

反馈强度调制增强混沌光通信的保密性^{*}

郭东明 杨玲珍 王安帮 张秀娟 王云才[†]

(太原理工大学物理系, 太原 030024)

(2008 年 12 月 31 日收到 2009 年 4 月 4 日收到修改稿)

注入锁定式光混沌同步通信系统对收发机的参数失配有较大的容忍度, 这在一定程度上降低了信息的安全性. 提出采用反馈强度的调制来提高系统的保密性. 数值模拟分析了调制前后系统提取信号质量的变化, 以及收发机调制的速率失谐、延时对提取信号质量的影响. 研究发现: 仅在发射机增加反馈强度调制后, 同步性恶化、误码率增大两个数量级, 无法提取信号. 而在接收机引入相同的调制后, 系统同步性及误码率得到恢复. 此外, 收发机的反馈强度调制速率失谐和延时范围分别在 ± 5 MHz 和 ± 0.1 倍调制周期时, 信息提取质量较高. 反馈强度调制能够有效地增强传统混沌通信系统的保密性.

关键词: 反馈强度, 调制, 混沌通信, 保密

PACC: 4230Q, 4265T, 4255P

1. 引言

混沌光以其高维宽带、不可预测性和复杂的非线性动力学特性等优点成为光保密通信的理想载波^[1]. 混沌保密通信是将待传输信号用某种方式加载到发射机混沌载波中进行传输, 当接收机与发射机内部参数匹配时, 实现混沌同步, 达到混沌同步的接收机具有独特的滤波特性^[2], 基于此方可恢复传输信号, 即混沌激光通信是以发射机的内部参数作为密钥的物理层加密通信技术. 自混沌保密光通信提出后, 受到广泛的研究关注, 并相继提出和验证了不同结构的同步系统及信息加载方式^[3-11]. 2005 年 Argyris 等^[12]在雅典利用商用光通信网络实现了 1 Gbit/s 信号的低误码率混沌光保密通信, 传输距离达 120 km, 迈出了实用化的重要一步. 然而研究发现^[13], 在强注入锁定同步情况下, 系统对接收机与发射机内部参数失配有较大的容忍性, 这在一定程度上降低了信息的安全性. 因此, 单纯依靠发射机内部参数的保密通信的信息安全性仍然有待提高, 迫切需要进一步增加其保密性.

对于传统的光反馈半导体激光器作为发射机的混沌保密通信, 同步系统建立后, 系统的工作参数(包括激光器工作电流、反馈相位、反馈强度)都是固

定不变的. 这无疑给了破解者机会来推知系统的关键参数, 从而降低了系统的安全性. 文献 [14] 通过增加一个外腔的方式, 得到了较复杂的混沌输出. 可见增加工作参数的可控量能够改变原有通信系统单一参数下的同步性, 使得窃取者在未知发射机工作参数变化的情况下无法获得有用的传输信号, 从而增加系统的保密性. 2008 年 Bogris 等^[15]数值模拟了在短腔反馈条件下, 用反馈相位作为混沌保密通信系统密钥的可行性, 并从破解者角度分析了相位调制后, 不同信息格式和码率下信息提取的误码率随注入反馈比的关系. 然而在实际应用中, 腔长会随着温度的变化而改变, 相位调制受环境温度的影响较大, 不易实现. 本文提出利用对反馈强度的调制来控制发射机混沌的输出, 接收机通过反馈强度同步调制的方式来实现系统混沌同步及信息的有效提取. 数值模拟分析并验证了通过反馈强度调制增强系统安全的可行性, 并研究了此种方式下调制速率失谐和延时对系统提取信号质量的影响.

2. 反馈强度同步调制模型及方程

反馈强度同步调制模型如图 1 所示, 发射机由一个带反馈的半导体激光器(中心波长为 1550 nm 的分布式反馈激光器)中插入强度调制器构成, 强度

^{*} 国家自然科学基金(批准号: 60777041)和山西省国际科技合作计划和山西省青年科技研究基金(批准号: 200821008)资助的课题.

[†] 通讯联系人. E-mail: wangyc@tyut.edu.cn

$$\rho = \frac{[P_T(t) - P_T(t)] \mathbb{I} [P_R(t + \Delta t) - P_R(t + \Delta t)]}{\sqrt{|P_T(t) - P_T(t)|^2} \sqrt{|P_R(t + \Delta t) - P_R(t + \Delta t)|^2}}. \quad (4)$$

3. 模拟结果及分析

3.1. 反馈强度对同步及信号提取质量的影响

图 2 为闭环结构中发射机与接收机不同反馈系数对应的同步相关系数图. 横坐标表示发射机反馈系数 κ_T , 纵坐标表示接收机反馈系数 κ_R , 图中灰度的深浅代表不同的相关系数, 颜色越深表示相关系数越小, 同步性越差. 从图 2 可以看出, 只有在 $\kappa_T \approx \kappa_R$ 时, 系统的同步性较高(相关系数在 0.95 以上).

