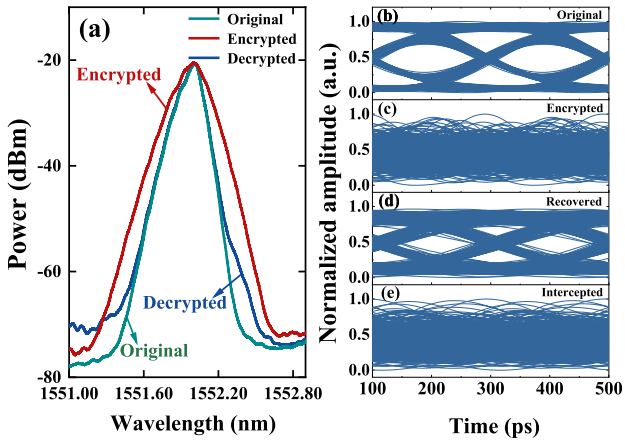

Fig. 3. (a) The optical spectrum of the original, encrypted and decrypted chaotic signals. The eye diagrams corresponding to (b) the original NRZ signal, (c) encrypted signal, (d) recovered NRZ signal, and (e) chaotic signal intercepted by an eavesdropper, respectively.

length of 128000 points to analyze the time delay signature and calculate the auto-correlation function (ACF). The detailed key hardware parameters and the corresponding values in the scheme is illustrated in Table I.

III. RESULTS AND DISCUSSION

To demonstrate the security enhancement of the proposed scheme, the encryption and decryption performances of the chaotic secure optical communication system are firstly investigated. Fig. 2(a) and (b) depict the temporal waveforms of the confidential chaotic modulated signal and the encrypted signal obtained after the external self-feedback hardware encryption module. It can be seen that the encrypted signal exhibits as a noise-like profile in the time domain and is clearly distinct from the chaotic modulated signal. Fig. 2(c) shows the waveform of the decrypted signal after the proper decryption module for a legitimate user, from which one could see that the decrypted signal is recovered well with similar profile to that of the original signal. The corresponding cross-correlation coefficient (CC) plot between the chaotic modulated signal and the hardware encryption chaotic signal is depicted in Fig. 2(d). Clearly, a rather low correlation coefficient of 0.06 is obtained, indicating that the confidential chaotic modulated signal is encrypted into a completely uncorrelated signal. In contrast, Fig. 2(e) shows the correlation plot between the original and decrypted signals. It is evident that most of the scatter points are concentrated on the diagonal and appear like bars, showing a high cross-correlation coefficient of up to ∼0.96 and excellent decryption can be achieved.

Fig. 3 illustrates the optical spectra of the original chaotic modulated signals, encrypted and decrypted signals, respectively. It can be seen that the optical spectrum of the encrypted chaotic signal by the hardware encryption module is spectrally expanded and reshaped due to the self-feedback phase modulation effect, as shown in Fig. 3(a). The corresponding eye diagram of the encrypted chaotic signal is shown in Fig. 3(c), which is completely closed, indicating that the confidential signal is temporally encrypted. The properly decrypted signal presented in the spectrum of Fig. 3(a) shows that the expanded spectrum is restored to a profile similar to the original spectrum, indicating

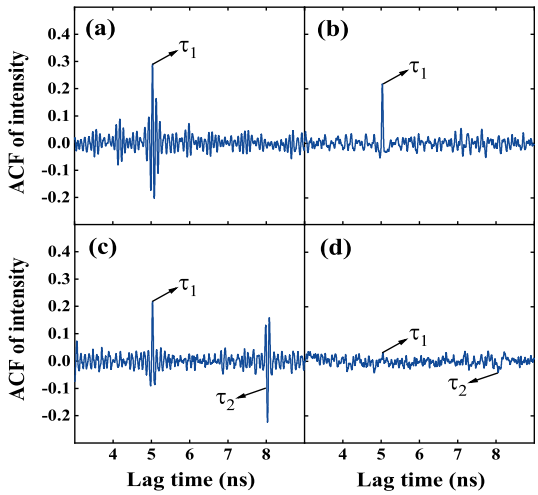

Fig. 4. The ACF (a) before and (b) after passing through D_1, and after passing through the self-feedback loop and D_2 with (c) a small phase modulation depth and dispersion value and (d) large hardware values.

