Research Article | Vol. 24, No. 20 | 3 Oct 2016 | OPTICS EXPRESS 23439

Optics EXPRESS

Maximizing the security of chaotic optical communications

T. T. HOU,[1] L. L. YI,[1,*] X. L. YANG,[1] J. X. KE,[1] Y. HU,[1] Q. YANG,[2] P. ZHOU,[2] AND W. S. HU[1]

[1]*State Key Lab of Advanced Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai, 200240, China*
[2]*State Key lab of Advanced Communication Technologies and Networks, Wuhan Research Institution of Posts & Telecommunications, Wuhan, 430074, China*
[*]*lilinyi@sjtu.edu.cn*

Abstract: The practical application of chaotic optical communications has been limited by two aspects: the difficulty in concealing the time delay - a critical security parameter in feedback chaotic systems, and the difficulty of significantly enlarging the key space without complicating the implementation. Here we propose an architecture to break the above limits. By introducing a frequency-dependent group delay module with frequency tuning resolution of 1 MHz into the chaotic feedback loop, we demonstrate excellent time delay concealment effect, and an additional huge key space of 10^{48} can be achieved at the same time. The effectiveness is proved by both numerical simulation and experiment. Besides, the proposed scheme is compatible with the existing commercial optical communication systems, thus pave the way for high-speed secure optical communications.

OCIS codes: (060.4510) Optical communications; (060.4785) Optical security and encryption; (140.1540) Chaos.

References and links

1. L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett. **64**(8), 821–824 (1990).
2. K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett. **71**(1), 65–68 (1993).
3. P. Colet and R. Roy, "Digital communication with synchronized chaotic lasers," Opt. Lett. **19**(24), 2056–2058 (1994).
4. G. D. VanWiggeren and R. Roy, "Communications with chaotic lasers," Science **279**(5354), 1198–1200 (1998).
5. S. Tang and J. M. Liu, "Message encoding-decoding at 2.5 Gbits/s through synchronization of chaotic pulsing semiconductor lasers," Opt. Lett. **26**(23), 1843–1845 (2001).
6. J. Paul, K. A. Shore, "3.5-GHz signal transmission in an all-optical chaotic communication scheme using 1550-nm diode laser," IEEE Photon. Technol. Lett. **17**(4), 920–922 (2005).
7. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, and I. Fischer, "Chaos-based communications at high bit rates using commercial fiber-optic links," Nature **438**, 343–346 (2005).
8. R. Lavrov, M. Jacquot, and L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications," IEEE J. Quantum Electron. **46**(10), 1430–1435 (2010).
9. N. Gastaud, S. Poinsot, L. Larger, J.-M. Merolla, M. Hanna, J.-P. Goedgebuer, and F. Malassenet, "Electro-optical chaos for multi-10 Gbit/s optical transmissions," Electron. Lett. **40**(14), 898–899 (2004).
10. R. Lavrov, M. Peil, M. Jacquot, L. Larger, V. Udaltsov, and J. Dudley, "Electro-optic delay oscillator with nonlocal nonlinearity: Optical phase dynamics, chaos, and synchronization," Phys. Rev. E Stat. Nonlin. Soft Matter Phys. **80**(2), 026207 (2009).
11. S. Ortin, M. Jacquot, L. Pesquera, M. Peil, and L. Larger, "Time delay extraction in chaotic cryptosystems base on optoelectronic feedback with variable delay," Proc. SPIE **699**, 0E. 1–12 (2008).
12. 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. **72**(5), 373–377 (2005).
13. 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. **45**(7), 879–1891 (2009).
14. S. Ortin, J. M. Gutie-rezc, L. Pesqueraa, and H. Vasqueza, "Nonlinear dynamics extraction for time-delay systems using modular neural networks synchronization and prediction," Physica A **351**, 133–141 (2005).
15. J. G. Wu, G. Q. Xia, and Z. M. Wu, "Suppression of time delay signatures of chaotic output in a semiconductor laser with double optical feedback," Opt. Express **17**(22), 20124–20133 (2009).

#270819 http://dx.doi.org/10.1364/OE.24.023439
Journal © 2016 Received 5 Aug 2016; revised 15 Sep 2016; accepted 15 Sep 2016; published 29 Sep 2016