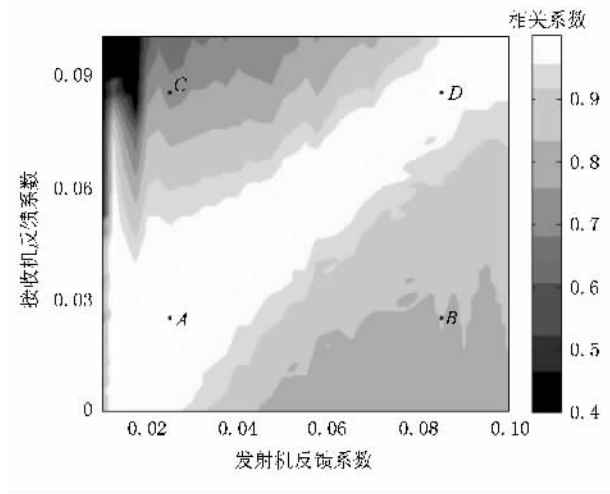


图 2 发射机与接收机不同反馈系数对应的同步相关系数图

选取图 2 中同步性较好的状态 A (0.025, 0.025) 作为参考, 比较反馈强度的变化对同步的影响. 括号中分别为发射机与接收机的反馈系数. A 的相关系数为 99.96%, 若接收机反馈强度保持不变, 随着发射机反馈强度的增大系统同步性下降. 同样, 若发射机反馈强度保持不变, 随着接收机反馈强度的增大同步性也是下降的. 只有发射机与接收机反馈强度保持同步变化时, 才能维持较好的同步性. 因此, 调制的选取原则上是使得反馈强度变化能够引起较大的同步性差异. 若变化范围较小就达不到增强保密的目的. 如图 2 中 B (0.085, 0.025) 和 C (0.025, 0.085) 同步性较差, 而同步调制后相关性恢复, D (0.085, 0.085) 相关系数为 99.76%.

下面从信息提取的角度来分析发射机反馈强度在动态调制前后误码率的变化情况. 模拟中选用电流键控的方式, 加载信息调制幅度为 0.05, 速率为 2.5 Gbit/s 非归零码进行传输. 图 3 为发射机反馈系数调制前后, 接收机提取信号误码率随接收机反馈

系数的变化曲线. 图 4 为不同形式的反馈强度调制下, 解调出信号的时间序列和对应的眼图. 图 3 中方块线表示发射机反馈强度未进行调制(即传统同步方式), 反馈系数为 0.025, 系统同步性较好, 相关系数最高为 99.96%, 解调出信号的时间序列与眼图分别对应于图 4(a) 和 (b), 误码率最小约为 0.001, 可见此时有较好的信息提取质量. 图 3 中圆点线表示发射机反馈强度采用 1 GHz 方波信号来调制, 调制系数 θ 为 2.4, 即反馈系数在 0.025 与 0.085 间进行转换. 可以看出调制后系统同步性变差, 误码率增高至 0.1 以上, 与未调制时相比增大了两个数量级. 图 4(c) 和 (d) 对应发射机调制后接收机反馈为 0.025 时提取信号的时间序列和眼图, 此时的误码率高达 0.2, 已不能有效地提取信号. 通过比较发现, 发射机反馈强度调制可以有效地破坏原系统的同步性, 使信息传输误码率增高. 图 4(e) 和 (f) 表示接收机和发射机采用同样的调制后信息提取的时间序列和眼图, 可以看出接收机采用同步调制后, 系统的同步性能恢复至较高水平, 误码率约为 0.004. 这证明了通过对反馈强度的调制能够控制系统的同步性及信息提取误码率, 从而进一步增强混沌保密通信系统的安全性.

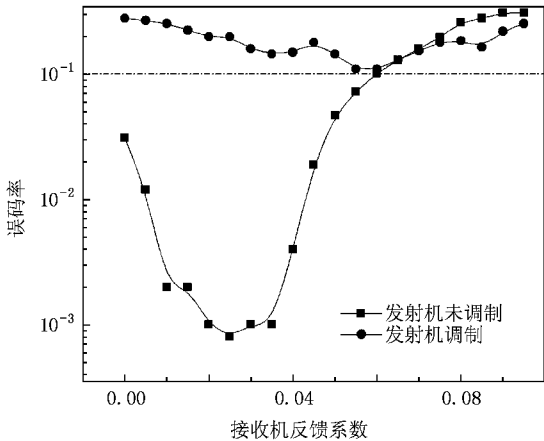


图 3 发射机反馈强度调制前后接收机提取信号误码率的变化曲线

3.2. 反馈强度调制速率失谐及延时的影响

反馈强度调制的引入, 必然存在调制速率失谐及调制延时的影响, 系统同步性和信息恢复质量对这两个量的敏感程度又进一步决定了此种调制方式增强保密性的能力.

