

基于动态参数的光电延迟振荡系统及其保密通信研究

胡汉平 苏 威 于志良* 刘凌锋

(华中科技大学图像识别与人工智能研究所, 湖北 武汉 430074)

摘要 由于现有的基于非线性器件的混沌系统(Ikeda 系统)容易受到重构攻击,影响通信的安全。在此基础上提出了一种基于非线性器件参数动态变化的光电延迟反馈混沌系统和基于该系统的安全通信方案。通过第一级混沌系统的输出改变注入激光的光强,使得第二级系统的增益系数产生动态变化,增加了系统可控参数的数目,进而对第二级系统的混沌动力学特性进行数值分析。分析了该系统在混沌调制下的同步通信情况,并且分析了增益系数不匹配和延迟时间不匹配等参数不匹配情况对系统同步的影响。实验结果表明本方法能提高混沌系统的复杂性,实现混沌保密通信。

关键词 非线性光学;混沌产生;光电反馈;混沌同步;混沌通信

中图分类号 O43 **文献标识码** A **doi**: 10.3788/AOS201333.0506006

Chaos Generation of Variable Parameters and Secure Communication Based on Optoelectronic Feedback Oscillation

Hu Hanping Su Wei Yu Zhiliang Liu Lingfeng

(Institute for Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan, Hubei 430074, China)

Abstract A new chaotic system and secure communication method are proposed based on optoelectronic feedback device with variable parameters, because the present system is easily attacked by the method of parameter estimation so as to affect the security of the communication. Dynamical changes of the gain coefficient of the second-class system are generated by changing the injected light intensity through the output of the first-class system, which increases the number of controllable parameters in the system. The chaotic dynamics of the system are theoretically and numerically analyzed. The communication situation of the system in the chaotic modulation conditions and the chaos synchronization when the parameters including gain coefficient and time delay are not compatible is analyzed. The experimental results show that this scheme can increase the chaotic complexity, and can achieve the chaotic secure communication.

Key words nonlinear optics; chaos generation; optoelectronic feedback; chaotic synchronization; chaotic communication

OCIS codes 140.1540; 140.3560; 190.4360; 230.0250

1 引 言

混沌信号具有不可预测、初值高度敏感等特性,这使得混沌保密通信具有极高的安全性^[1~3]。由于激光混沌具有宽频谱、低衰减和高传输速率等优点^[4],从欧盟的 OCCULT 和 PICASSO^[5] 计划实施以来,基于激光混沌的保密通信系统的研究成为了热点。国内在激光通信领域也有较多的研究成

果^[6~10]。目前光混沌产生方式主要有基于半导体激光器的光注入、光反馈、光电反馈和基于非线性器件的光电延迟反馈。然而在光注入和光反馈的系统中由于其对相位波动和漂移的敏感性等限制了它们在商业网络中的大规模部署,而基于非线性器件的延迟光电反馈系统具有可以利用现有光通信系统的常用器件、便于调节和混沌复杂度高等优点,得到了

收稿日期: 2012-11-06; 收到修改稿日期: 2013-01-29

基金项目: “十二五”国家密码基金(MMJJ201102016)资助课题。

作者简介: 胡汉平(1960—),男,博士,教授,博士生导师,主要从事信息安全方面的研究。E-mail: 577647317@qq.com

* 通信联系人。E-mail: shxboy@gmail.com

广泛的应用^[11]。

光混沌保密通信要求混沌载波有较宽的频谱才能够有效地掩盖信息,防止被窃听,在基于非线性器件的光电延迟反馈混沌系统中,可以通过增加系统的增益系数来实现。同时 Vicente 等^[12]的研究证明系统的复杂度随着增益系数的增加而增加,然而实验表明增益系数受到器件带宽的限制;另外,针对该系统 Udaltsov 等^[13,14]提出了一种分析非线性函数类型和重构系统参数的一类破解方法,因此现有的基于非线性器件的光电延迟反馈系统并不安全。

本文提出了一种基于非线性器件的动态参数的光电延迟反馈混沌系统。通过增益系数动态的变化,改进混沌系统的结构,在相同的增益系数条件下提高了混沌系统的复杂度和抗攻击能力。研究了参数不匹配对该系统同步的影响,实现了在混沌调制情况下保密通信系统的搭建。