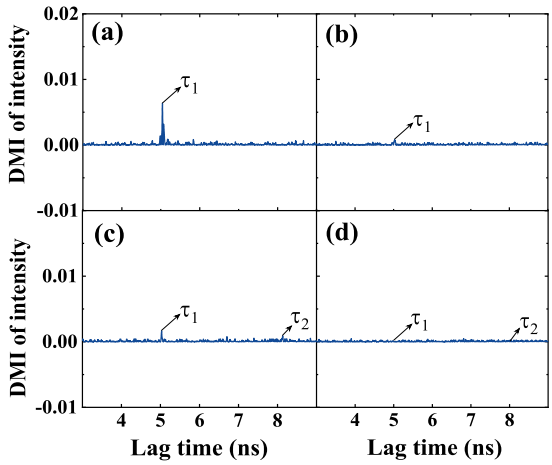

Fig. 5. The DMI (a) before and (b) after passing through D_1, and after passing through the self-feedback loop and D_2 with (c) a small phase modulation depth and dispersion value and (d) large hardware values.

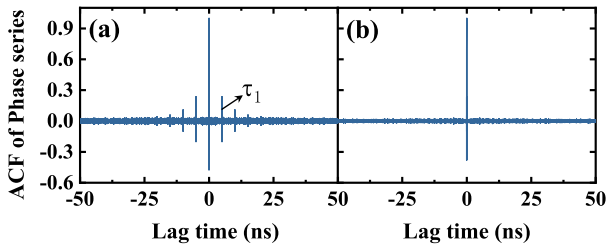

Fig. 6. The ACF of the chaotic phase time series for (a) the original chaotic signal before D_1 and (b) after passing through the hardware self-feedback loop and D_2.

that encryption effect of the self-feedback loop has been successfully erased. Fig. 3(b) and (d) are the eye diagrams of the original NRZ signal and the finally recovered NRZ signal after proper decryption and subtraction with the synchronized chaotic carrier. Compared with the original signal in Fig. 3(b), the eye diagram of the recovered confidential signal is clearly opened, indicating that excellent decryption and chaos synchronization have been achieved. In contrast, the eye diagram for a malicious eavesdropper without the hardware decryption module is still fully closed, showing the security enhancement of the chaotic optical communication system based on the proposed scheme, as depicted in Fig. 3(e).

Having investigated the en/decryption performances of the chaotic optical communication system after introducing the hardware module of self-feedback phase encryption, attention is now turned into the TDS characteristic of the system that is particularly important for the system security. In the chaotic communication system, if an eavesdropper calculates the ACF of the confidential chaotic modulated signal exposing in the public transmission link to crack the TDS, it is possible to reconstruct the chaotic receiver architecture and seriously threaten the security of the system. Thanks to the proposed encryption scheme, the dispersion component of D_1 firstly distort the confidential chaotic modulated signal, whose TDS of the ECSL can be slightly suppressed. After imposing the self-feedback phase encryption loop and followed phase to intensity conversion of the chaotic signals, the time domain distribution of the chaotic optical signal can be greatly disturbed and scrambled, inducing the TDS elimination and security enhancement. Fig. 4(a)∼(d) shows the ACF of the chaotic modulated signal at different locations. As shown in Fig. 4(a), the ACF of the original chaotic modulated signal after the IM exhibits clear TDS at 5 ns with a prominent peak representing the time delay information induced by the external cavity of the MSL. After the chaotic optical signal is scrambled by D_1 in the time domain, it can be seen from Fig. 4(b) that the peak value of TDS decreases from 0.3 to around 0.22 as the value of D_1 gradually increases to ∼1000 ps/nm, indicating that D_1 is able to slightly suppress the TDS. Then, after the signal goes through the self-feedback phase loop and D_2 with a phase modulation depth of around 0.5 and 200 ps/nm, the ACF is calculated and shown in Fig. 4(c). It is found that when the hardware parameters are relatively small, the TDS of τ_1 still exist in the ACF. Additionally, a TDS at 8 ns appears which is caused by the round-trip time delay of τ_2 in the electro-optic feedback loop. Instead, by adjusting the hardware parameters of phase modulation depth for the self-feedback loop and D_2 to be around 2.8 and 1000 ps/nm, the TDS in the ACF greatly suppressed down to the background noise can be obtained, which is shown in Fig. 4(d). Besides analyzing the ACF, the delayed mutual information (DMI) of the chaotic intensity signal at different locations is also calculated, which is shown in Fig. 5(a)∼(d). Similar tendency to the ACF of the chaotic intensity signal in Fig. 4 is obtained. Compared with the DMI of the original chaotic modulated signal that has a TDS spike at the ECSL delay time of 5 ns, as shown in Fig. 5(a), the introduction of the hardware temporal self-feedback encryption module can effectively suppress the DMI spike to around zero as well, as illustrated in Fig. 5(b)∼(d) that have the same hardware parameters setting as in Fig. 4. In addition, the TDS characteristic for the chaotic phase time series is also evaluated by ACF in Fig. 6(a)∼(b). Clearly, the