图 5 为发射机反馈强度调制速率为 1 GHz 时,

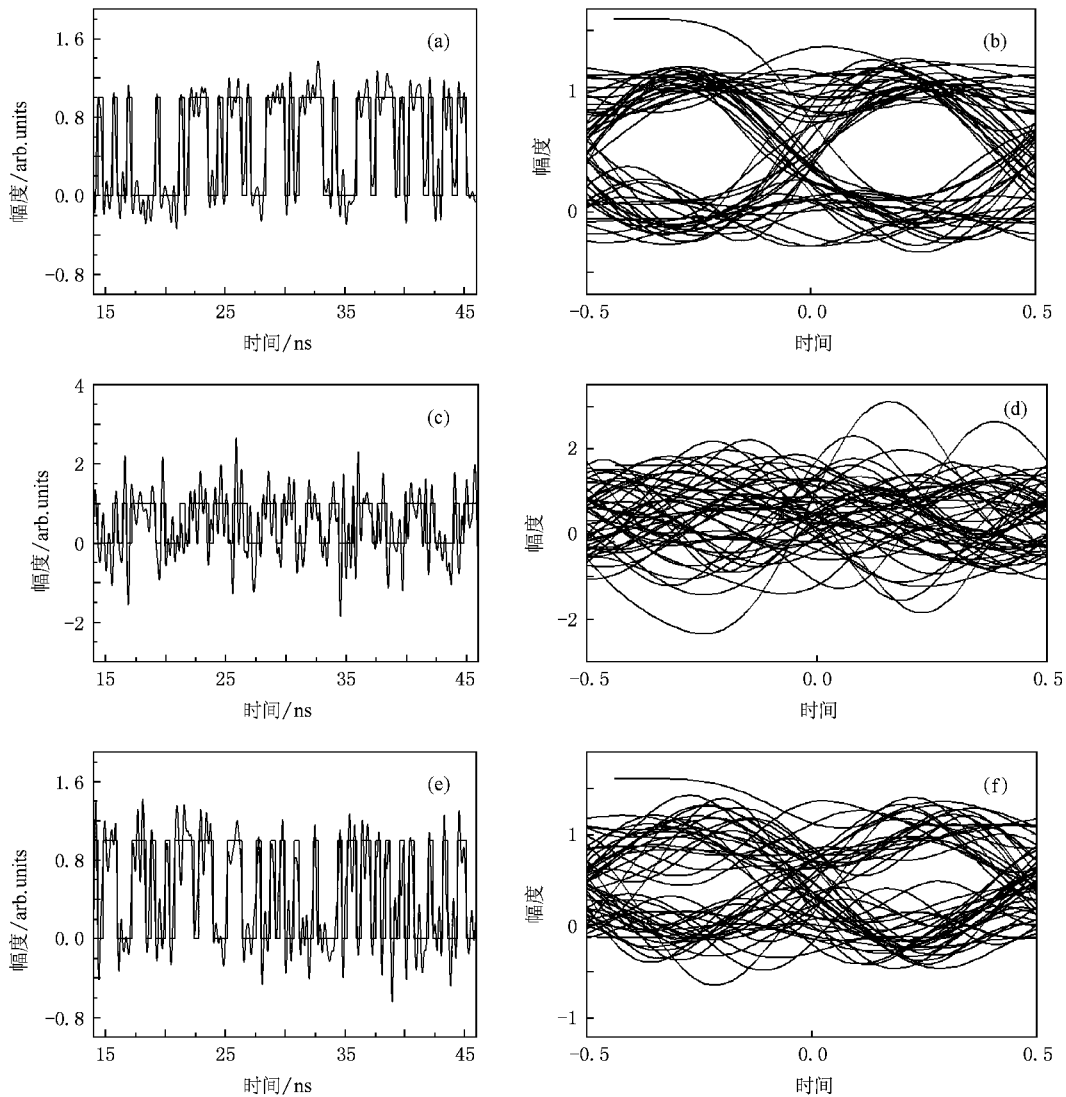


图 4 反馈强度调制对信息提取的影响 (a)(c)(e)为信息提取时间序列 (b)(d)(f)为对应的眼图

接收机反馈调制速率失谐 Δf 与误码率的关系. 从图 5 可以看出, 只有调制速率失谐接近 0 GHz 时信息提取误码率最低. 内插图给出反馈调制速率失谐范围为 ± 5 MHz 时, 信息提取的误码率小于 0.1, 可见此种调制方式对调制速率失谐的容忍度较差. 对于传统同步系统而言, 发射机和接收机的同步与注入延时无关, 而反馈强度经过调制后混沌的输出也是调制信号的函数, 因此我们考虑了发射机与接收机间延时与系统误码率的关系. 模拟中采用的反馈强度调制信号为周期信号, 因此延时与误码率有一定的周期性, 周期为调制信号的周期, 如内插图中所示为 1 GHz 调制信号, 误码率与延时的关系, 周期为 1 ns. 图 6 为延时在 0.2 ns 范围内三种调制速率下, 延时量 $\Delta\tau$ 与系统信息提取误码率的关系. 比较得

出, 只有延时量 $\Delta\tau$ 为 0 ns 时, 误码率最低, 随着延

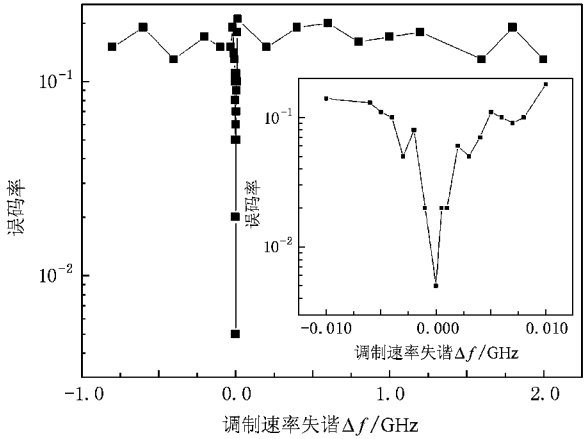


图 5 调制速率失谐 Δf 与误码率的关系

时量的增加,信息提取误码率增大,且调制速率越快,信息提取质量下降越快.同时,延时量范围在 ± 0.1 倍的调制周期时,误码率小于0.1.

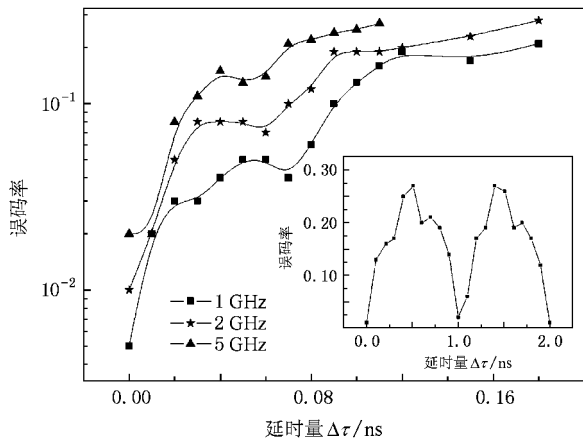