2 变参数光电延迟反馈混沌系统结构

本文提出的变参数光电延迟反馈混沌系统结构

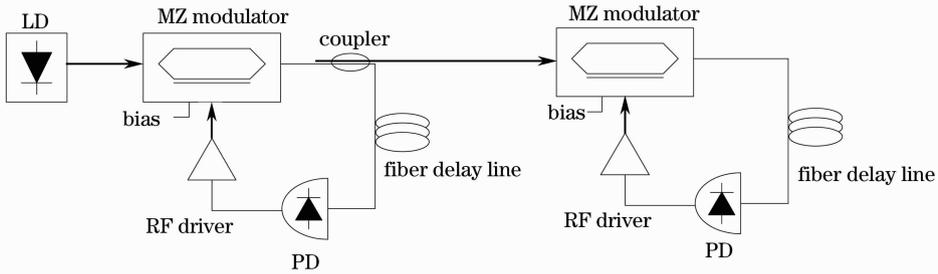


图 1 变参数混沌系统框图

Fig. 1 Block diagram of the chaotic system with variable parameters

令 $x_1(t) = \frac{\pi V(t)}{2V_{\pi RF}}$; 高通截止时间 $\tau = \frac{1}{2\pi f_H}$; 低

通截止时间 $\theta = \frac{1}{2\pi f_L}$; $\phi_1 = \frac{\pi V_B}{2V_{\pi DC}}$, $\beta_1 = PgGA \frac{\pi}{2V_{\pi RF}}$,

其中 ϕ_1, β_1 分别代表第一级系统中 MZ 调制器的偏置和增益系数。由于 $f_H \gg f_L$, 第一级系统方程变为

$$x_1(t) + \tau \frac{d}{dt} x_1(t) + \frac{1}{\theta} \int_{t_0}^t x_1(t) dt = \beta_1 \cos^2[x_1(t - T_1) + \phi_1]. \quad (3)$$

时滞微分方程(3)式也被称为 Ikeda 方程。基于 Ikeda 方程的系统为超混沌系统,具有高维的吸引子,已证明系统的 Lyapunov 维数在 $T_1 = 30$ ns, $\beta_1 = 5$ 时大于 1000^[15]。

根据(3)式,第一级系统的输出为

$$C_1(t) = P \cos^2[x_1(t) + \phi_1]. \quad (4)$$

如图 1 所示。其中 LD 为连续光激光二极管(波长 $\lambda = 1550$ nm),功率为 P ;马赫-曾德尔(MZ)调制器作为系统的非线性器件,输出特性为

$$P_{out} = P_{in} \cos^2 \left[\frac{\pi V(t)}{2V_{\pi RF}} + \frac{\pi V_B}{2V_{\pi DC}} \right], \quad (1)$$

式中 P_{out} 为输出的光功率, P_{in} 为输入光功率, $V(t)$ 为加载在 MZ 调制器上的调制电压,偏置电压用 V_B 表示, $V_{\pi RF}$ 为射频(RF)半波电压, $V_{\pi DC}$ 为偏置半波电压。PD 为快速光电转换器,有一定的放大作用,增益为 g ; RF 驱动器用来驱动 MZ 调制器,同时也起带滤波器的作用,增益为 G 。带通滤波器的高低截止频率分别为 f_H 和 f_L 。整个第一级系统的衰减为 A 。则第一级系统方程为

$$\left(1 + \frac{f_L}{f_H}\right) V(t) + \frac{1}{2\pi f_H} \frac{d}{dt} V(t) + 2\pi f_L \int_{t_0}^t V(t) dt = PgGA \cos^2 \left[\frac{\pi V(t - T_1)}{2V_{\pi RF}} + \frac{\pi V_B}{2V_{\pi DC}} \right], \quad (2)$$

式中 T_1 为第一级系统的光延迟。

将混沌光 $C_1(t)$ 注入第二级系统的 MZ 调制器中,调制产生新的混沌光载波。若设第二级系统的光延迟为 T_2 , MZ 调制器的偏置为 ϕ_2 , 增益系数为 β_2 , 设两级系统的器件参数相同, 则 $\beta_2 = C_1(t) g'G'A' \frac{\pi}{2V_{\pi RF}}$, 整个系统的动力学方程为

$$x_2(t) + \tau \frac{d}{dt} x_2(t) + \frac{1}{\theta} \int_{t_0}^t x_2(t) dt = k_2 \cos^2[x_1(t - T_2) + \phi_1] \cos^2[x_2(t - T_2) + \phi_2], \quad (5)$$

