第 17 卷 第 11 期 光 学 学 报 Vol. 17, No. 11
1997 年 11 月 ACTA OPTICA SINICA November, 1997

光学双稳系统混沌驱动保密通讯原理研究

刘金刚[1, 2] 沈 柯[2] 周立伟[1]

1, 北京理工大学工程光学系, 北京 100081
2, 长春光机学院理学分院, 长春 130022

摘 要 根据声光双稳系统混沌驱动下的动力学行为, 提出利用系统的相位特性实现信息的混沌加密, 并且由接收端混沌驱动产生的混沌信号完成信息提取的原理。发现在较大的噪声覆盖下仍然可以实现信息的安全传送, 由于信息解密不需要与载波完全同步的混沌信号而只利用传输信号与接收端被驱动系统输出信号的相位关系, 因此这种方法具有实际应用价值。

关键词 光学双稳系统, 混沌, 保密通讯。

自从 Pecora 和 Carroll[1~3] 提出混沌同步的概念以来, 混沌同步及随之产生的利用混沌同步实现保密通讯的研究[4~10, 12~14] 得以展开。特别是混沌保密通讯的研究应用前景广阔, 因而引起不少研究者的注意[9~14]。其中 Parlitz 等[9] 提出一种基于混沌同步的混沌保密通讯原理, 他利用 Logistic 映射产生的混沌研究了通讯信号的加解密效果, 编码方式为混沌载波与和二进制 0, 1 相对应的 1, – 1 量相乘作为传输信号, 解码时使用完全同步的混沌信号与之做码位区间相关运算, 其最大的优点就是利用相关处理使得抗噪声能力强, 但必须实现混沌的实时同步。其他学者也基本上按照这种以混沌同步为前提的办法来研究。其中大部分基于信息与混沌信号直接相加传送并将其作为接收端同步驱动信号(因而信息必须是小信号) 的方法抗噪声能力都较弱, 而对于 Pyragas 同步化方法实现混沌保密通讯则更不希望有噪声[10]。

最近, Oksasoglu 等人利用 Chua 电路的混沌及接收与解调电路的特殊设计, 提出线性反变换混沌无同步保密通讯原理的可能性[14], 其信息的恢复使用线性逆反电路及混沌电路的另外一个信号, 因而是双通道信号传输。他研究了传输信息是正弦模拟量的情况, 但没有考虑噪声的影响。从混沌同步化本身讲噪声的存在将给同步的实现带来困难, 但是近来发现无噪声或微小噪声下的混沌保密通讯也有可能被细心的截获者破译[13], 因此, 从这种意义上看, 抗噪声的混沌保密通讯更安全, 因而会更实用。

本文提出利用声光双稳系统的相位特征实现混沌保密通讯的原理。即以声光双稳混沌系统产生的混沌信号 $x(t)$ 为基础, 来驱动两个声光调制器, 在发射端开环的声光调制器上进行信息调制产生信号 $y(t)$, 在接收端相同特性的调制器上产生解调信号 $z(t)$, 根据信息 $s(t)$ 导致的 $y(t)$ 和 $z(t)$ 的相位相关关系把 $s(t)$ 提取出来。其特点是只有一个混沌系统, 无需传统的混沌同步的实现, 这一点与文献[14] 类似, 但解调过程无需逆反电路, 抗噪声能力强, 信号

收稿日期: 1996 年 7 月 18 日; 收到修改稿日期: 1997 年 4 月 16 日

载波可为光信号(也可以变为电信号)。这些特点为光学保密通讯提供了应用基础。由于已有的无同步混沌保密通讯研究多使用多变量系统，其方法不适于本文的单变量的声光双稳系统，但本文提出的这种方法却可适用于其他多变量系统。目前，此项研究国内外未见报道。

1 声光双稳系统混沌调制与相位特征

布拉格(Bragg)型声光双稳系统动力学方程为[15]:

$$\mathrm{d}w(t)/\mathrm{d}t + w(t) = \pi\{A - \lambda \sin^2[w(t-\tau) - b]\} \tag{1}$$

