

基于双光电反馈振荡器的单向混沌同步通信*

操良平¹, 董晓云², 王泽钰¹, 汪崇渝¹

(1. 重庆师范大学 教育科学学院, 重庆 401331; 2. 重庆师范大学 初等教育学院, 重庆 400700)

摘要:利用半导体激光器和马赫-曾德尔调制器构建了一个基于双光电反馈振荡器的单向混沌同步通信系统,数值研究了该系统的同步特性及通信性能。结果表明,系统输出的混沌波具有更宽的频带和更为复杂的频谱,有利于提高通信容量和系统的安全性;当系统无参数失配时,能获得高质量混沌同步,并能实现实时通信;参数失配对系统同步性能和通信质量有影响,但在一定的参数失配范围内,系统仍能实现较好的混沌通信。

关键词:混沌同步;混沌通信;双光电反馈;半导体激光器;马赫-曾德尔调制器

中图分类号: TN248.4; TN918.91

文献标志码: A

文章编号: 1672-6693(2014)04-0126-05

随着计算机科学技术和网络技术的飞速发展,现代社会对通信的安全性和通信容量提出了更高要求。2005年,王小云等先后破译了用于构造公众密钥的 MD5 系列 Hash 函数及 Hash 函数标准 SHA-1^[1-2],轰动了密码界。这表明传统密码体制的安全性随着密码学和计算机技术的发展已受到巨大挑战。近年来,利用物理学原理来保护信息的混沌加密技术倍受相关领域学者的关注。与传统加密方式相比,混沌保密通信将加密过程从算法层降低到物理层,因而提高了通信的保密性^[3]。早期的激光混沌保密通信系统大多采用单外腔光反馈半导体激光器(Semiconductor laser, SL)作为混沌发射源^[4-8]。虽然其结构简单、易于实现两个以上正 Lyapunov 指数的混沌输出,但是,随着人们对延时系统分析技术的不断提高,使得从激光器混沌输出获取相关参数重构不法系统成为可能^[9-11],这无疑将使混沌通信的安全性受到严重威胁。针对这一问题,相关领域学者提出了采用双光反馈 SL 系统来提高混沌载波的复杂性,增加信息破译难度^[12-14]。双光反馈 SL 系统产生的混沌信号不仅能很好地隐藏外腔反馈延时特征^[15],而且比单光反馈 SL 系统产生的混沌输出具有更高的关联维数和更大的混沌带宽^[16],这将有利于提高混沌通信的安全性和通信容量。然而,目前大多数相关研究主要集中于相干光双反馈 SL 系统,而对双光电反馈振荡器系统的研究还相对比较少。基于此,本文利用 SL 和马赫-曾德尔调制器(Mach-Zehnder modulator, MZ)组成双光电延迟反馈振荡器,构建了一个单向混沌同步通信系统(图1),其混沌输出具有较高的关联维数和大的带宽;系统对光相位作用不敏感,更容易实现混沌同步,提高通信性能。