式中 $k_2 = Pg'G'A' \frac{\pi}{2V_{\pi RF}}$ 。

3 混沌系统仿真分析

取 $T_1 = T_2 = 30$ ns, $\phi_1 = \phi_2 = \pi/4$, $\tau = 20$ ps,

$\theta = 1.6 \mu s, \beta_1 = k_2 = 5$ 。

(5)式为时滞微分方程,可以通过 Runge-Kutta 方法求解。运用 Matlab 进行仿真,步长设置为 1×10^{-11} 。

图 2 和图 3 为第一级混沌系统与变参数混沌系

统在时域上的对比。

为了观察混沌系统的整体特性,图 4 和图 5 显示了两个系统的混沌分叉图。对其进行了对比,发现新混沌系统能够更快地进入混沌状态,便于实现保密通信。

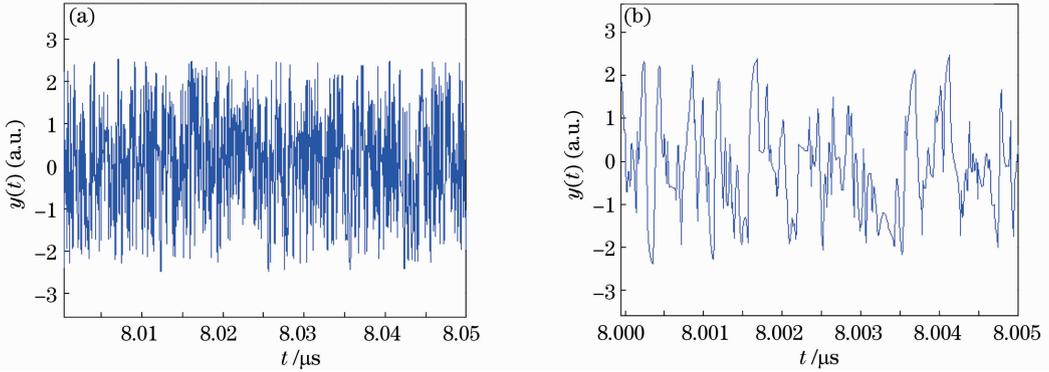


图 2 (a)第一级混沌系统时域图;(b)放大图

Fig. 2 (a) Time-domain diagram of the first-level chaotic system; (b) details for (a)

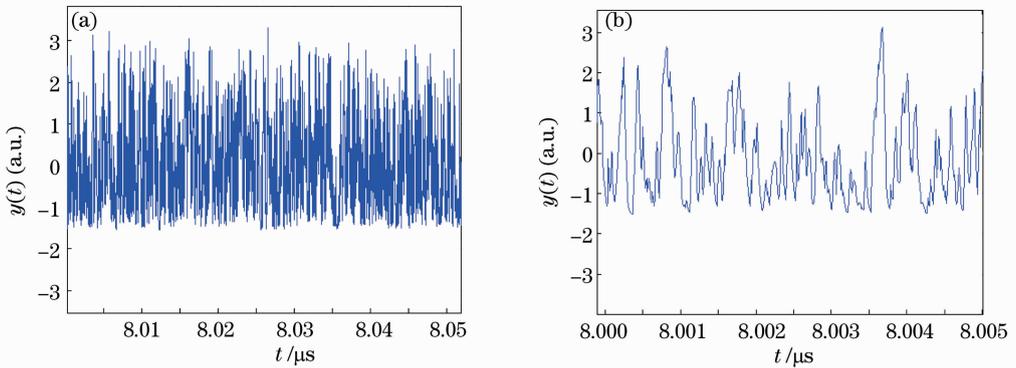


图 3 (a)变参数混沌系统时域图;(b)放大图

Fig. 3 (a) Time-domain diagram of the variable parameters chaotic system; (b) details for (a)