式中 $w(t)$ 为系统状态变量; A 和 b 为系统参数，分别与放大器和驱动源的偏置有关; λ 与入射光强及放大器放大倍数有关，是决定系统运行状态的分叉参数; t 和 τ 是以系统响应时间为单位的时间变量及系统延时时间。对于长延时($\tau \gg 1$)情况，(1)式是典型的混沌系统，在某些参数范围$\{(A, \lambda, b) \mid (A, \lambda, b) \in U_{\mathrm{chaos}}, U_{\mathrm{chaos}} \subset R^3\}$及一定的初始条件下求解，将得到混沌解 $w(t) \in D$, D 为(1)式的混沌解空间，U_{chaos} 为混沌参数空间。现构造一套这样的系统，使它成为开环声光调制器，其中被调制的输入变量为(1)式中输出变量 $w(t-\tau) = x(t)$(即以 $x(t)$ 驱动调制器)，由于开环的声光调制器与闭环的声光双稳系统的差别只在于方程右边的变量由谁提供，因此不难推出开环的声光调制器的变量输出满足:

$$\mathrm{d}y(t)/\mathrm{d}t + y(t) = \pi\{A_1 - \lambda_1 \sin^2[x(t) - b_1]\} \tag{2}$$

若二系统中(1)和(2)式的参数完全相同 $(A_1, \lambda_1, b_1) = (A, \lambda, b)$，则显然 $y(t)$ 与 $w(t)$ 将保持同步的混沌。若参数差别较大，则 $y(t)$ 与 $w(t)$ 会大不相同(因而也与 $x(t) = w(t-\tau)$ 不同)。可以记 $y(t) \in D_{12}$, D_{12} 为(2)式在 $x(t) \in D$ 驱动下的解空间。若 $y(t)$ 为混沌解，记其混沌解空间为 $D_1 \subset D_{12}$，满足 $y(t) \in D_1$ 的参数空间记为 U_1。由于混沌系统驱动周期系统也可以产生混沌解，因此 $V = (U_1 - U_1 \cap U_{\mathrm{chaos}}) \neq \phi$。记 $V_{\mathrm{chaos}} = U_1 \cap U_{\mathrm{chaos}}$，且记子空间 $D_2 \subset D_1$ 为(2)式的 $\forall (A_1, \lambda_1, b_1) \in V_{\mathrm{chaos}}$ 的 $y(t)$ 解空间。

对于 D_2 中的解，可以先选择性地研究两类极端情况: 一类的相位与 $w(t)$ 比较接近而且波形有一定的相似性; 另一类的相位与 $w(t)$ 的相位相差较大并且因非线性变换导致了二者的波形无关，将这两类的参数空间及解空间分别记为 $V_1 \subset V_{\mathrm{chaos}}$ 和 $V_2 \subset V_{\mathrm{chaos}}$ 及 $y^*(t) \in D_{21}$ 和 $y(t) \in D_{22}$。图1所示为$(A, \lambda, b) \in U_{\mathrm{chaos}}$ 的轨道 $w(t) \in D$, $(A_1, \lambda_1, b_1 = b) \in V_1$ 的轨道 $y^*(t) \in D_{21}$ 及$(A_1, \lambda_1, b_1) \in V_2$ 的 $y(t) \in D_{22}$。由图1可见，$y^*(t)$ 与 $w(t)$ 尽管不相同，但形状和趋势是相似的，而 $y(t)$ 与 $w(t)$ 却毫不相似。这是因为处于不稳定状态的双稳系统开环后所成为的调制器，对信号的非线性调制作用会因它们相位的相关性质而导致响应信号与驱动信号是否会有一定的相似性。图中参数 $\tau = 10$: 图1(a): $(A = -0.25, \lambda = 1.2, b = 0.4\pi)$; 图1(b): $(A_1 = -0.7, \lambda_1 = 1.7, b_1 = 0.4\pi)$; 图1(c): $(A_1 = -0.7, \lambda_1 = 1.7, b_1 = 0.65\pi)$。

由于后面保密通讯要同时使用 $w(t)$ 和 $y(t)$，从安全性考虑应不使用 $y^*(t)$ 而选用 $y(t) \in D_{22}$，因此以下研究将主要针对 $(A_1, \lambda_1, b_1) \in V_2$ 且 (A_1, λ_1, b_1) 与 (A, λ, b) 有较大差别的情况。如果在系统(2)的右边输入变量中加入一调制项 $S = s\pi/2$，则它相当于对相位进行调制，不同的调制参数导致不同的相位改变，(2)式写为:

$$\mathrm{d}y(t)/\mathrm{d}t + y(t) = \pi\{A_1 - \lambda_1 \sin^2[x(t) - b_1 + \pi s(t)/2]\} \tag{3}$$