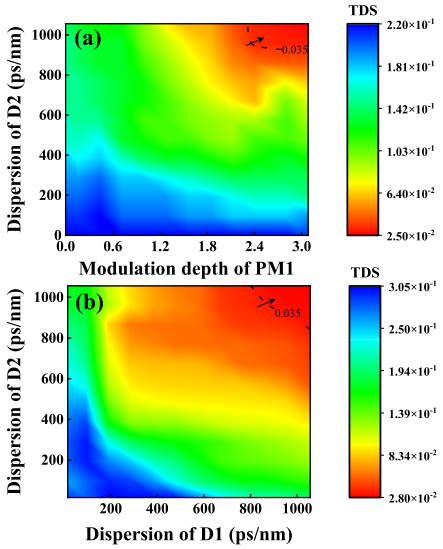

Fig. 7. The contour plot of TDS for (a) different PM modulation depth and D_2, (b) different D_1 and D_2.

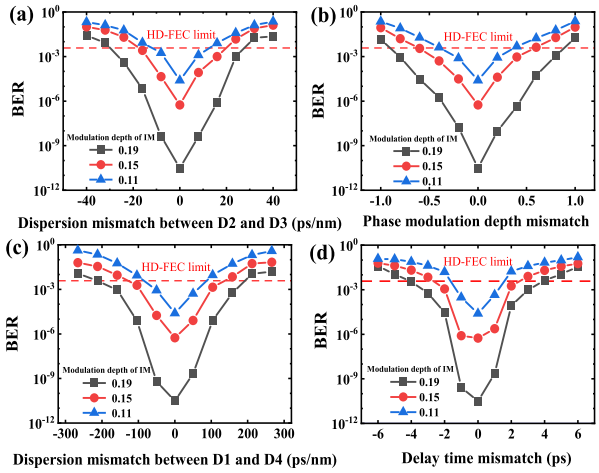

Fig. 8. BER curves for (a) dispersion mismatch between D_2 and D_3, (b) phase modulation depth mismatch, (c) dispersion mismatch between D_1 and D_4, and (d) delay time mismatch between the feedback loops.

TDS peak can be observed in the ACF of original chaotic phase time series as anticipated, but it is greatly suppressed down to zero after the proposed hardware temporal encryption module, as shown in Fig. 6(b), which validates the security enhancement for even chaotic phase time series. From the analysis of the ACF and DMI above, it is evident that both the TDS of the ECSL and the self-feedback loop for ACF and DMI are eliminated when properly select the hardware parameters of the encryption module, which can prevent eavesdroppers from conducting ACF and DMI attack on the chaotic modulated signal to intercept key parameters, and avoid eavesdroppers from reconstructing an identical decryption and chaotic synchronization receiver to threaten the security of the system. Therefore, it is essential to explore the optimal parameter ranges of the hardware encryption module for suppressing the TDS to enhance the system security.