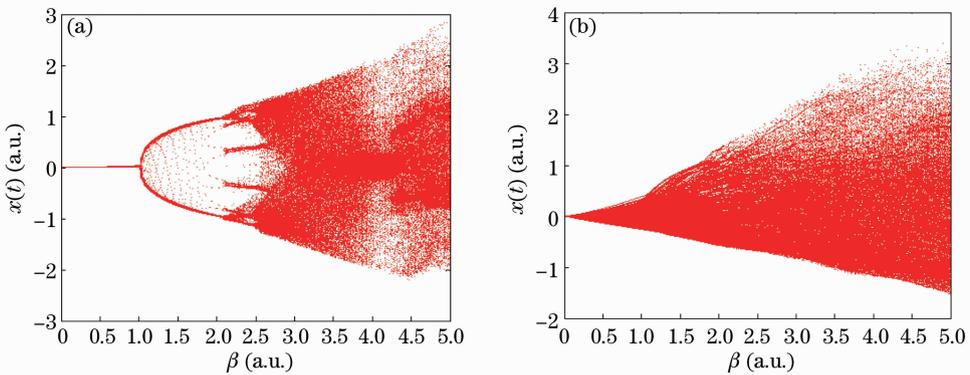


图 4 (a)第一级系统和(b)变参数系统的混沌分叉图

Fig. 4 Chaotic bifurcation diagrams of (a) the first-level system and (b) the variable parameters system

4 混沌同步通信系统

图 6 为变参数混沌系统的同步通信框图,调制

的光信号可以用 $p_0 m(t)$ 来表示,其中 p_0 代表信号 1 的光强度, $m(t)$ 为信息信号,系统动力学方程为

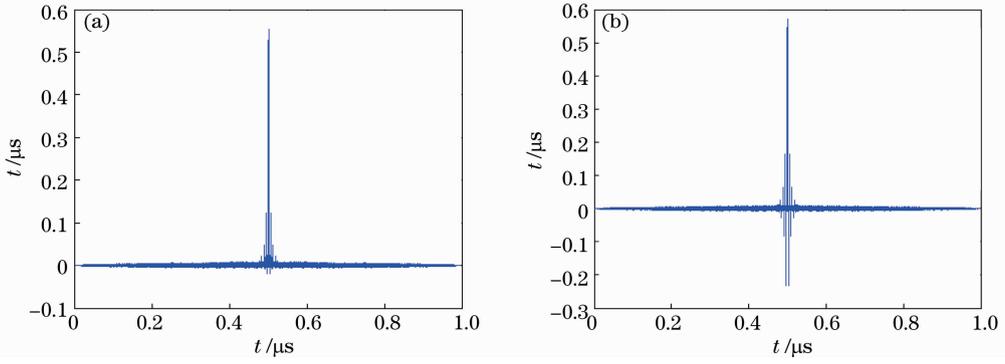


图 5 (a)第一级系统和(b)变参数混沌系统输出的自相关图

Fig. 5 Autocorrelagram of (a) the first-level system and (b) the variable parameters system

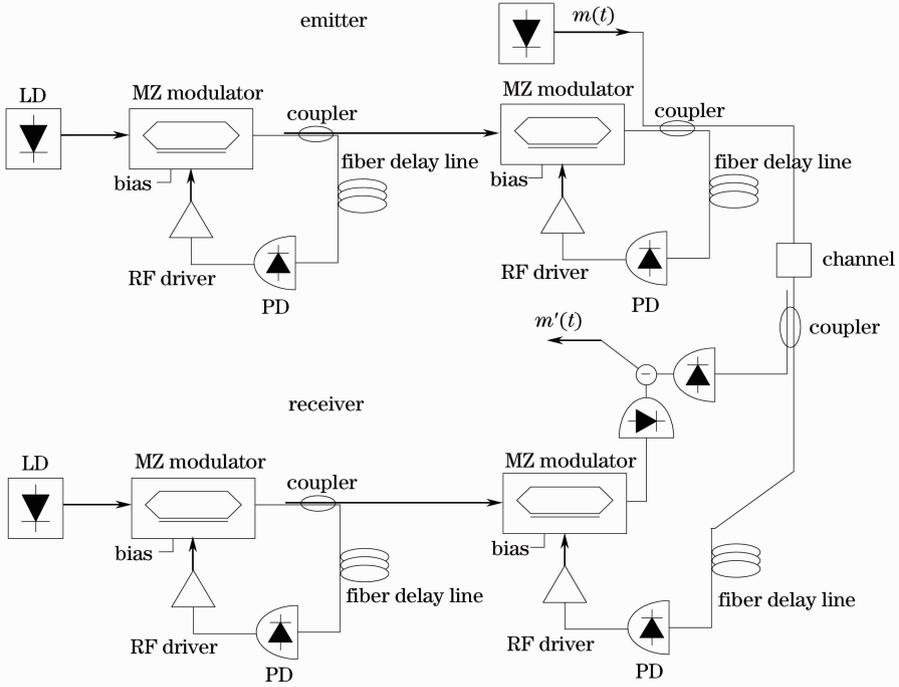


图 6 系统同步通信框图

Fig. 6 System structure with synchronization

$$x_2(t) + \tau \frac{d}{dt}x_2(t) + \frac{1}{\theta} \int_{t_0}^t x_2(t) dt = k_2 \cos^2[x_1(t - T_2) + \phi_1] \cos^2[x_2(t - T_2) + \phi_2] + k_2 (p_0/P) m(t - T_2). \quad (6)$$