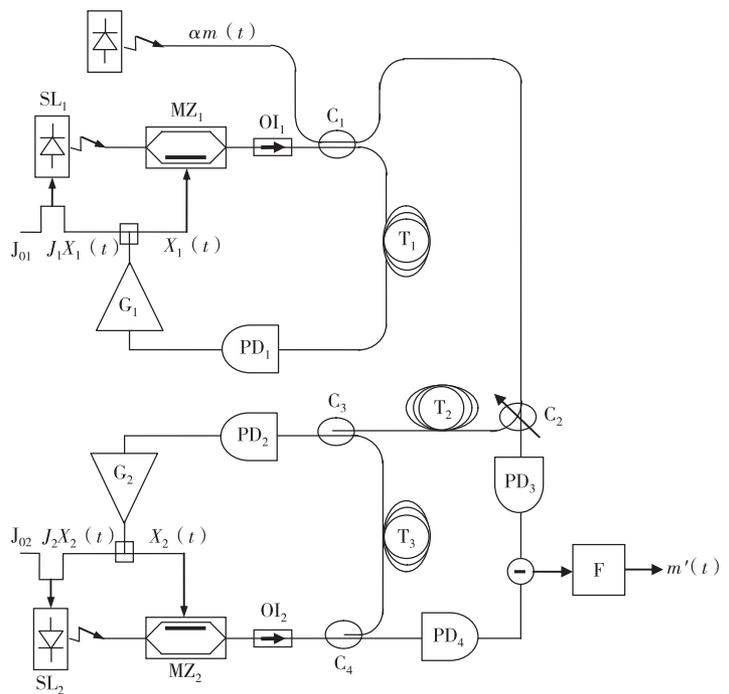


图1 基于双光电反馈振荡器的单向混沌同步通信系统示意图

* 收稿日期:2013-09-22 修回日期:2013-11-22 网络出版时间:2014-7-3 23:03
资助项目:国家自然科学基金(No. 11204248);重庆市教委科学技术研究资助项目(No. KJ130621)
作者简介:操良平,副教授,研究方向为光通信,E-mail:CLP1999@163.com
网络出版地址:http://www.cnki.net/kcms/detail/50.1165.N.20140703.2303.025.html

1 系统模型

在图1中发射机激光器 SL_1 发出的激光经调制器 MZ_1 、光隔离器 OI_1 在光耦合器 C_1 处与待传送信息 $m(t)$ 耦合后被分为两路。一路经延迟线 T_1 、光电探测器 PD_1 和射频放大器 G_1 反馈回 SL_1 和 MZ_1 形成双光电反馈,使其产生混沌输出;另一路经光纤注入接收端,在 C_2 处又被分为两束。其中,一束通过 T_2 ,在 C_3 处与接收机自反馈激光耦合后通过 PD_2 、 G_2 分别注入接收机激光器 SL_2 和调制器 MZ_2 ;另一束通过 PD_3 后与 MZ_2 的输出相减,再经滤波器 F 实现对信息 $m(t)$ 的解码(解码恢复的信息为 $m'(t)$)。调节 C_2 可改变发射机注入接收机的激光强度。与其它光电反馈振荡器系统相比,该系统不同之处在于 SL 本身也处于混沌状态,因此产生的混沌载波更为复杂。在该系统中,如果去掉调制器 MZ ,系统将变为单光电反馈 SL 的混沌通信系统^[17]。

2 理论分析

基于 SL 及 MZ 的理论模型^[18],在未加载信息 $m(t)$ 时,图1系统的动力学行为可用下列速率方程组描述:

$$\frac{dS_1(t)}{dt} = [G_1(N_1) - \gamma_1]S_1(t) \quad (1)$$

$$\frac{dN_1(t)}{dt} = J_{01} - \gamma_{e1}N_1(t) - G_1S_1(t) + J_1X_1(t) \quad (2)$$

$$X_1(t) + \tau_1 \frac{dX_1(t)}{dt} + \frac{1}{\theta_1} \int_{t_0}^t X_1(s) ds = \beta_1 S_1(t - T_1) \cos^2[X_1(t - T_1) + \varphi_1] \quad (3)$$

$$\frac{dS_2(t)}{dt} = [G_2(N_2) - \gamma_2]S_2(t) \quad (4)$$

$$\frac{dN_2(t)}{dt} = J_{02} - \gamma_{e2}N_2(t) - G_2S_2(t) + J_2X_2(t) \quad (5)$$

$$X_2(t) + \tau_2 \frac{dX_2(t)}{dt} + \frac{1}{\theta_2} \int_{t_0}^t X_2(s) ds = \beta_2 S_2(t - T_2) \cos^2[X_2(t - T_2) + \varphi_2] + \sigma S_1(t - T_s) \cos^2[X_1(t - T_s) + \varphi_1] \quad (6)$$