Optics EXPRESS

16. Y. Wu, "Can fixed time delay signature be concealed in chaotic semiconductor laser with optical feedback?" IEEE J. Quantum Electron. **48**(11), 1371–1379 (2012).
17. W. H. Kye, M. Choi, M. W. Kim, S. Y. Lee, S. Rim, C. M. Kim, and Y. J. Park, "Synchronization of delayed systems in the presence of delay time modulation," Phys. Lett. A **322**(5-6), 338–343 (2004).
18. D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, "Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback," Opt. Lett. **32**(20), 2960–2962 (2007).
19. G. Aromataris and V. Annovazzi-Lodi, "Enhancing privacy of chaotic communications by double masking," IEEE J. Quantum Electron. **49**(11), 955–959 (2013).
20. L. Ursini, M. Santagiustina, and V. Annovazzi Lodi, "Enhancing Chaotic Communication Performances by Manchester Coding," IEEE Photonics Technol. Lett. **20**(6), 401–403 (2008).
21. R. M. Nguimdo, P. Colet, and C. Mirasso, "Electro-optic delay devices with double feedback," IEEE J. Quantum Electron. **46**(10), 1436–1443 (2010).
22. J. Hizanidis, S. Deligiannidis, A. Bogris, and D. Syvridis, "Enhancement of chaos encryption potential by combining all-optical and electro-optical chaos generators," IEEE J. Quantum Electron. **46**(11), 1642–1649 (2010).
23. R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, "Digital key for chaos communication performing time delay concealment," Phys. Rev. Lett. **107**(3), 034103 (2011).
24. R. M. Nguimdo and P. Colet, "Electro-optic phase chaos systems with an internal variable and a digital key," Opt. Express **20**(23), 25333–25344 (2012).
25. Z. Wang, "Optical Steganography Over a Public DPSK Channel with Asynchronous Detection," IEEE J. Quantum Electron. **13**, 48–50 (2011).
26. Z. Wang, M. P. Fok, L. Xu, J. Chang, and P. R. Prucnal, "Improving the privacy of optical steganography with temporal phase masks," Opt. Express **18**(6), 6079–6088 (2010).
27. N. Kostinski, K. Kravtsov, and P. R. Prucnal, "Demonstration of an all-optical OCDMA encryption and decryption system with variable two-code keying," IEEE Photon. Technol. Lett. **20**(24), 2045–2047 (2008).
28. S. S. Li, Q. Liu, and S. C. Chan, "Distributed feedbacks for time-delay signature suppression of chaos generated from a semiconductor laser," IEEE Photon. J. **4**(5), 1930–1935 (2012).
29. J. R. Kuttler and G. D. Dockery, "Theoretical description of the parabolic approximation/Fourier split-step method of representing electromagnetic propagation in the troposphere," Radio Sci. **26**(2), 381–393 (1991).

1. Introduction

Chaotic systems have been considered as good candidate for providing information security attributed to its broadband, noise like, and unpredictability nature [1,2]. Since the first experimental demonstration using chaotic laser for digital communications [3], the chaotic dynamics has been extensively exploited for chaos-based secure optical communications [4–10]. However, the security of chaotic optical systems remains the key issue to be addressed [11]. In principle, chaotic systems with feedback loop are able to generate infinite-dimensional chaotic carrier, and the feedback time delay parameter serves as a critical secure key. Unfortunately, it was proved that with several methods such as auto correlation functions, mutual information and extrema statistics, the delay time can be successfully extracted [12,13]. Then, with the knowledge of the delay time, other hardware parameters can be easily estimated. Once the eavesdroppers have figured out all the hardware keys, they can use technologies such as artificial neuron networks to reconstruct the chaotic system [14]. Therefore, two remaining essential questions need to be addressed to improve the security of chaotic optical communication: how to conceal the time delay and how to improve the key space. There have been a wide variety of methods to conceal the time delay signature (TDS). It has been demonstrated the TDS can be suppressed in a double optical feedback chaotic systems [15]. However, the fixed time delay cannot be concealed in optical feedback chaotic systems even for multiple feedback cavities using spectrum analysis method [16]. Variable time delay by time delay modulation has been proposed to conceal the TDS [17], but it has been shown that the period of the time delay can be extracted from experimental data by using the mutual information function [11]. Choosing the feedback delay time around the relaxation frequency of the laser can also conceal the TDS [18], but at the expense of reducing the chaotic complexity. Therefore, a valid TDS concealment method is still required. Except for TDS concealment, increasing the chaotic complexity is also a way to improve the security level. The security can be improved to a certain extent by using double masking [19], Manchester coding [20], combining all-optical and electro-optical feedback schemes [21,22]. Undoubtedly, simultaneously concealing the TDS and increasing the security key space is the

Optics EXPRESS

best way to improve security. By using double electro-optic feedback loops in parallel or serial configuration to improve the chaotic complexity and introducing a digital key into the feedback loop, the TDS can be greatly suppressed and the key space is extremely increased by entropy amplification [23,24], which could be considered with the highest security level in the chaos-based optical communication systems ever reported. However, the configuration of chaotic emitter and receiver is quite complicated, which will increase the implementation difficulty and only simulations have been performed. Besides, the distribution and synchronization of the digital key remains an issue for chaotic optical communications.