在一定的参数范围 $\{[A_1, \lambda_1, b_1 - \pi s(t)/2] \mid [A_1, \lambda_1, b_1 - \pi s(t)/2] \in V_2\}$ 内且 $x(t) = w(t-\tau) \in D$，若令其他条件不变而只是分别考虑 $s(t) = 0$ 及 $s(t) = 1$，则二种情况下由相同的 $x(t)$ 驱动所得的 $y(t)$ 保持反相混沌的特点，而它们与 $x(t+\tau) = w(t)$ 又无相似之处。图2所示给

出 $s(t) = 1$ 及 $s(t)$ 在 0, 1 间以 $T = 12\tau$ 为周期切换时的变量 $y(t)$ 波形。对比图 1(c) 和图 2 可见, 在 T 的大部分区间内, 同相和反相的特征都表现出来, 可把混沌信号作为信息 $s(t)$ 的载波。

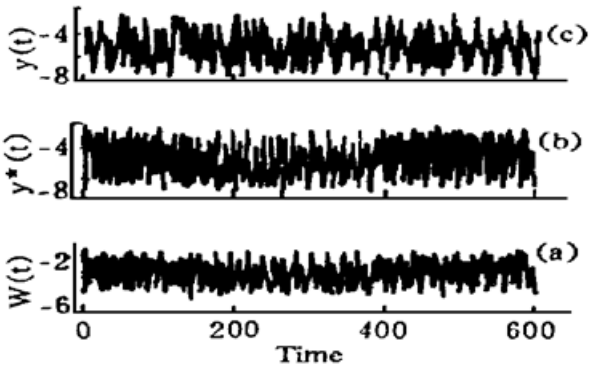

Fig. 1 Waveforms of AOM driven by chaotic signal. (a) $w(t) \in D$; (b) $y^*(t) \in D_{21}$; (c) $y(t) \in D_{22}$

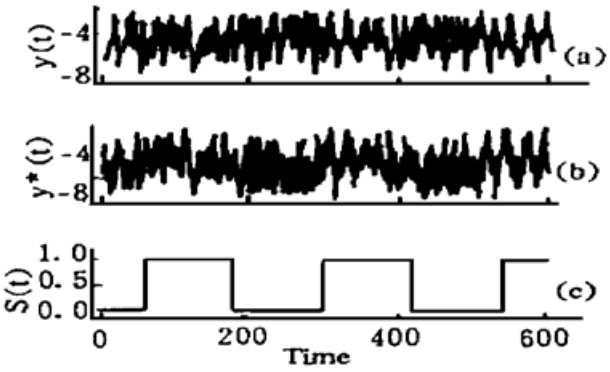

Fig. 2 Waveforms of the system modulated with different parameters. where: (a) $s(t) = 1$; (b) waveform when $s(t)$ switches between 0 and 1; (c) $s(t)$

2　信号调制与解调

总的原理图见图 3, 混沌驱动系统 driver 产生混沌信号 $w(t)$, 以 $x(t) = w(t - \tau)$ 驱动另外的一个参数不同的声光调制器(由混沌系统开环而成), 其作用是产生载波并进行信息 $s(t)$ 的调制, 已调制信号 $y(t)$ 和混沌驱动信号 $x(t)$ 放大后为 $x''(t)$ 和 $y''(t)$, 经双通道传输到达接收端。接收器得到的信号 $x'(t)$ 和 $y'(t)$ 等量放大后变成与发射端基本相同, 即 $x(t)$ 和 $y(t)$。用驱动信号 $x(t)$ 驱动与信号调制端相同的声光调制系统, 使产生的新的混沌信号 $z(t)$ 作为解调信号(它记录了无信息即 $s(t) = 0$ 时应该出现的传输信号的特征), 然后把 $y(t)$ 和 $z(t)$ 送入相关运算器 C 中, 在位码区间作相关运算, 实现信息 $s(t)$ 的恢复。图中, 驱动系统 driver 是熟知的经典声光双稳混沌系统, 放大器和加法器以简写 Am. 及 Ad. 表示, 后面的数字相同时表明它们的特性参数是完全相同的。Am. m 是信号调制放大器, 若 $s(t)$ 是二进制 0, 1 信号, 则其放大倍率为 $p/2$。Am. r 是接收信号放大器, 它使所得到的传输信号恢复为原来的幅度。