Fig. 7(a) and (b) show the dependence of TDS with the phase modulation depth and dispersion values of D_1 and D_2 for the ACF of chaotic intensity signal. As shown in the contour plot of Fig. 7(a), when D_1 is set as 1000 ps/nm, the dispersion D_2 and phase modulation depth should be selected in the range above the dotted black line, which corresponds to a TDS of as low as 0.035 that is comparable to the background noise level. It is found that the dispersion value of D_2 and phase modulation depth should be larger than 800 ps/nm and 2.4 to make the TDS approach the boundary. Similarly, as shown in Fig. 7(b), when fixing the phase modulation depth as 2.4, a minimum dispersion of $\sim$800 ps/nm for D_1 is desired to simultaneously suppress the TDS of both the ECSL and self-feedback phase loop below the background noise. Therefore, it is recommended to set those hardware parameters higher than the minimum required values and to be in the region above the dotted back line in Fig. 7 to guarantee the system security.

Since the external temporal self-feedback hardware module is the most critical part to ensure the system security, it is essential to explore the hardware parameter mismatch tolerances in the security-enhanced optical communication system. Fig. 8(a) depicts the BER performance versus the dispersion mismatch between D_2 and D_3 for different chaotic intensity modulation depths. It can be seen that the sensitivity of BER to the dispersion mismatch increases with the decreasing of the modulation depth of IM. For an IM depth of $\sim$0.19, a dispersion mismatch tolerance of around $\pm$23 ps/nm is obtained for a BER at the 7% hard-decision forward error correction (HD-FEC) limit. Fig. 8(b) presents the relationship of BER performance with the phase modulation depth mismatch between PM_1 and PM_2. The BER performance exhibits similar tendency to the dispersion mismatch tolerance. Higher IM depth leads to higher mismatch tolerance of phase modulation depth. As the IM depth increases from 0.11 to 0.19, the phase modulation depth mismatch tolerance also increases from $\pm$0.4 to $\pm$0.8 for the HD-FEC limit. Similarly, Fig. 8(c) shows the dependance of BER performance with the dispersion mismatch between D_1 and D_4. It is found that the maximum dispersion mismatch tolerance is around $\pm$180 ps/nm. The BER performance is hence more sensitive to the dispersion mismatch between D_2 and D_3 than that of D_1 and D_4, which is mainly caused the residual phase modulation to intensity modulation conversion by the self-feedback phase en/decryption loop. As the dispersion mismatch between D_2 and D_3 increases, the residual dispersion causes the transformation of phase encryption of the chaotic optical signal to intensity scrambling due to the PM-to-IM conversion, which greatly disturbing the distribution of the chaotic optical signal and deteriorating the decryption performance, resulting a much strict dispersion mismatch tolerance for D_2 and D_3. In addition, as another critical parameter, the round-trip delay time mismatch between the encryption and decryption self-feedback loops is also depicted in Fig. 8(d), from which it can be seen that a delay time mismatch of around $\pm$4 ps can be tolerated for an IM depth of 0.19. The higher the IM depth, the larger the delay time mismatch tolerance. Hence, it is desirable to precisely control the delay time in the self-feedback loop to guarantee

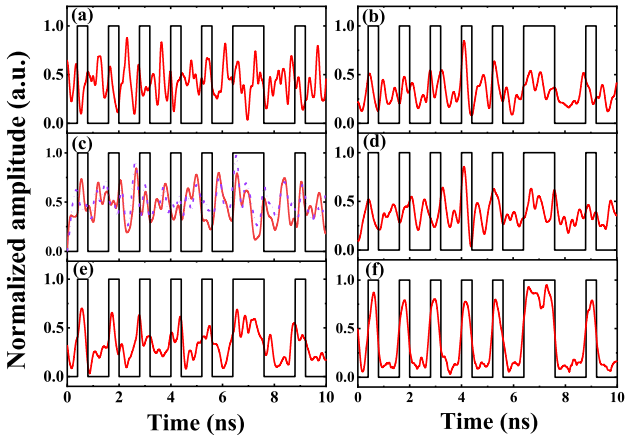

Fig. 9. (a) The waveforms of original data and intercepted by the DLF attack. (b)-(d) The waveforms intercepted by synchronization utilization attack under different scenarios: (b) w/o PM_2, (c) w/o D_3 (red solid line) or D_4 (blue dashed-dot line), (d) with τ_3 mismatch. (e) The waveform intercepted by the hardware decryption module, without the SSL. (f) The waveform for a legal receiver.