In this article, we propose a new scheme that significantly increases the security level of chaotic optical communication without complicating the implementation. The key idea is to introduce a frequency-dependent group delay (FDGD) module with high frequency tuning resolution into the chaotic feedback loop, which acts as a hardware key to significantly conceal the TDS and increase the security key space. The eavesdroppers must generate exactly the same FDGD curve to cancel the chaotic carrier for signal decryption. Fiber Bragg grating (FBG) can be regarded as a kind of FDGD module, and it has been applied to optical security fields before, such as in steganography communication systems [25,26], optical code division multiple access (OCDMA) systems [27] and chaotic optical communications [28]. However, the group delay curve is not easy to be flexibly tuned with high resolution in FBG therefore the key space is very limited. In our approach, we use a FDGD module consisting of cascaded Gires-Tournois (G-T) etalons to generate arbitrary group delay curve with high frequency resolution. The security key space can be adjusted according to the security demand in different application scenarios by changing the structure of the FDGD module. We demonstrate a 10^{48} secure key space enlargement with a FDGD module consisting of 16 cascaded G-T etalons as an example. Another striking advantage of this structure is the significant time delay concealment effect. Instead of performing the time delay concealment in time domain as the methods suggested in most of the previous research [14,16,18,25,26,28], this concealment is skillfully achieved in frequency domain. Because of the present of the FDGD module, different frequency components of the chaotic laser experience different delay time, therefore the time periodicity is broken and the TDS vanishes from both time-domain auto-correlation function and frequency-domain spectrum analysis methods, which have been verified by both numerical simulation and experimental demonstration. Besides, the FDGD module can be manufactured with mass production capability and the match of FDGD modules in emitter and receiver is feasible by using the same structure and the same setting of the G-T etalons after calibration. These contributions together enable the proposed scheme to pave the way for high-speed secure optical communications.

2. Principles and results

2.1 System architecture

The architecture of the proposed setup is depicted in Fig. 1, where the electro-optical feedback configuration is adopted due to its implementation feasibility and potential to support high bit rate [9]. The basic part of the emitter side is an electro-optical feedback delay loop, where the chaotic carrier is generated from the non-linearity of a high-speed lithium niobate Mach-Zehnder modulator (MZM) with a small half-wave voltage, which is seeded by a continuous-wave (CW) semiconductor laser diode (LD1). The message m(t) is carried by the output of LD2 and mixed with the chaotic carrier through an optical coupler (OC). The coupler splits the mixed signal into two arms, one beam is send to the receiver after fiber transmission while the other is injected into the feedback loop. Note that the message participates in the chaotic generation process by perturbing the original chaotic dynamics, thus further increases the chaotic complexity. The feedback signal is first subjected to a certain time delay, then sent into the key component in our system, a FDGD module, which is manufactured by a series of cascaded G-T etalons. Optical beam is subjected to zero-loss

Optics EXPRESS

transmission in the cavity of G-T etalons, but experienced different group delay for different frequency components, thus the FDGD could be considered as a frequency-dependent group delay component. More details about FDGD and G-T etalons will be presented later. A broadband photo-detector (PD) converts the output signal from the FDGD module into electrical waveform as the electrical input of the MZM after being boosted by a broadband radio frequency (RF) driver. Once the output voltage of the RF driver is two to three times of V_π, the chaotic carrier can be generated. In the receiver side, the open loop synchronization configuration is adopted due to its simplicity [7]. If all the parameters including the delay time, the frequency responses of MZM, RF driver and PD and the group delay curve of the FDGD module are matched, the chaotic carrier can be synchronized and the message can be recovered.

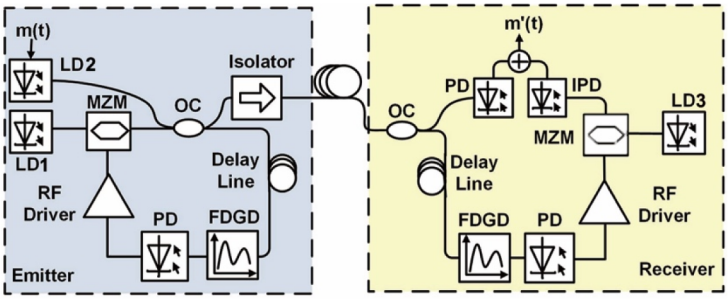

Fig. 1. System architecture.

G-T etalon is a kind of optical interferometer made by two parallel reflective mirrors, where the back one is perfectly reflective and the front one is partially reflective. Figure 2(a) depicts the schematic architecture of FDGD consisting of 16 cascaded G-T etalons. It should be noted that more G-T etalons can produce broad group delay curves, and will result in higher cracking difficulty for illegal users, as well as larger encryption difficulty for legal users, so the number should be properly designed. The FDGD curve of G-T etalons can be controlled by several parameters such as cavity length, reflectivity and reflective index. Here we use etalons with variable cavity lengths, which can be accurately controlled by precise temperature control with a tuning resolution of 0.001°C, as the case of a commercial tunable dispersion compensator also consisting of cascaded G-T etalons from II-VI photonics.