信道中传输的信号为

$$C(t) = P \cos^2[x_1(t) + \phi_1] \cos^2[x_2(t) + \phi_2] + p_0 m(t). \quad (7)$$

接收端通过开环对称自同步结构,从第二级 MZ 调制器输出端恢复出混沌载波信号,接收端动力学方程为

$$y_2(t) + \tau \frac{d}{dt}y_2(t) + \frac{1}{\theta} \int_{t_0}^t y_2(t) dt = k'_2 C(t - T_2). \quad (8)$$

当接收端与发射端参数完全匹配时,(6)式和(8)式的解相同,即

$$x_2(t) = y_2(t). \quad (9)$$

接收端第二级 MZ 调制器输出为

$$Q(t) = P \cos^2[y_1(t) + \phi_1] \cos^2[y_2(t) + \phi_2]. \quad (10)$$

接收端恢复的信息信号为

$$m'(t) = C(t) - Q(t) = p_0 m(t). \quad (11)$$

由于第一级混沌系统的存在,使得通过时间极

值分析非线性方程的参数来达到破译系统的方法^[16,17]难以实现,因为第二级系统的增益系数是动态变化的,这要求在接收端两个混沌系统都同步的情况下,信号才能恢复出来。

信号的调制深度 ξ 定义为

$$\xi = \frac{\langle |p_0 m(t)| \rangle}{\langle |P \cos^2[x_1(t) + \phi_1] \cos^2[x_2(t) + \phi_2]| \rangle} \quad (12)$$

为了观察调制深度 ξ 对混沌的影响,用 Matlab 仿真,取步长为 1×10^{-12} , $m(t)$ 取 10 Gb/s 的随机序列如图 7(a)所示。图 7(b)和(c)分别显示调制深度为 0%的信号(即未加信号)和 1%的信号输出时的时间序列图。图 8 为调制深度为 1%时发射端和接收端的混沌同步情况。其中传输通道仿真为 400 km 的对称色散补偿模块,采用分步傅里叶数值求解算法,对光纤的非薛定谔方程求解。从图中可以看出,系统仍

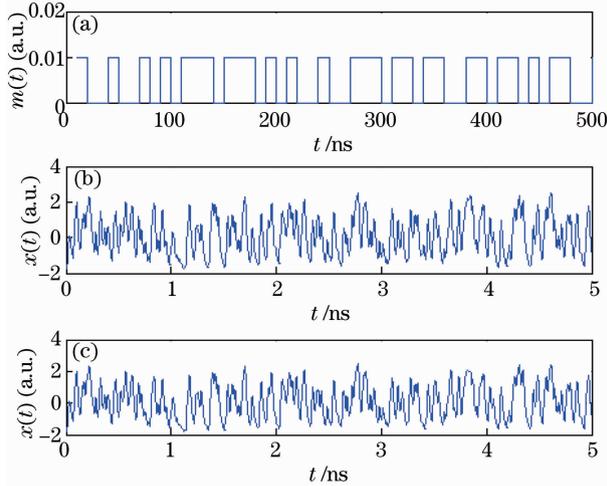


图 7 (a)信息信号、调制深度为(b) 0%和(c)1%的信号输出时的时间序列图

Fig. 7 (a) Time-domain diagram of message and the outputs with modulation depth of (b) 0% and (c) 1%