其中, $G_i(N_i) = \frac{g_c(N_i - N_0)}{1 + \epsilon S_i(t)}$, $i=1,2$; S 为激光器腔内光子数; N 为载流子数; N_0 为透明载流子数; g_c 为激光增益系数; γ 为光子衰变速率; γ_e 为载流子衰变速率; ϵ 为饱和系数; J_0 为激光器偏置电流; $X(t)$ 为光电反馈函数, $JX(t)$ 为激光器的反馈电流; $\tau = 1/(2\pi f_H)$, $\theta = 1/(2\pi f_L)$, f_H 、 f_L 分别是 MZ 的高频和低频截止频率; φ 是偏置相位; β 为自反馈系数; σ 为注入系数; T_s 为注入延迟时间, T 为自反馈延迟时间。在理想情况下, MZ 输出的功率 $p = h\nu S \cos^2[X(t) + \varphi]$, h 为普朗克常数, ν 为光子频率。

系统输出的同步性能由互相关函数来表征,其定义为

$$C(\Delta t) = \frac{\langle [P_1(t) - \langle P_1(t) \rangle][P_2(t + \Delta t) - \langle P_2(t) \rangle] \rangle}{\sqrt{\langle |P_1(t) - \langle P_1(t) \rangle|^2 \rangle \langle |P_2(t) - \langle P_2(t) \rangle|^2 \rangle}}$$

其中: $P(t)$ 是 MZ 的输出功率, Δt 是计算关联函数的时移, $\langle \cdot \rangle$ 表示对时间求平均。互相关函数的域值为 $[-1, 1]$, $|C(\Delta t)|$ 越大,系统收发两端的同步质量越高。当 $|C(\Delta t)| = 1$ 时,表明系统达到完全同步状态。

3 结果与讨论

采用四阶 Runge-Kutta 对方程(1)~(6)进行数值求解。为了简便,假设 SL 、 MZ 具有相同的内部参量,相关参数取值为: $g_c = 1.5 \times 10^4 \text{ s}^{-1}$, $\epsilon = 5 \times 10^{-7}$, $\gamma = 3.3 \times 10^{11} \text{ s}^{-1}$, $\gamma_e = 5.0 \times 10^8 \text{ s}^{-1}$, $N_0 = 1.2 \times 10^8$, $\tau = 25 \text{ ps}$, $\theta = 5 \text{ } \mu\text{s}$, $\varphi = 0.6$, $\beta_1 = 2.6 \times 10^{-5}$, $\beta_2 = 1.0 \times 10^{-5}$, $\sigma = 1.6 \times 10^{-5}$, $T_1 = T_2 = T_s = 2.5 \text{ ns}$, $J_h = 7.1 \times 10^{16} \text{ s}^{-1}$, $J_0 = 1.6J_h$; $J = 0.11J_0$ 。

3.1 混沌及其同步

图2(a2)、(b2)是系统在未加载 $m(t)$ 时 MZ_1 输出的时间序列和功率谱。为便于比较,图2(a1)、(b1)还给出了单光电反馈时 SL_1 输出的时间序列和功率谱。从图2中可以看出,两种系统的输出均处于混沌状态。采用 G-

P 算法得到单光电反馈时 SL_1 输出的关联维数为 2.5, 而双光电反馈时 MZ_1 输出的关联维数达到了 3.8, 说明双光电反馈系统比单光电反馈系统输出的混沌波更为复杂; 双光电反馈系统输出的带宽为 43.05 GHz, 而单光电反馈系统输出带宽为 13.41 GHz, 前者为后者 3.2 倍。在这里, 带宽是包含各种频率成份光谱能量 80% 的频带宽度^[19]。 MZ_2 输出情况与 MZ_1 基本相同。上述结果表明, 双光电反馈系统相比于单光电反馈系统由于增加了一个自由度, 其动力学特性更为复杂, 频带更宽。

图 3 是 MZ_2 与 MZ_1 输出的互相关函数。从图 3 可知: 当 $\Delta t=0$ 时, 互相关函数的最大值为 0.996, 说明图 1 所示的双光电反馈系统能实现零时延的高质量混沌同步; 当 Δt 不为零时, 其同步特性明显变差。