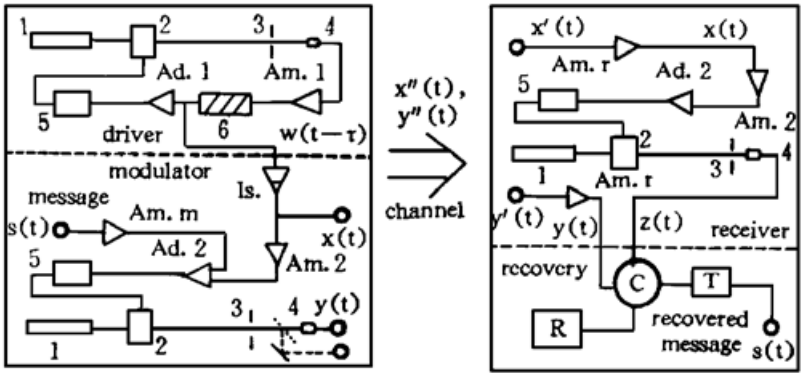

Fig. 3 Block diagram of masking and recovering message device. where: 1. He-Ne Laser, 2. AOM, 3. diaphragm, 4. detector, 5. ultrasonic driver, 6. delay line. Is. isolator Am. amplifier Ad. adder Am. m. modulating amplifier Am. r. receiving amplifier C. correlation calculator R. correcting device T. translator of message

值得注意的是校正装置 R, 它使每段相关运算区间刚好与信号位码区间重合, 这可以通过在初始发射的固定的{01010101…} 序列时间内进行有效的调整。T 是把相关运算所得的高

低不同的阶梯解释为 0, 1 数字码的装置, 它的上下触发阈值 H_u 及 H_b 的选择适当时, 可以排除因发射时所加噪声及处理中产生的小偏差而可能带来的信息恢复时出现的误码率, 这一点将在下面看到。以上是简单的原理性描述, 下面给出数值例子。

把宽度为 T 的方波形式的数字信号 $s(t)$ 加入方程(3), 则 $y(t)$ 将携带着信息 $s(t)$。信号 $x(t)$, $y(t)$ 同时发射出去, 为防止信息被重构者窃取(见下节), 把 $y(t)$ 加入噪声后发射, 到达接收端被恢复为原来的幅度。以 $x(t)$ 驱动与(2)相同的系统

$$\mathrm{d}z(t)/\mathrm{d}t + z(t) = \pi\{A_1 - \lambda_1 \sin^2[x(t) - b_1]\} \tag{4}$$

将得到与不加调制和噪声的 $y(t)$ 近似相同的 $z(t)$。现在 $y(t)$ 和 $z(t)$ 的差别只在于外加噪声及相位在 $s(t) = 1$ 时反相(由于是混沌系统, 系统响应时间远小于延时 τ, 而混沌加密时显然应有 $\tau < T$, 所以在 T 时间内的很长一段中, 反相的特征都能表现出来)。因此做相关分析便可以把信息提取出来。作法是在每段 T 的间隔内(T 称为位码长度)做

$$C(t' + iT) = C_i = \int_0^T y(t'' + iT) + e(t'' + iT)]z(t'' + iT)\,\mathrm{d}t'' \tag{5}$$

式中 $e(t)$ 为发射时加入的噪声, $0 < t' < T$, C_i 为第 i 个位码区间内信号 $y(t)$ 与 $z(t)$ 的相关量。把 C_i 与经过标准信息校正过的触发器上下触发阈值 H_u、H_b 比较即可得到信息 $s_r(t)$ 的恢复。由于混沌信号的无规律性及噪声的影响, 对同样的 0 或 1 信息在不同码段得到的 $C_i(t)$ 将有所不同, 这时就需要 H_u 尽可能小而 H_b 尽可能大, 且满足 $H_u > H_b$, 而允许加入的最大噪声也就由初始标准信息传送时统计的上下限 $\max(C_i^1)$ 及 $\min(C_j^0)$ 与 H_u 及 H_b 的大小所决定, 其中上标是对应的信息码值。由于触发器阈值差应有一下限 $D_T = H_u - H_b$, 因此应有

$$\max(C_i^1) > H_u, \qquad \min(C_j^0) < H_b \qquad 及 \qquad \min(C_i^0) - \max(C_j^1) > D_T \tag{6}$$