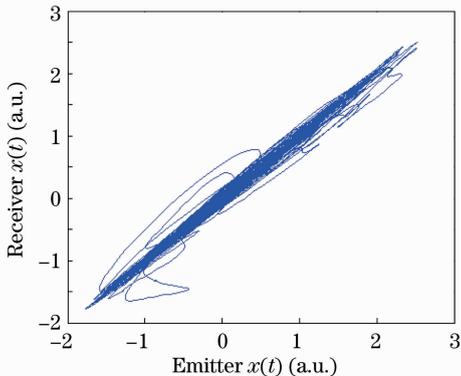


图 8 调制深度为 1%时系统的同步情况

Fig. 8 Synchronization with modulation depth of 1%

能保持较好的同步性能。

同时还分析了加入信息信号之后的系统同步误差 σ 与不同调制深度 ξ 之间的关系,如图 9 所示,在实际通信中可以根据相应的同步误差规定来选取调制深度。

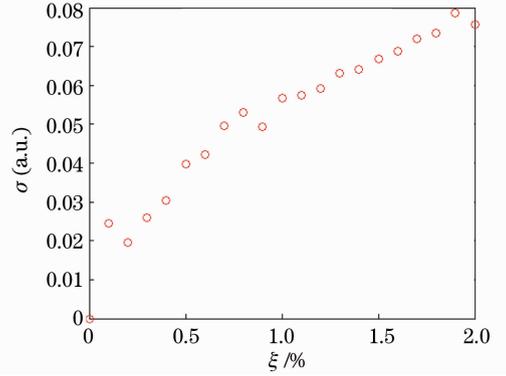


图 9 加入信息信号之后的系统同步误差 σ 与调制深度 ξ 之间的关系

Fig. 9 Relationship between system error σ and modulation depth ξ after inputting information signal

5 参数不匹配情况下的系统同步

本系统因为拥有两个混沌系统,可调参数包括第一级和第二级系统的延迟时间 T ,偏置相位 ϕ ,增益系数 β ,高通和低通截止时间 τ 和 θ 。假设发送端第一级系统和接收端第一级系统的参数完全匹配,只分析第二级系统参数不匹配对整个通信系统同步的影响。

由于 MZ 调制器的偏置相位 ϕ 一般设置为固定值,高低频特征时间 τ 和 θ 则主要由器件的设置来决定,通信中通常不会变动,所以主要分析了增益系数 β 不匹配和延迟时间 T 不匹配的情况。

5.1 增益系数 β 不匹配

用平均同步误差 σ 来衡量参数不匹配所造成的影响。发送端的输出为 $x(t)$,参数不匹配情况下的接收端输出为 $x'(t)$,则

$$\epsilon_{\Delta r} = x(t) - x'(t), \quad (13)$$

$$\sigma = \sqrt{\frac{\langle \epsilon_{\Delta r}^2 \rangle}{\langle x(t)^2 \rangle}}, \quad (14)$$