3.2 参数失配对同步性能的影响

在激光混沌通信中, 收发两端振荡器的内参数由于制造原因往往会存在一定的差异, 即参数失配。参数失配将影响系统混沌同步的强度, 这直接关系到信息解码和通信安全。混沌保密通信的密钥是收发系统的结构及参数。就信息解码角度而言, 系统对参数失配的容忍性越好, 接收机就越容易与发射机实现良好同步, 信息解码质量也会越高, 但是, 随着系统对参数失配容忍性的增加, 窃密者就越容易构建非法接收机, 通信的安全性就会降低。在实际应用中, 如何合理兼顾取舍, 这正是混沌保密通信面临的关键问题之一。因此, 研究内参数失配对同步性能的影响有着重要意义。

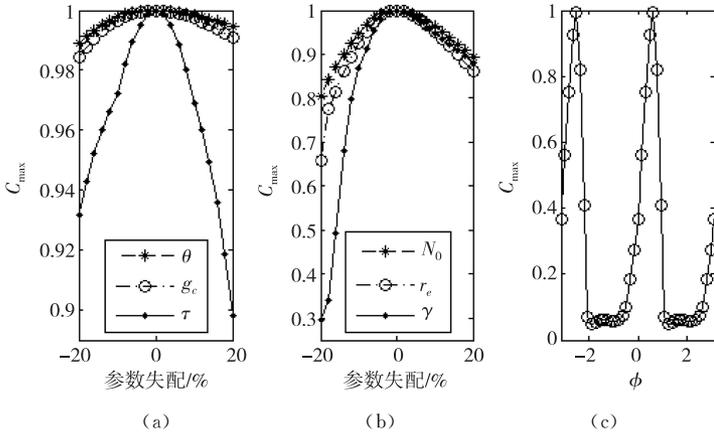


图 4 互相关函数最大值与内部参数失配的变化关系

为了进一步说明光注入强度对系统同步性能的影响, 图 5 给出了 $\beta_2 + \sigma = 2.6 \times 10^{-5}$ 条件下, 注入系数 σ 取不同值时 MZ_2 与 MZ_1 输出的互相关函数最大值随参数 g_c 、 θ 失配的变化关系。从图 5 中可以看出, 在 $\pm 20\%$ 失配范围内, 注入系数 σ 越大, 互相关函数的最大值也越大, 即系统对参数失配越不敏感。这是因为随着注入系数的增加, 系统进入注入锁定区, 因而对参数失配的容忍性更好。在实际应用中, 通过选择不同的注入系数 σ , 可改变系统对参数失配的敏感程度以适用于不同场合对解码质量和安全性的需要。

以上仅仅是考虑单个参数失配得到的结果。在实际应用中, 往往会同时遇到多个参数失配, 系统的同步性能可能会受到更大影响。因此, 应尽可能使系统收、发两端 SL 和 MZ 的参数保持一致, 以提高同步性能。

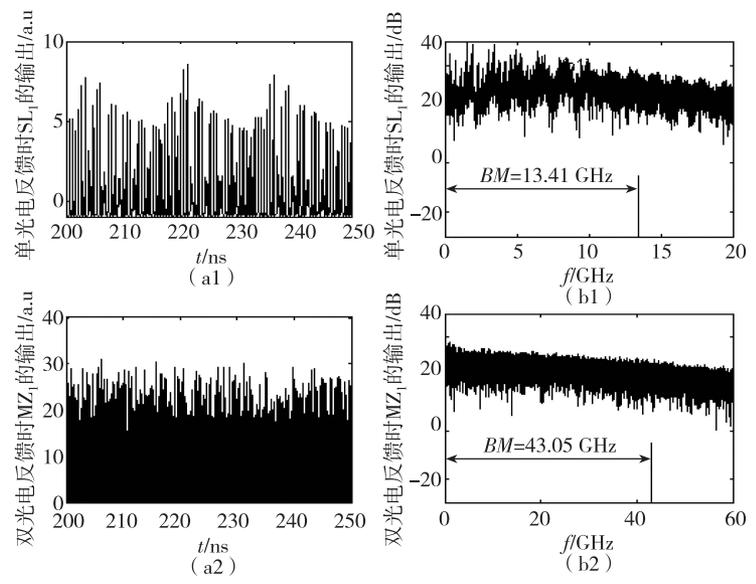


图 2 SL_1 , MZ_1 输出的时间序列(左列)及功率谱(右列)