图6 三种调制速率下延时量 $\Delta\tau$ 与误码率的关系

从上述分析中可以得出,通过发射机系统反馈强度调制的引入,致使破解者在考虑混沌保密通信系统内部参数匹配的同时,又增加了反馈强度调制带来的调制速率失谐和调制延时的影响,还有调制系数、调制信号类型等其他因素,大大增加了破解难度,使通信系统的安全性得到提高.

4. 讨 论

在混沌保密通信中,信号的有效传输恢复,不仅

与系统本身内部参数匹配有关,信息的加载方式、加载幅度和滤波器的选择等因素也对最终提取质量有所影响.由于计算限制,这里仅采用电流键控方式对2.5 Gbit/s 的非归零码进行了研究,码元个数为1225,旨在定性地描述反馈强度调制对混沌通信系统信息提取性能的影响,所选参数对应的信息恢复误码率在 10^{-3} 量级,与文献[12]中所述2.5 Gbit/s 信号误码率为同一量级.文献[4]详细分析比较了不同加载方式下系统的误码率,可见通过对特定码率信号的加载方式、调制幅度、滤波器等参数的优化选择,能够进一步降低该系统传输的误码率,实现高质量通信.

5. 结 论

本文提出利用对反馈强度的调制实现混沌同步及信息的传输.通过理论模拟论证了反馈强度调制能够提高原混沌通信系统的保密性,并分析了反馈强度调制速率失谐和延时对系统信息提取质量的影响.结果表明,发射机反馈强度调制后,能够有效破坏原系统的同步性,增大误码率.接收机采用反馈强度同步调制后,又可恢复系统的同步.同时,只有调制速率失谐和延时量在一定范围内才能达到较好的信息提取效果.这一调制方式的提出对以后通信系统安全性的提高具有重要的指导意义.