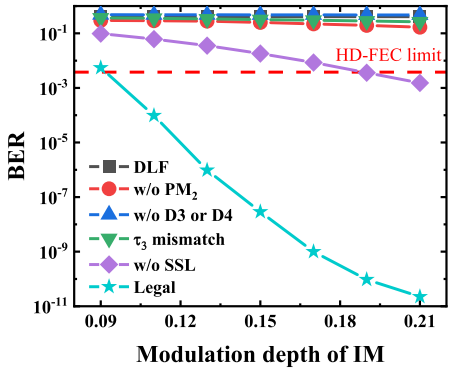

Fig. 10. BER performances versus the intensity modulation depth for various attack scenarios and legal users.

the decryption performance whilst ensuring the security of the hardware encryption module.

Furthermore, we emulate various attack scenarios to investigate the security of the proposed chaotic optical communication system, as shown in Fig. 9. Fig. 9(a) depicts the waveforms of the original confidential NRZ data and the intercepted signal by an eavesdropper employing a fourth-order low-pass filter with a cutoff frequency equaling to the transmission bit rate for DLF attack. Compared with the original waveform, it can be easily observed that Eve is indeed not able to intercept the confidential information by simple DLF attack, which indicates the security enhancement than the conventional chaotic communication scheme [27]. Then, the security robustness against the synchronization utilization attack is also investigated for different scenarios, as illustrated in Fig. 9(b)–(d). If Eve employs a matched ECSL at the receiver but without a proper decryption hardware module with matched hardware parameters to remove the self-feedback phase encryption effect, the eventual recovered waveform still cannot coincide with the original waveform, as shown in Fig. 9(b) without PM_2 and (c) without D_3 or D_4, and in Fig. 9(d) with τ_3 mismatch in the decryption hardware module. Similarly, if the self-feedback hardware decryption module is available to an eavesdropper but without the SSL, as shown in Fig. 9(e), the obtained waveform will exhibit as the chaotic modulated signal with the confidential NRZ data concealed in the chaotic waveform. It is still quite difficult to intercept the confidential data without chaos synchronization and signal subtraction processing as long as the depth of the modulated information is properly controlled within a certain limit, as will be discussed later. In comparison, the legitimate user with a proper hardware decryption module and a matched chaotic receiver is able to successfully recover a consistent waveform with the original confidential data, as shown in Fig. 9(f), which proves that the proposed scheme can guarantee the security and decryption performance well.

To further investigate the communication performance of the proposed system, the obtained BER by the legitimate user and an eavesdropper for different modulation depths are shown in Fig. 10.

It is clear that the BER for all the above mentioned DLF and synchronization utilization attacks are all above the HD-FEC limit, indicating that the proposed system is immune to the malicious attacks. It is also worth noting that the BER performance for the legitimate user is closely related to the IM modulation depth of the chaotic carrier. The higher the modulation depth of the IM, the better the BER performance is due to the increased ratio between the confidential signal and chaotic carrier. When the IM modulation depth is adjusted at ∼0.09, the BER for the legal user corresponds to the HD-FEC limit, thus setting the lower bound for the IM modulation depth to be ∼0.09. Increasing the IM modulation depth will cause the reduction of the BER accordingly. However, a potential security threat for increasing the IM modulation depth is the DLF attack in the case of eavesdropping with proper decryption hardware module but without the chaotic receiver, in which case the confidential data may be directly intercepted by low pass filtering for relatively high IM modulation depth. As shown in the square curves in Fig. 10, when the IM modulation depth approaches ∼0.19, the BER for an eavesdropper is reduced down to the HD-FEC limit, indicating the upper bound for the IM modulation depth. Therefore, the IM modulation depth for the chaotic modulation is recommended to be controlled in the range of ∼0.09 to ∼0.19 in order to guarantee the trade-off between the system security and decryption performance.