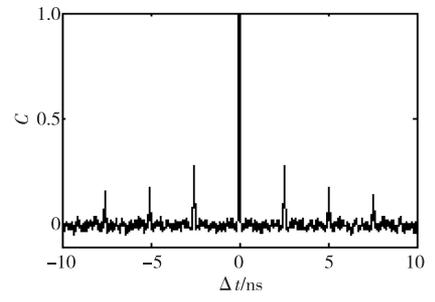


图 3 MZ_2 与 MZ_1 的互相关函数

图 4 是 MZ_2 与 MZ_1 输出的互相关函数最大值随系统内部参数失配的变化关系。从图 4(a)、(b)可知, 在 $\pm 20\%$ 失配范围内, θ 、 g_c 失配对应的值均在 0.98 以上, 表明系统对 θ 、 g_c 失配具有很高的容忍性; γ 失配对应的值是一条左低右高的不对称曲线, 说明系统对 γ 负失配更敏感, 同时系统对 γ_e 、 N_0 负失配也较为敏感; 与此相反, 当失配大于 10% 时, 系统对 τ 正失配更为敏感。从图 4(c)中可以看出, ϕ 对应值的周期为 π , 当 $\phi = -2.54$ 和 0.6 时, 互相关函数最大值均在 0.99 以上; 当 ϕ 稍偏离这两个值时, 同步质量急剧下降, 说明系统对 ϕ 失配也非常敏感。

3.3 信息的加载与解调

利用图 1 所示的系统, 可实现单向混沌通信。信息 $m(t)$ 的加载采用附加混沌调制 (ACM)。 $m(t)$ 通过光耦合器 C_1 被同时注入到收发两端, 避免信息加载对系统对称性的影响, 确保系统在加载信息后仍具有良好的同步质量。 $m(t)$ 是频率为 1 GHz 伪随机方波, 其调制系数为 5%。

图 6 给出的是信息的编码和解码情况。图 6(a) 为编码前的原始信息, 图 6(b)、(c) 分别为无参数失配时加载 $m(t)$ 后的混沌波和解码恢复的信息, 图 6(d)、(e) 分别为 γ 失配 1% 和 2% 时解码恢复的信息。从图 6(b) 可知, 信息 $m(t)$ 能很好地隐藏在混沌载波中。将图 6(d)、(e) 与 (c) 比较, 可以看出, 随着 γ 失配的增加, 解码恢复信息的质量变差。这主要是参数失配降低了系统的同步性能 (图 4)。因此, 参数失配对系统的通信性能有影响, 但在一定的参数失配范围内系统仍能成功恢复信息, 实现实时通信。

4 结论

本文提出了基于双光电反馈振荡器的单向混沌保密通信系统。数值分析了系统的同步特性及通信性能。研究表明, 双光电反馈系统与单光电反馈系统相比, 频带更宽, 动力学特性更为复杂, 有利于提高系统的通信容量和安全性; 在无参数失配时, 系统输出的相关系数达到 0.996, 能成功恢复编码的信息; 系统对 γ 负失配和 φ 失配非常敏感; 当接收端的反馈系数与注入系数之和保持不变时, 增加光注入强度可降低系统对参数失配的敏感程度; 参数失配对系统同步性能和通信质量有影响, 但在一定的失配范围内, 系统仍能成功恢复信息, 实现通信。

参考文献:

[1] Wang X Y, Yu H B. How to break MD5 and other hash functions[J]. Lecture Notes in Computer Science, 2005, 3494:19-35.
 [2] Wang X Y, Yin Y Q, Yu H B. Finding collisions in the full SHA-1[J]. Lecture Notes in Computer Science, 2005, 3621:17-36.
 [3] Klir E, Gross N, Kopelowitz E, et al. Public-channel cryptography based on mutual chaos pass filters[J]. Phys Rev E, 2006, 74(4):046201-046205.
 [4] Argyris A, Syvridis D, Larger L, et al. Chaos-based commu-