The frequency response of a single G-T etalon can be expressed as:

$$H(\omega) = \frac{r - e^{i\delta}}{1 - re^{i\delta}}, \tag{1}$$

where r is the reflective coefficient of the partially reflecting mirror and δ donates the phase shift of the optical beam in one round-trip of the cavity, which is defined by:

$$\delta = \frac{4\pi nd}{\lambda}\cos\theta, \tag{2}$$

In this equation, n and d are the refractive index and thickness of the cavity medium, respectively, while λ and θ represent the wavelength and the incidence angle of the incoming light. Use i to distinguish each etalon contained in FDGD, and the frequency response of the ith etalon can be further expressed in exponential form as:

$$H_i(\omega) = \exp\{i\varphi_i(\omega)\} = \exp\left\{-i\int_{-\infty}^{\omega}\tau_i(\omega')d\omega'\right\}, \tag{3}$$

Combine Eq. (3) with Eq. (1),the phase spectrum and group delay spectrum of the ith etalon can be deduced as:

Optics EXPRESS

$$\varphi_i(\omega) = -arctg\frac{(1-r_i)\sin\delta_i}{2\sqrt{r_i}-(1+r_i)\cos\delta_i}, \tag{4}$$

$$\tau_i(\omega) = \frac{2n_i d_i\cos\delta_i}{c}\frac{1-r_i}{2\sqrt{r_i}\cos\delta_i-(1+r_i)}, \tag{5}$$

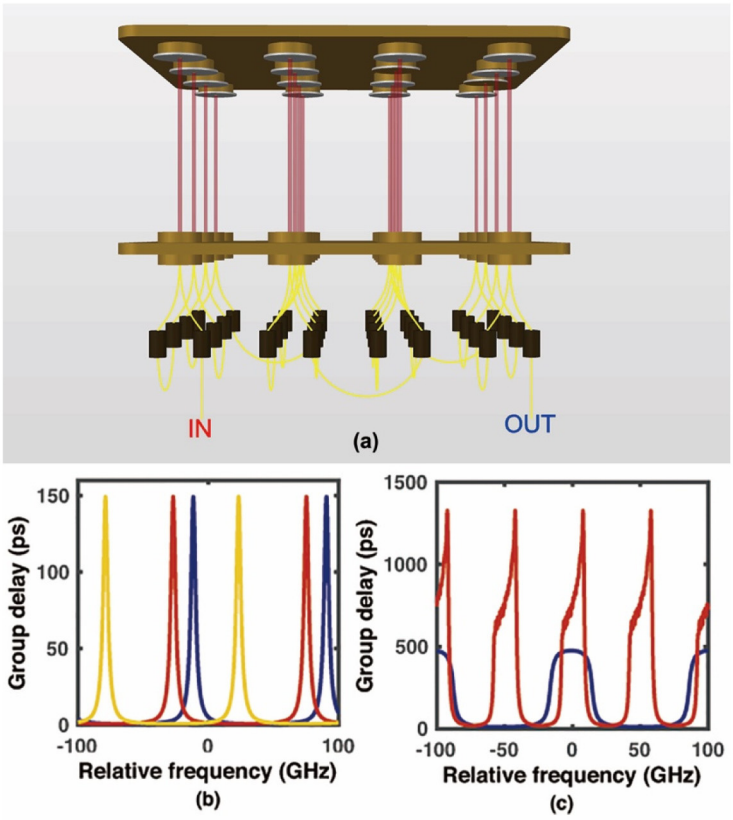

Fig. 2. (a) Schematic architecture of the FDGD module, (b) the group delay spectra of three individual G-T etalons and (c) the superposed group delay spectra of 16 cascaded G-T etalons.

The frequency response of FDGD is the superposition of the frequency response of 16 cascaded G-T etalons, and can be described as:

$$H(\omega) = \sum_{i=1}^{i=16} H_i(\omega) = \exp\{i\varphi(\omega)\} = \exp\left\{-i\int_{-\infty}^{\omega}\tau(\omega')d\omega'\right\}, \tag{6}$$

Similarly, the phase and group delay spectra of FDGD are expressed as follows:

$$\varphi(\omega) = \sum_{i=1}^{i=N}\varphi_i(\omega), \tag{7}$$

$$\tau(\omega) = \sum_{i=1}^{i=N}\tau_i(\omega), \tag{8}$$

In above equations, $H(\omega)$ is the frequency response of each etalon, $\varphi(\omega)$ and $\tau(\omega)$ respectively represent the phase spectrum and group delay spectrum of the module.

Figure 2(b) shows the group delay spectra of three uniform individual G-T etalons distinguished by color. The three G-T etalons have different temperature settings, which

Optics EXPRESS

result in different cavity length and further produce different group delay curves according to Eq. (5). Figure 2(c) represents the superposed group delay spectra of 16 cascaded etalons, where different colors correspond to different temperature setting combinations of 16 G-T etalons.

2.2 Chaotic dynamics

The dynamics model of the overall chaotic system can be expressed as follows. The complex envelope of the electrical field at the MZM output can be expressed as:

$$E(t)=\frac{1}{2}E_0\left\{1+e^{\frac{\pi V(t)}{v_\pi}+\frac{\pi V_B}{V_{DC}}}\right\}, \tag{9}$$

where V_π and V_{DC} represent the RF half-wave voltage and the bias half-wave voltage, $V(t)$ and V_B represent RF input and DC bias. To boost the nonlinearity of the modulator, MZM with low V_π and RF driver with high output voltage are used. Let $E'(t)$ be the electrical field output of the FDGD module, which obeys the following function:

$$E'(t)=F^{-1}\left\{F\left[E(t\text{-}T)+\alpha_m m(t-T)\right]e^{i\varphi(\omega)}\right\}, \tag{10}$$

where T donates the overall cavity delay time including both the frequency-independent time delay from all optical/electrical components in the feedback loop and the frequency-dependent time delay from the FDGD module as described in Eq. (8). $m(t)$ represents the message added into the chaotic carrier and α_m represents the amplitude ratio between the message and the chaotic carrier, $\varphi(\omega)$ is the phase spectrum of the FDGD. F and F^{-1} represent Fourier transform and its reverse transform, respectively.