[1] Vanwiggeren G D ,Roy R 1998 *Science* **279** 1198

[2] Wang Y C ,Li Y L ,Wang A B ,Wang B J ,Zhang G W ,Guo P 2007 *Acta Phys. Sin.* **56** 4686 (in Chinese) [王云才、李艳丽、王安帮、王冰洁、张耕玮、郭 萍 2007 物理学报 **56** 4686]

[3] Heil T ,Mulet J ,Fischer I ,Mirasso C R ,Peil M ,Colet P ,Elsasser W 2002 *IEEE J. Quantum Electron.* **38** 1162

[4] Liu J M ,Chen H F ,Tang S 2002 *IEEE J. Quantum Electron.* **38** 1184

[5] Argyris A ,Kanakidis D ,Bogris A ,Syvridis D 2004 *IEEE J. Select. Topics Quantum Electron.* **10** 927

[6] Yan S L 2005 *Acta Phys. Sin.* **54** 2000 (in Chinese) [颜森林 2005 物理学报 **54** 2000]

[7] Wu J G ,Wu Z M ,Lin X D ,Zhang Y ,Zhong D Z ,Xia G Q 2005 *Acta Phys. Sin.* **54** 4169 (in Chinese) [吴加贵、吴正茂、林晓东、张 毅、钟东洲、夏光琼 2005 物理学报 **54** 4169]

[8] Annovazzi-Lodi V ,Benedetti S ,Merlo S ,Norgia M 2005 *IEEE Photon. Technol. Lett.* **17** 1995

[9] Lee M W ,Rees P ,Shore K A ,Ortin S ,Pesquera L ,Valle A 2005 *Proc. IEEE Optoelectron.* **152** 97

[10] Tronciu V Z ,Ermakov I V ,Colet P ,Mirasso C R 2008 *Opt. Commun.* **281** 4747

[11] Liu H J ,Feng J C 2009 *Acta Phys. Sin.* **58** 1484 (in Chinese) [刘慧杰、冯久超 2009 物理学报 **58** 1484]

[12] Argyris A ,Syvridis D ,Larger L ,Annovazzi-Lodi V ,Colet P ,Fischer I ,Garcia-Ojalvo J ,Mirasso C R ,Pesquera L ,Shore K A 2005 *Nature* **437** 343

[13] Ohtsubo J 2002 *IEEE J. Quantum Electron.* **38** 1141

[14] Lee M W ,Larger L ,Udaltsov V ,Genin E ,Goedgebuer J P 2004 *Opt. Lett.* **29** 325

[15] Bogris A ,Rizomiliotis P ,Chlouverakis K E ,Argyris A ,Syvridis D 2008 *IEEE J. Quantum Electron.* **44** 119

Modulation of feedback strength to enhance the security of chaos optical communication system^{*}

Guo Dong-Ming Yang Ling-Zhen Wang An-Bang Zhang Xiu-Juan Wang Yun-Cai[†]

(*Department of Physics ,Taiyuan University of Technology ,Taiyuan 030024 ,China*)

(Received 31 December 2008 ; revised manuscript received 4 April 2009)

Abstract

There is a high tolerance on parameters mismatch between transmitter and receiver in the chaos communication system based on injection locking synchronization ,so to a certain extent ,the information security has been reduced. We propose the synchronous modulation of feedback strength to improve the system security. The change of signal extraction quality after modulation is studied numerically and the effects of modulation rate detuning and modulation delay time on signal extraction are analyzed too. The research results indicate that the synchronization of the original system is destroyed and the bit error rate increases by two orders of magnitude when the transmitter feedback strength is modulated. The information can not be recovered unless the receiver uses the same modulation. Furthermore ,the results also show that high quality information could be obtained when rate detuning and delay time are in the range of ± 5 MHz and ± 0.1 times the modulation cycles , respectively. All of these prove that modulating the feedback strength can enhance the security of chaos communication efficiently.

Keywords : feedback strength , modulation , chaos communication , security

PACC : 4230Q , 4265T , 4255P

^{*} Project supported by the National Natural Science Foundation of China (Grant No. 60777041) , the International Science and Technology Cooperation Program of Shanxi Province ,China and the Natural Science Foundation for Young Scientists of Shanxi Province , China (Grant No. 200821008).

[†] Correspondence author. E-mail : wangyc@tyut.edu.cn