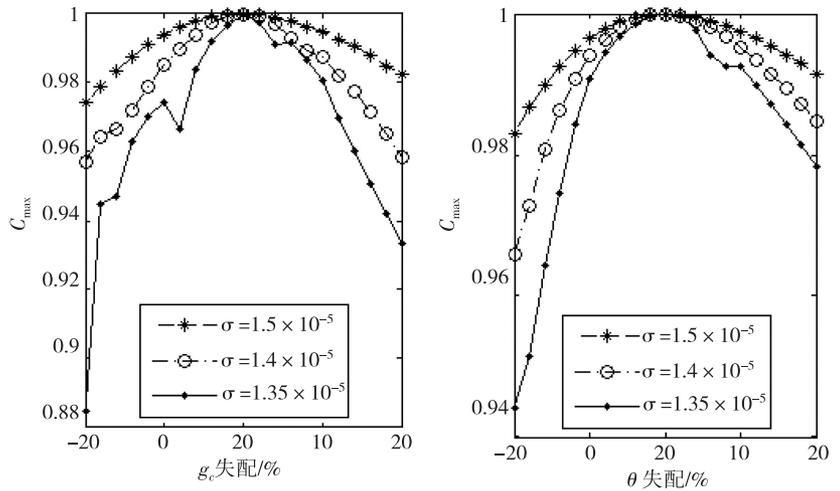


图 5 $\beta_2 + \sigma = 2.6 \times 10^{-5}$ 时不同注入系数下互相关函数最大值与 g_c 、 θ 失配的变化关系

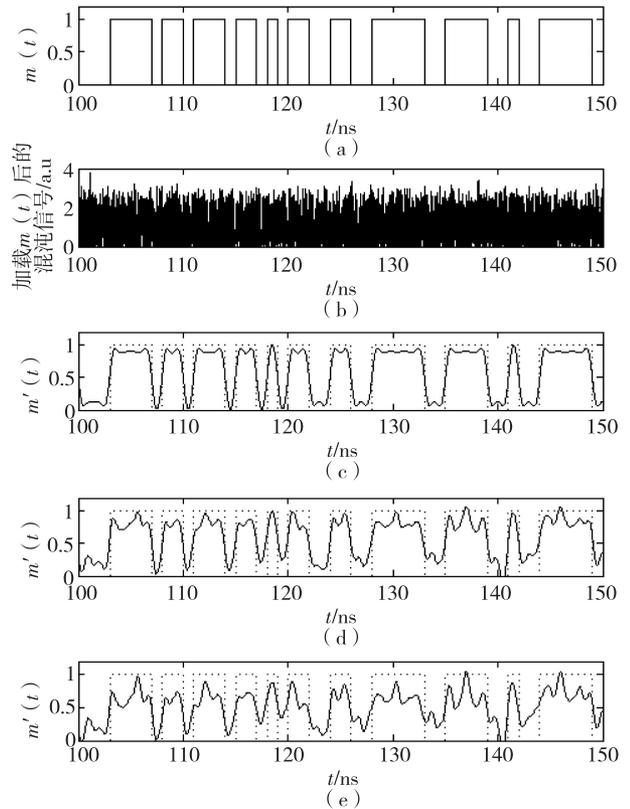


图 6 信息的编码和解码

nications at high bit rates using commercial fibre-optic links[J]. Nature, 2005, 438:343-346.
 [5] Mirasso C R, Mulet J, Masoller C. Chaos shift-keying encryption in chaotic external-cavity semiconductor lasers using a single-receiver scheme[J]. IEEE Photon Technol Lett, 2002, 14(4):456-458.
 [6] Ohtsubo J. Chaos synchronization and chaotic signal making in semiconductor laser with optical feedback [J]. IEEE J Quantum Electron, 2002, 38(9):1141-1154.
 [7] Chen H F, Liu J M. Open-loop chaotic synchronization of