Finally, the BER performances versus the bit rate of the confidential signal for various intensity modulation depths are also evaluated, as illustrated in Fig. 11. It is clear that the BER of the recovered confidential signal is degraded with the increase of the bit rate. For the upper bound of intensity modulation depth of ∼0.19, a bit rate of ∼5 Gb/s will cause the BER deteriorated to the HD-FEC limit. On the other hand, reducing the intensity modulation depth could reduce the supportable bit rate accordingly. When the intensity modulation depth is reduced to 0.03, the maximum bit rate that can be supported by the confidential system is reduced down to ∼1 Gb/s to ensure the BER is below the HD-FEC limit. It is therefore quite essential to make the transmission bit rate lower than the maximum supportable bit rate according to different modulation depths,

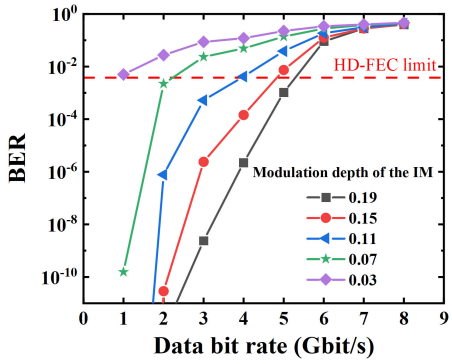

Fig. 11. BER and security of the system versus various intensity modulation depths at different transmission bit rates.

so as to guarantee both the system security against malicious eavesdropping and transmission performance.

IV. Conclusion

In summary, we propose and numerically demonstrate a security enhancement scheme for chaotic optical communication systems based on external temporal self-feedback hardware encryption and decryption, where the confidential chaotic modulated signal is encrypted into a temporally scrambled chaotic signal that has very low cross-correlation with the original signal. The TDS embedded in the original chaotic carrier is fully suppressed based on this scheme, which also greatly increases the difficulty for an eavesdropper to intercept the confidential data by simple direct linear filtering or synchronization utilization attack. The proposed chaotic hardware encryption scheme can provide additional hardware key parameters so as to greatly enhance the system security. It is believed that the pluggable external hardware encryption and decryption scheme is very powerful and promising for future security enhanced chaotic optical communication.