式中 $\langle \rangle$ 为取时间的平均。

仿真参数选取与前面相同。当接收端的第二级系统增益发生不匹配时, $k'_2 = k_2(1 + \eta)$, η 为不匹配度。

图 10 和图 11 显示不匹配度为 1%时发射端和接收端的混沌同步情况。

当第二级系统的增益不匹配度 η 在 0%~2%

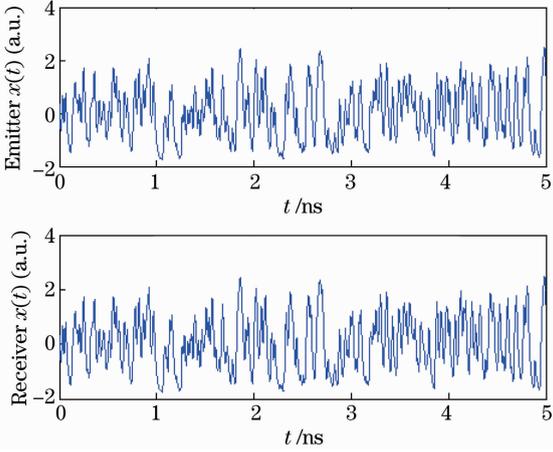


图 10 发射系统和接收系统的时间序列图

Fig. 10 Time-domain diagrams of the emitter and receiver

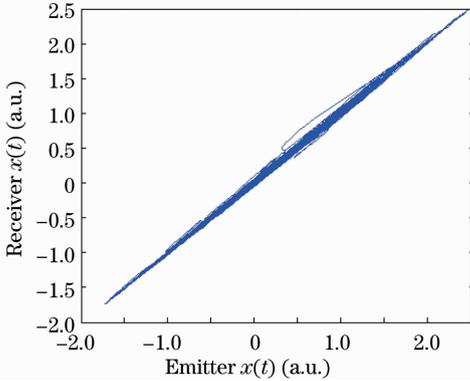


图 11 $\eta=1\%$ 时系统的同步效果图

Fig. 11 Synchronization with mismatch $\eta=1\%$

变化的时候,整个系统的同步误差 σ 变化情况如图 12 所示。

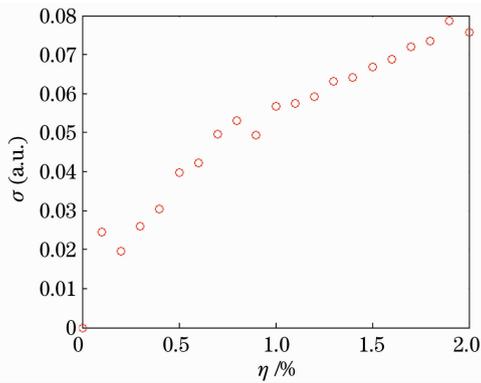


图 12 增益系数 β 不匹配时的系统同步误差图

Fig. 12 Synchronization error with the gain coefficient mismatch

5.2 延迟时间 T 不匹配

当延迟时间 T 不匹配,例如延迟时间增加 2 ps 时,如图 13 所示,发现得到的波形相比原波形会发生一个前移,同时在一些细节方面发生变化。从图 14 可以看出延迟不匹配 2 ps(10%)时的同步效果并

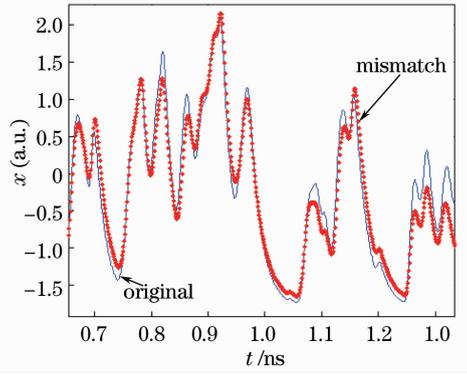


图 13 延迟不匹配 2 ps 时的时域效果对比图

Fig. 13 Time-domain diagram with the delay time mismatch of 2 ps

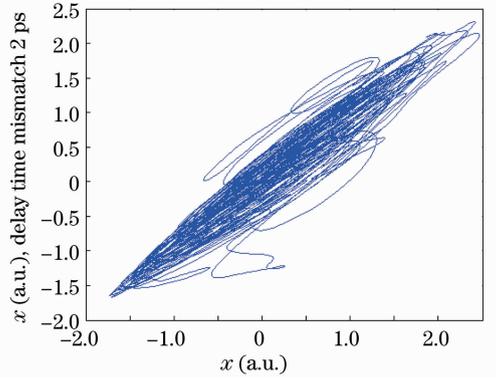


图 14 系统同步效果图

Fig. 14 Synchronization of the system

不好。

为了进一步分析延迟时间 T 对系统同步的影响,计算了不同延迟时间 T 误差所产生的同步误差,如图 15 所示。

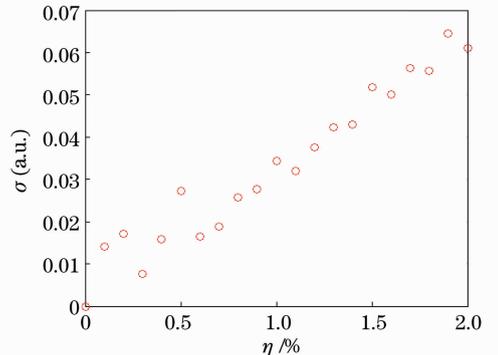


图 15 系统同步误差 σ 与延迟时间不匹配度 η 之间的关系

Fig. 15 Relationship between system error σ and the time delay mismatch η

6 结 论

提出了一种新的基于非线性器件的光电延迟混

沌通信系统的构建方法,通过增加一个混沌系统使得原混沌系统的增益系数动态变化,同时也增加了可调参数的数目,该结构增加了系统的复杂性和抗攻击的能力。同时分析了系统参数不匹配时的同步情况,得到了不同参数不匹配对系统同步误差的影响。系统通过混沌调制的方式能够实现保密通信,分析了信号调制深度与混沌同步误差之间的关系,为选取合适的信号调制深度提供了参考。