- injection-locked semiconductor lasers with gigahertz range modulation[J]. *IEEE J Quantum Electron*, 2000, 36(1): 27-34.
- [8] 操良平, 夏光琼, 邓涛, 等. 基于非相干光反馈半导体激光器的双向混沌通信研究[J]. *物理学报*, 2010, 59(8): 5541-5546.
- Cao L P, Xia G Q, Deng T, et al. Bidirectional chaos communication based on semiconductor laser with incoherent optical feedback[J]. *Acta Phys sin*, 2010, 59(8): 5541-5546.
- [9] Zhou C, Lai C H, Extracting messages masked by chaotic signals of time-delay systems[J]. *Phys Rev E*, 1999, 60(1): 320-323.
- [10] Bezruchko B P, Karavaev A S, Ponomarenko V I, et al. Reconstruction of time-delay systems from chaotic time series [J]. *Phys Rev E*, 2001, 64(5): 056216-1-056216-6.
- [11] Zhao Q C, Wang Y C, Wang A B. Eavesdropping in chaotic optical communication using the feedback length of an external-cavity laser as a key[J]. *Appl Opt*, 2009, 48(18): 3515-3520.
- [12] Lee M W, Rees P, Shore K A, et al. Dynamical characterization of laser diode subject to double optical feedback for chaotic optical communications[J]. *IEEE Proc Optoelectron*, 2005, 152(2): 97-102.
- [13] 邓伟, 夏光琼, 吴正茂. 基于双光反馈垂直腔面发射激光器的双信道混沌同步通信[J]. *物理学报*, 2013, 62(16): 164209-1-164209-8
- Deng W, Xia G Q, Wu Z M. Dual-channel chaos synchronization and communication based on a vertical-cavity surface emitting laser with double optical feedback[J]. *Acta Phys Sin*, 2013, 62(16): 164209-1-164209-8.
- [14] 丁灵, 吴加贵, 夏光琼, 等. 双光反馈半导体激光混沌系统中外腔延时反馈特征的抑制[J]. *物理学报*, 2011, 60(1): 014210-1-014210-6.
- Ding L, Wu J G, Xia G Q, et al. Suppression of time delay signatures in a semiconductor laser with double optical feedback[J]. *Acta Phys. sin*, 2011, 60(1): 014210-1-014210-6.
- [15] Wu J G, Xia G Q, Wu Z M. Suppression of time delay signatures of chaotic output in a semiconductor laser with double optical feedback [J]. *Opt Express*, 2009, 17(22): 20124-20133.
- [16] 赵严峰. 双反馈半导体激光器的混沌特性研究[J]. *物理学报*, 2009, 58(9): 6058-6062.
- Zhao Y F. Chaos characteristics of the semiconductor laser with double external cavity optical feedback[J]. *Acta Phys Sin*, 2009, 58(9): 6058-6062.
- [17] Abarbanel H D I, Kennel M B, Illing L, et al. Synchronization and communication using semiconductor lasers with optoelectronic feedback[J]. *IEEE J Quantum Electron*, 2001, 37(10): 1301-1311.
- [18] Ngumdo R M, Colet P, Mirasso C. Electro-optic delay devices with double feedback[J]. *IEEE J Quantum Electron*, 2010, 46(10): 1436-1443.
- [19] Wang Y C, Zhang G W, Wang A B. Enhancement of chaotic carrier bandwidth in laser diode transmitter utilizing external light injection[J]. *Opt Commun*, 2007, 277(1): 156-160.

Unidirectional Chaotic Synchronization Communication Based on Oscillator with Double Optoelectronic Delay Feedback

CAO Liangping¹, DONG Xiaoyun², WANG Zeyu¹, WANG Chongyu¹

(1. College of Education Science, Chongqing Normal University, Chongqing 401331;

2. Elementary Education College, Chongqing Normal University, Chongqing 400700, China)

Abstract: Au unidirectional chaotic synchronization communication system based on oscillator with double optoelectronic feedback was constructed. Its synchronization characteristics and communication performances are numerically investigated. The results show that the chaotic outputs of such a system become more complex and have larger bandwidth, which is helpful to improve the communication capacity, the system security as well. When the parameters are mismatched, good-quality chaos synchronization and simultaneous unidirectional transmission can be achieved; when mismatched, the synchronization quality and communication performance are affected to a certain extent, but the system can still realize chaos communication within a range of mismatched parameters

Key words: chaos synchronization; chaos communication; double optoelectronic feedback; semiconductor laser; Mach-Zehnder modulator