References

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 6, no. 8, pp. 142–145, Jun. 1996.
[2] A. Argyris, D. Syvridis, and A. Bogris, "Chaos-based communications at high bit rates using commercial fiber-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, Oct. 2005.
[3] 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.
[4] L. Wang, Y. Guo, D. Wang, Y. Wang, and A. Wang, "Experiment on 10-Gb/s message transmission using an all-optical chaotic secure communication system," *Opt. Commun.*, vol. 453, Dec. 2019, Art. no. 124350.
[5] G. Xia, Z. Wu, and J. Wu, "Theory and simulation of dual-channel optical chaotic communication system," *Opt. Exp.*, vol. 13, no. 9, pp. 3445–3453, Jun. 2005.
[6] M. Jacquot, R. Lavrov, J. Oden, Y. K. Chembo, and L. Larger, "Field experiment optical chaos communication @ 10Gb/s demonstrating electro-optic phase chaos principles," in *Proc. CLEO Europe/EQEC*, 2011, pp. CI3_1.
[7] J. Ke, L. Yi, G. Xia, and W. Hu, "Chaotic optical communications over 100-km fiber transmission at 30-Gb/s bit rate," *Opt. Lett.*, vol. 43, no. 6, pp. 1323–1326, Mar. 2018.
[8] N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, pp. 1536–1539, Apr. 2019.
[9] S. Li and S. Chan, "Chaotic time-delay signature suppression in a semiconductor laser with frequency-detuned grating feedback," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 6, Nov./Dec. 2015, Art. no. 1800812.
[10] S. Priyadarshi, Y. Hong, I. Pierce, and K. A. Shore, "Experimental investigations of time-delay signature concealment in chaotic external cavity VCSELs subject to variable optical polarization angle of feedback," *IEEE J. Sel. Topics Quantum Electron.*, vol. 19, no. 4, Jul./Aug. 2013, Art. no. 1700707.
[11] L. Zhang, W. Pan, L. Yan, B. Luo, X. Zou, and M. Xu, "Isochronous cluster synchronization in delay-coupled VCSEL networks subjected to variable-polarization optical injection with time delay signature suppression," *Opt. Exp.*, vol. 27, no. 23, pp. 33369–33377, Nov. 2019.
[12] 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.
[13] E. M. Shahverdiev and K. A. Shore, "Impact of modulated multiple optical feedback time delays on laser diode chaos synchronization," *Opt. Commun.*, vol. 282, no. 17, pp. 3568–3572, Sep. 2009.
[14] 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, Dec. 2018.
[15] N. Jiang, C. Wang, C. Xue, G. Li, S. Lin, and K. Qiu, "Generation of flat wideband chaos with suppressed time delay signature by using optical time lens," *Opt. Exp.*, vol. 25, no. 13, pp. 14359–14367, Jun. 2017.
[16] Y. Fu et al., "Wavelength division multiplexing secure communication scheme based on an optically coupled phase chaos system and PM-to-IM conversion mechanism," *Nonlinear Dyn.*, vol. 94, pp. 1949–1959, Jul. 2018.
[17] S. Li, X. Li, and S. Chan, "Chaotic time-delay signature suppression with bandwidth broadening by fiber propagation," *Opt. Lett.*, vol. 43, no. 19, pp. 4751–4754, Oct. 2018.
[18] J. Wu, G. Xia, L. Cao, and Z. Wu, "Experimental investigations on the external cavity time signature in chaotic output of an incoherent optical feedback external cavity semiconductor laser," *Opt. Commun.*, vol. 282, no. 15, pp. 3153–3156, Aug. 2009.
[19] A. Zhao, N. Jiang, S. Liu, C. Xue, and K. Qiu, "Wideband time delay signature-suppressed chaos generation using self-phase-modulated feedback semiconductor laser cascaded with dispersive component," *J. Lightw. Technol.*, vol. 37, no. 19, pp. 5132–5139, Jul. 2019.
[20] 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, May 2017.
[21] J. Wu, G. Xia, and Z. Wu, "Suppression of time delay signatures of chaotic output in a semiconductor laser with double optical feedback," *Opt. Exp.*, vol. 17, no. 22, pp. 116954–116963, May 2014.
[22] Y. Xu, M. Zhang, L. Zhang, P. Lu, S. Mihailov, and X. Bao, "Time-delay signature suppression in a chaotic semiconductor laser by fiber random grating induced random distributed feedback," *Opt. Lett.*, vol. 42, no. 20, pp. 4107–4110, Mar. 2017.
[23] A. Zhao, N. Jiang, J. Peng, S. Liu, Y. Zhang, and K. Qiu, "Parallel generation of low-correlation wideband complex chaotic signals using CW laser and external-cavity laser with self-phase-modulated injection," *Opt.-Electron. Adv.*, vol. 5, no. 5, Mar. 2022, Art. no. 200026.
[24] N. Jiang, A. Zhao, S. Liu, C. Xue, B. Wang, and K. Qiu, "Generation of broadband chaos with perfect time delay signature suppression by using self-phase-modulated feedback and a microsphere resonator," *Opt. Lett.*, vol. 43, no. 21, pp. 5359–5362, Nov. 2018.
[25] A. Wang, Y. Wang, and J. Wang, "Route to broadband chaos in a chaotic laser diode subject to optical injection," *Opt. Lett.*, vol. 34, no. 8, pp. 1144–1146, May 2009.
[26] N. Jiang, C. Xue, J. Zhang, X. Yi, and K. Qiu, "Secure chaos communication with semiconductor lasers subject to sinusoidal phase-modulated optical feedback," in *Proc. Conf. Lasers Electro-Opt. Pacific Rim*, 2017, Art. no. 611731.
[27] N. Jiang, C. Zhang, and K. Qiu, "Secure passive optical network based on chaos synchronization," *Opt. Lett.*, vol. 37, no. 21, pp. 4501–4503, Nov. 2012.
[28] A. Bogris, A. Argyris, and D. Syvridis, "Encryption efficiency analysis of chaotic communication systems based on photonic integrated chaotic circuits," *IEEE J. Quantum Electron.*, vol. 46, no. 10, pp. 1421–1429, Oct. 2010.
[29] C. Xue et al., "Security-enhanced chaos communication with time-delay signature suppression and phase encryption," *Opt. Lett.*, vol. 41, no. 16, pp. 3690–3693, Aug. 2016.
[30] N. Jiang, A. Zhao, Y. Wang, S. Liu, and K. Qiu, "Security-enhanced chaotic communications with optical temporal encryption based on phase modulation and phase-to-intensity conversion," *OSA Continuum*, vol. 2, no. 12, pp. 3422–3437, Dec. 2019.