Using subscripts "1", "2" to distinguish the emitter and the receiver, a generalized dynamical model of the proposed chaotic transmitter can be described as:

$$V_1(t)+\tau_1\frac{dV_1(t)}{dt}+\frac{1}{\theta_1}\int_{t_0}^{t}V_1(t')dt'=G_1S_1\left|E_1'(t-T_1)\right|^2, \tag{11}$$

where G and S represent the gain of the electrical driver and the sensitivity of the photo detector, respectively. Note that the electrical response of the feedback loop is equivalent to a first-order band-pass filter, where τ and θ corresponding to high cut-off frequency and low cut-off frequency of the equivalent band-pass filter, respectively. All the variables are expressed in the normalized form. The dynamic model of the chaotic receiver can be described as:

$$V_2(t)+\tau_2\frac{dV_2(t)}{dt}+\frac{1}{\theta_2}\int_{t_0}^{t}V_2(t')dt'=G_2S_2\left|E_2'(t-T_2)\right|^2, \tag{12}$$

For perfect chaotic synchronization, all the hardware parameters of each component, including MZM, optical delay line, FDGD, PD, and RF driver, should be matched.

First, to prove the chaotic capability of the proposed architecture, we tested the generated chaotic dynamics under different conditions, and the results are plotted in Fig. 3. A digital real-time oscilloscope was used to record traces up to 2,000,000 points, under 40 GS/s sampling rate. The sample time is 50 μs, covering over 200 times of the feedback delay time, thus is sufficiently enough for time delay identification. An electrical spectrum analyzer (ESA, Anritsu MS266C7) is used for spectrum analysis. In each figure, we use black line to illustrate the situation without cavity feedback, which is achieved by disconnecting the feedback loop. Fig. 3(a)-3(d) are chaotic intensity time series, and the corresponding radio-frequency (RF) spectrums and optical spectrums are respectively presented in Fig. 3(e)-3(h) and Fig. 3(i)-3(l). In Fig. 3(a), the FDGD is replaced by a fiber jumper which has the same

Optics EXPRESS

length with the FDGD pigtail, while in Fig. 3(b) and Fig. 3(c), the FDGD group delay curves are set to be linear within the chaotic spectrum, and the dispersion values are 2000ps/nm and 1000ps/nm, respectively. In Fig. 3(d), the FDGD has an irregular group delay curve. For clear display, only 1000 points were plotted in each time-domain trace, although the sample length is 2,000,000. From the RF spectra in the middle column of Fig. 3, the bandwidth of the generated chaotic spectrum is around 5 GHz, matching with the bandwidth of the electrical driver, which is the component with the narrowest band in the experiment. It could be observed that the spectrum of non-chaotic signal (black lines) is increased at around 4.5 GHz. We make a reasonable judgment that this is caused by the intrinsic property of the ESA, since the spectrum has the same shape with the noise floor. The spectrum amplitude suffers a slight reduction in Fig. 3(f)-3(h) compared to that in Fig. 3(a), due to the FDGD module's insertion loss. The optical spectra in the right column of Fig. 3 prove the broadband characteristic of the chaotic signal again. Another significant conclusion is that introducing the FDGD will not break the chaotic status of the original system, which is the basis for our following investigations.

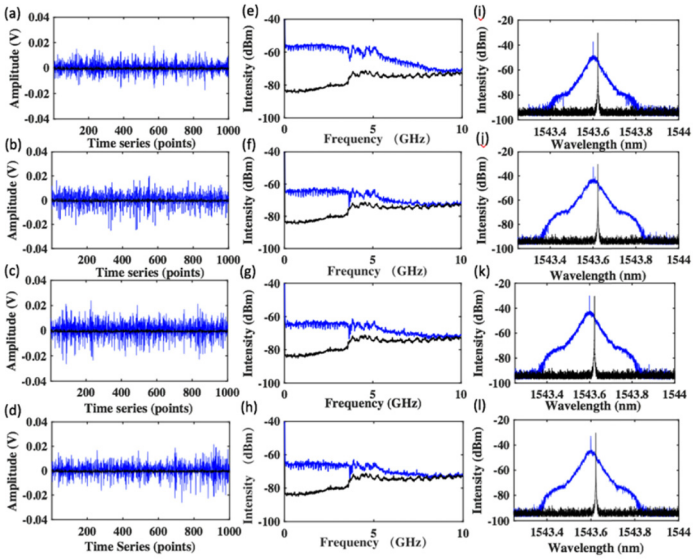

Fig. 3. Chaotic time series (a) (b) (c) (d), corresponding RF spectrums (e) (f) (g) (h) and optical spectrums (i) (j) (k) (l). Black lines in each figures represent the situation without feedback. (a) (e) (i) represents chaotic system without FDGD. (b) (f) (j) represent chaotic system with FDGD where the group delay curve is linear within the chaotic spectrum with a 2000ps/nm dispersion. (c) (g) (k) represents chaotic system with FDGD where the group delay curve is linear within the chaotic spectrum with a 1000ps/nm dispersion. (d) (h) (l) represents chaotic system with FDGD where the group delay curve is irregular within the chaotic spectrum.