致谢 感谢夏光琼教授、王云才教授和颜森林教授对作者的指导和帮助。

参 考 文 献

- 1 L. M. Pecora, T. L. Carroll. Synchronization in chaotic systems [J]. *Phys. Rev. Lett.*, 1990, **64**(8): 821~824
- 2 L. M. Pecora, T. L. Carroll. Driving systems with chaotic signals [J]. *Phys. Rev. Lett.*, 1991, **44**(4): 2374~2383
- 3 R. Brown, N. F. Rulkov, N. B. Tufillaro. Synchronization of chaotic systems; the effects of additive noise and drift in the dynamics of the driving [J]. *Phys. Rev. Lett.*, 1994, **50**(6): 4488~4508
- 4 C. R. Mirasso, P. Colet, P. Garcia-Fernandez. Synchronization of chaotic semiconductor lasers: application to encoded communications [J]. *IEEE Photon. Technol. Lett.*, 1996, **8**(2): 299~301
- 5 V. Annovazzi-Lodi, A. Argyris, M. Benedetti *et al.*. A chaos-based approach to secure communications [J]. *Optics & Photonics News*, 2008, **19**(10): 36~41
- 6 Xu Yin, Zhang Hua. Solution and stability of ultraviolet localized optical vortex solitons in air [J]. *Acta Optica Sinica*, 2012, **32**(6): 0619003
徐寅, 张华. 空气中紫外波长局域涡旋光孤子的解及其稳定性[J]. *光学学报*, 2012, **32**(6): 0619003
- 7 An Junge, Wu Baojian, Li Zhi *et al.*. Influence of fiber loss on optical parametric process with pump depletion [J]. *Acta Optica Sinica*, 2012, **32**(6): 0619001

- 安俊鸽, 武保剑, 李智等. 光纤损耗对抽运消耗光纤参变过程的影响分析[J]. *光学学报*, 2012, **32**(6): 0619001
- 8 Li Liyan, Wu Bing, Yuan Yonggui *et al.*. Research on nonlinear error compensation method for single-frequency laser interferometer [J]. *Acta Optica Sinica*, 2011, **31**(7): 0726003
李立艳, 吴冰, 苑勇贵等. 单频激光干涉仪非线性误差补偿方法研究[J]. *光学学报*, 2011, **31**(7): 0726003
- 9 Yang Fei, Chen Dijun, Pan Zhengqing *et al.*. Short linear cavity single-frequency fiber laser with active frequency stabilization by fiber Bragg grating [J]. *Chinese J. Lasers*, 2012, **39**(9): 0902005
杨飞, 陈迪俊, 潘政清等. 光纤光栅主动稳频的短直线腔单频光纤激光器 [J]. *中国激光*, 2012, **39**(9): 0902005
- 10 Liu Yujin, Zhang Shenghai, Yang Hua *et al.*. Application in secret communication of chaos driving synchronization of vertical cavity surface emitting lasers with optical feedback [J]. *Chinese J. Lasers*, 2012, **39**(9): 0905004
刘玉金, 张胜海, 杨华等. 反馈垂直腔面发射半导体激光器的混沌驱动同步在保密通信中的应用[J]. *中国激光*, 2012, **39**(9): 0905004
- 11 A. Argyris, D. Syvridis, L. Larger. Chaos-based communications at high bit rates using commercial fibre-optic links [J]. *Nature*, 2005, **438**(7066): 343~346
- 12 R. Vicente, J. Dauden, P. Colet *et al.*. Analysis and characterization of the hyperchaos generated by a semiconductor laser subject to a delayed feedback loop [J]. *IEEE J. Quantum Electron.*, 2005, **41**(4): 541~548
- 13 V. S. Udaltsov, J. P. Goedgebuer, L. Larger *et al.*. Cracking chaos-based encryption system ruled by nonlinear time delay differential equations [J]. *Phys. Lett. A*, 2003, **308**(1): 54~60
- 14 V. S. Udaltsov, L. Larger, J. P. Goedgebuer. Time delay identification in chaotic cryptosystems ruled by delay-differential equations [J]. *J. Opt. Technol.*, 2005, **72**(5): 373~377
- 15 Romain Modeste Nguimdo. Chaos and Synchronization in Opto-Electronic Devices with Delayed Feedback [D]. Palma de Mallorca: Universitat de les Illes Balears, 2011
- 16 M. D. Prokhorov, V. I. Ponomarenko, A. S. Karavaev *et al.*. Reconstruction of time-delayed feedback systems from time series [J]. *Physica D*, 2005, **203**(3-4): 209~223
- 17 Xiaogang Wu, Zuxi Wang. Estimating parameters of chaotic systems synchronized by external driving signal [J]. *Chaos, Solitons & Fractals*, 2007, **33**(2): 588~594

栏目编辑: 王晓球