2.3. Time delay signature concealment

We performed both simulation and experiment to evaluate the TDS concealment capability of the FDGD module in the feedback loop. The experimental setup is the same as the emitter in Fig. 1. Traditional numerical approach for nonlinear chaotic system is Forth-order Runge-Kutta integration, which calculates the chaotic dynamics by time domain iteration, but the FDGD module is a frequency-dependent component, thus can only be modeled in frequency domain. Therefore, we take another method, the Split-Step Fourier Transformation, which is extensively used for dispersive media and non-linear dynamics [29]. 1,000,000 points were calculated in each trace, with a step size of 50 and a window width of 2,000.

Optics EXPRESS

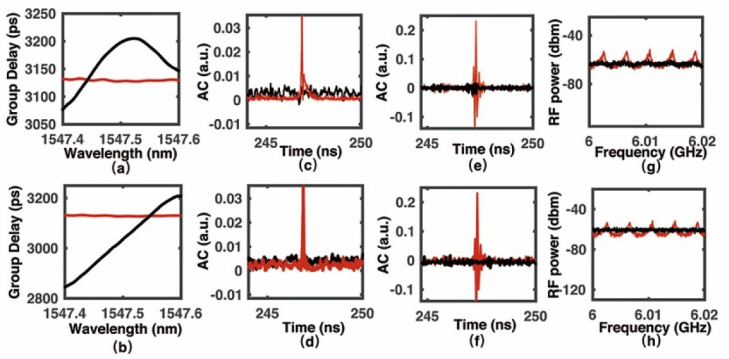

Fig. 4. Evidence of TDS concealment. To ensure reliable time delay concealment capability, we tested two different group delay curves in parabolic and linear shape, which are plotted in (a) (b), the corresponding TDS concealment ability is demonstrated in time domain (c) (d) (e) (f) and frequency domain (g) (h), both from numerical calculation (c) (d) and experimental demonstration (e) (f) (g) (h). Contrast between the situations with (black line) and without (red line) FDGD are distinguished by different colors in each figure.

To ensure reliable time delay concealment capability, we tested two different group delay curves in parabolic and linear shape, which are plotted in Fig. 4(a) and 4(b). The simulation results are shown in Fig. 4(c) and 4(d), while the experimental results are shown in Fig. 4(e)-4(h). In each plot, black and red lines represent the situation with and without FDGD, respectively. For the case without FDGD, the group delay is same for all the frequency components, while for the case with FDGD, we set linear and parabolic group delay curves within the chaotic spectral bandwidth as representative to verify the TDS capability of the FDGD module. Firstly, we adopt the time-series analysis method, the well-known auto-correlation function (ACF) trace to evaluate the TDS concealment performance. Without FDGD, there is a clear peak shown on the ACF trace, which is around 247 ns, exactly corresponding to the overall cavity time delay. For the case of FDGD with both linear and parabolic group delay curves, the peak is suppressed to an invisible value, proving the TDS concealment capability of the FDGD module. The agreement between simulation and experimental results proves the theoretical validity and robustness of the numerical model. Then we evaluate the TDS concealment using spectrum analysis method [16] and the experimental results are shown in Fig. 4(g) and 4(h). Without FDGD, the frequency resonance peaks with interval of 4.05 MHz, corresponding to the 247 ns peak in ACF traces, are observed on the electrical spectrum of the chaotic carrier. However, the frequency resonance peaks are disappeared for both linear and parabolic group delay curves, proving the TDS concealment capability of the FDGD module from the spectrum analysis method.

To crack a traditional chaotic optical system, eavesdroppers need to figure out the feedback delay time first, typically with auto-correlation method. With the acknowledge of delay time, they can figure out other hardware parameters with mathematical methods, then the whole system can be reconstructed and the chaotic system can be cracked. However, the TDS is suppressed by FDGD in the proposed system, which will prevent eavesdroppers from figuring out the delay time. If eavesdroppers try to generate the same FDGD curve with the chaotic transmitter by traversal algorithm to crack the system, they have to know all the other parameters first, otherwise even if they have the right FDGD curve, data still cannot be recovered from chaotic time series. But in order to figure out chaotic hardware parameters, they have to know the cavity delay time first, which is suppressed by FDGD. In general, it is the chaotic carrier that conceals the FDGD curve, and the FDGD curve in turn prevents the chaotic system parameters to be cracked, they build up a robust security system together.

Optics EXPRESS

2.4 Key space enlargement

After introducing the FDGD module into the chaotic system, the FDGD curve becomes a part of the secure key. According to the chaotic synchronization theory, the receiver should have a FDGD module made of the same material and with the same physical properties. Even so, mismatching in group delay curves due to different parameter setting of the FDGD module could result in decryption failure. This concept was proved by our simulation work. To demonstrate the security enhancement effect originated from the group delay curve of FDGD module, other influencing factors, that is, all the hardware parameters in the receiver side, are identical to that in the emitter in the following simulations.

The security level is evaluated by calculating the bit error rate (BER) of the received signal. The BER result is calculated by comparing the decrypted message with the original one, instead of using the formula of signal-to-noise ratio (SNR) relation with BER, therefore with a higher level of accuracy. For complete decryption of the received signal, the FDGD curves in emitter and receiver must be have a high matching-degree, including the cascaded numbers of G-T etalons, the structure and hardware parameters such as the cavity material, thickness and facet relativity of each G-T etalon. Even with the same hardware setting, the temperature variation of each G-T etalon will slightly affect the refractive index and the cavity thickness therefore changing the free spectrum range (FSR) of the group delay curve and the group delay peak position. In the following simulation, we assume the FDGD modules in emitter and receiver have the exactly same hardware setting and the mismatch only comes from the temperature setting of each G-T etalon. Since the temperature coefficient of G-T etalon varies with the manufacturing material and structure of the etalon, it is more convenient to describe the temperature mismatch of etalons using frequency mismatch of the group delay peaks.

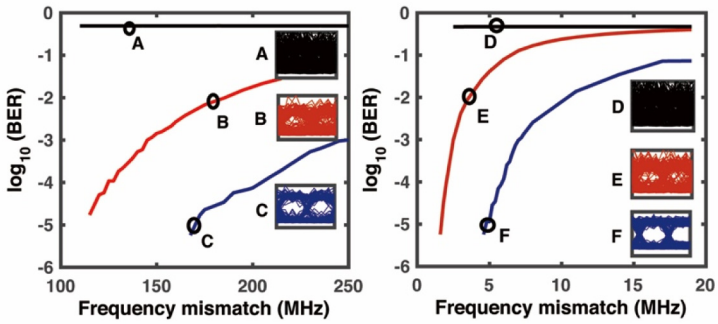

Fig. 5. BER variation of the decrypted signal with the frequency mismatch of the FDGD modules in emitter and receiver. (a) The FDGD modules in emitter and receiver have a single G-T etalon configuration. (b) The FDGD modules in emitter and receiver have 16 cascaded G-T etalons. The insets show corresponding eye diagrams. Black lines represent the BER results without decryption. Red and blue lines represent the evolution of BER according to the frequency mismatch of the center-positioned and edge-positioned etalon in FDGD module, respectively.

Figure 5(a) and 5(b) show the BER variation with frequency mismatch in two cases of FDGD pairs. In Fig. 5(a) the FDGDs at emitter and receiver side consist only one etalon, while in Fig. 5(b) the FDGD pair with 16 cascaded etalons are used. It should be noted that each etalon can be tuned independently, and the frequency mismatch in Fig. 5(b) comes from one of the 16 cascaded etalons. Insets show the corresponding eye diagrams. The power ratio between the message and the chaotic carrier is set at 1:5 so that message can be effectively concealed in chaotic time series. The message is non-return-to-zero on-off-keying (NRZ-OOK) signal operating at 10 Gb/s with pseudo-random bit sequence (PRBS) length of 2^{31}-1. As is presented above, the chaotic carrier bandwidth is mainly restricted by the bandwidth of

Optics EXPRESS

optical/electronic components in the feedback loop, but in simulation, we can easily adjust the chaotic bandwidth by changing the low and high cut off equivalent frequency in Eq. (10) and (11). In the following simulation, we set the chaotic bandwidth higher than 10 GHz, which is achievable using the commercial available components. Presumably, the influence of each etalon to synchronization quality will change with the relativeness of its center frequency to the center frequency of chaotic carrier. So both the influence of edge-positioned etalon, which means the group delay peak positioned at the edge of the chaotic carrier spectrum (blue line) and center-positioned etalon, whose group delay curve peak at the center of the chaotic carrier spectrum (red line) are investigated, and the BER before decryption is depicted in black line, where the FDGD module is not used in the receiver. The BER difference between red lines and blue lines in Fig. 5 proved our assumption that frequency mismatch of center-positioned etalons has much stronger influence on BER than edge-positioned etalons. Another important conclusion by comparing Fig. 5(a) and 5(b) is that as the number of cascaded etalons in FDGD increases, the synchronization quality will be more sensitive to the frequency mismatch of each etalon in FDGD. Considering the situation in Fig. 5(b) with 16 cascaded G-T etalons, for legal users, BER below 10^{-5} can be achieved with a 1 MHz frequency mismatch of the center-positioned etalon, while for eavesdroppers, under the most insensitive situation, that is, for the edge-positioned etalon, a 10 MHz frequency mismatch will cause the BER to degrade to 10^{-2}. For achieving perfect chaotic synchronization quality, the frequency tuning resolution of each etalon should be less than 1 MHz. Since a 0.001°C temperature tuning resolution can be achieved with commercially available thermal control solution, and considering the temperature coefficient of the etalon made by quartz is 0.67 GHz/°C around 1550 nm, thus 0.67 MHz frequency tuning resolution is possible to be achieved using quartz made etalon. Noted that the FDGD module with 16 cascaded G-T etalons made of silicon is commercially available but the one made of quartz needs to be customization. For the eavesdroppers, 10 MHz frequency mismatch on edge-positioned etalon, corresponding to a BER of 10^{-2}, is the critical point to achieve the useful information, therefore the eavesdroppers must tune the group delay peak of each etalon with a resolution of less than 10 MHz to crack the information even if they get the same FDGD module in the receiver and all the other receiver parameters are matched with the emitter, which is almost impossible in practice. To calculate the key space, we consider the maximal frequency tuning range of each etalon is 10 GHz, within the spectral bandwidth of the chaotic carrier, corresponding to around 15°C tuning range of the quartz made G-T etalon. One etalon can contribute 10^3 (10 GHz/10 MHz) key space to the security system, so 16 cascaded etalons together can enlarge the key space by 10^{48}. Since for the center-positioned etalon, frequency mismatch beyond 4 MHz will result in decryption failure, the key space should be much larger than 10^{48} in practice for the FDGD module with 16 cascaded G-T etalon made by quartz. Besides, from the calculation, we can see the key space of the proposed chaotic optical systems can be further improved by increasing the numbers of cascaded etalons, and increasing the spectral bandwidth of the chaotic carrier, which can be achieved by using high-speed modulator, RF driver and PD in the chaotic feedback loop.

3. Discussion and conclusion

In summary, we have proposed a chaotic optical system with a significant improvement in the level of security achieved by introducing a FDGD module into the electro-optic feedback chaotic system. In this proposed architecture, it is the chaotic carrier that conceals the FDGD curve, and the FDGD curve in turn prevents the chaotic system parameters to be cracked, so they build up a robust secure communication system together. It may be questioned that with such sensitivity to frequency shift, whether the unavoidable frequency detuning between the lasers and the FDGD curve causes detrimental effect. In fact, in the open-loop synchronization configuration, the laser output only serves as the optical carrier of the chaotic signal and will not affect the chaotic synchronization performance, which has also been

Optics EXPRESS

verified by our simulation, further proving the feasibility of the proposed scheme. We found there is no difference when we detune the laser wavelength between the chaotic emitter and receiver. Based on this principle, the laser wavelength could be modulated to increase the attack complexity for the eavesdroppers since it is more difficult to achieve the useful information from the broadened chaotic carrier spectrum.

More importantly, from the viewpoint of practical implementation, the FDGD modules are rather easy to be manufactured with the same hardware parameters such as cavity material, cavity length, facet reflectivity and cascaded cavity numbers. The software parameters, which are the temperature setting of each cavity can be preset after calibration, therefore no security parameter distribution and synchronization are required as other digital encryption methods. Any two FDGD modules with the same hardware parameters and software setting can be used in chaotic emitter and receiver for chaotic generation and synchronization. Once a FDGD module is in failure, one can replace it using another FDGD module with the same setting. These features make it feasible for massive deployment of chaotic optical communication.

Using theoretical and numerical investigation accompanied with experimental evaluation, we have proved that our proposed system integrates a valid time delay concealment and a huge additional key space without introducing much extra effort in implementation. As is presented in the article, a FDGD module with 16 G-T etalons will increase the key space of optical chaotic system by an impressive 10^{48}, the key space can even be further enlarged by increasing the cascaded number of etalons and the spectral bandwidth of chaotic carrier. We take the cascaded number of 16 and the chaotic carrier bandwidth of 10 GHz as an example to evaluate the security level just because these components are commercially available and the chaotic optical systems based on them are feasible. Besides, except for the cascaded G-T etalons, any other optical component with reconfigurable FDGD function can be used to enlarge the key space, as long as an identical one is available at the receiver side to synchronize the chaotic carrier and decrypt the signal. We should aware of the fact that it's very difficult to achieve an equivalent security key space with traditional encryption methods, which can employ complicate encryption algorithms. Even so, investigations on chaotic optical communications are still beneficial because the information can be physically protected, which provides physical-layer security on the basis of algorithm encryption methods.

After solving the security issue of the chaotic optical communication, we assume increasing the chaotic transmission speed, extending the chaotic transmission distance and networking multiple chaotic nodes will become more important topics and the related work is under investigations now. We anticipate this research will pave the way for the practical applications of chaotic optical communication, as well as inspire other new ideas for chaos dynamics.

Funding

National Natural Science Foundation of China (NSFC) (61322507).

Acknowledgments

The authors thank Dr. Amos Martinez from Aston University for fruitful discussion and manuscript polishing, also thank II-VI photonics to provide the TDC module for time delay concealment experiment.