(6)式是确定触发器阈值及发射时可加最大噪声的关系式, 一般情况应留有一定的余量。

图 4 给出了被传送的信息 $s(t)$, 混沌驱动信号 $x(t+\tau)$, 已调制信号 $y(t)$ 及噪声 $e(t)$ 和 $y(t) + e(t)$ 的波形图, 噪声幅度为信号 $y(t)$ 幅度的 400%。图 5 为接收端用来进行信息恢复的 $z(t)$ 及 C_i(计算时的离散采样时间 $\Delta t = 0.1$)和恢复信息 $s_r(t)$, 码宽 $T = 12\tau$。由图 5 可见, 当存在较大的噪声时, 信息仍能被安全地恢复。如果噪声减小, 则信息的恢复将更容易。图中取 $H_u = 14000$ 和 $H_b = 12000$, 由图 5 可见, 若 H_u 选择过大(比如 16000)可能导致其中的一个码出错。因此 H_u 和 H_b 的选择很主要。

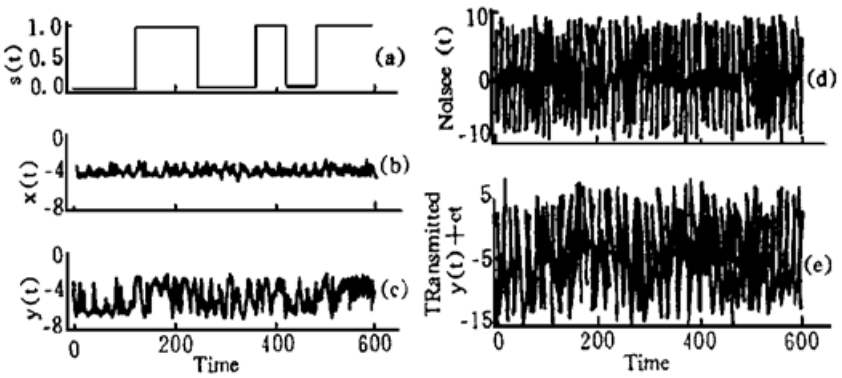

Fig. 4 Message and transmitted signals (a) $s(t)$; (b) $x(t+\tau)$; (c) $y(t)$; (d) $e(t)$, (e) $y(t) + e(t)$

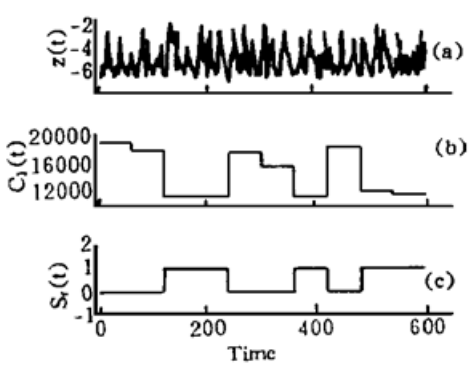

Fig. 5 Recovery of messsage at the receiving end. (a) $z(t)$; (b) $C_i(t)$, (c) $s_r(t)$

总的说来, 混沌系统作为信号源, 两个开环声光调制器作为非线性元件把混沌信号进行非线性变换, 其中一个把信息加入相位并产生载波, 另一个为接收端恢复信息时所用, 与已

有的单变量混沌系统利用混沌同步进行信息传输法[10]相比，这种方法不需要混沌系统的同步，由于使用相关处理，抗噪声能力强因而更实用。

3　保密性能

随着对混沌动力学研究的深入，人们发现携带外加信息的混沌信号或多或少地与无外加信息的混沌有所区别，而且这种区别可以用混沌动力学的某些特殊描述反映出来，正是根据这一点，窃听者有可能破译出被加密的信息，这要求对混沌的种类和特性有深入的了解。例如文献[13]通过对 Lorenz 系统进行特殊的重构返回映射，根据映射图的规则劈裂(数字量加密)或规则伸展(模拟量加密)来提取信息，其前提是在无噪声或噪声相当小的情况下才能实现。如果把频谱能够覆盖混沌频谱的噪声加入到信号通道中，那么通过上面的映射重构也很难把信息破译出来。但是，噪声的引入又将限制通讯效果，而本文提出的根据混沌相位特性由相关信号处理实现的混沌保密通讯可以减弱这种限制。

图 6 给出了试图以离散模型重构返回映射进行破译的结果。由图可见，当噪声在 20% 时有效的破译就十分困难，而在前面图 4 中引入的噪声已达 400%。破译时重构返回映射比做吸引子实际且容易，但由于延时系统的动力学复杂性，实际截取的变量极值来自连续微分方程的解，进行返回映射重构不象图 6 离散模型重构中出现规则劈烈那样，因此返回映射重构更加困难。如果做相空间吸引子图也可以发现，含噪声时两片劈裂的吸引子(分别对应于 0. 1 信息)迭合在一起使得破译失败。目前未发现较好的破译方法和文献中还没有报道。

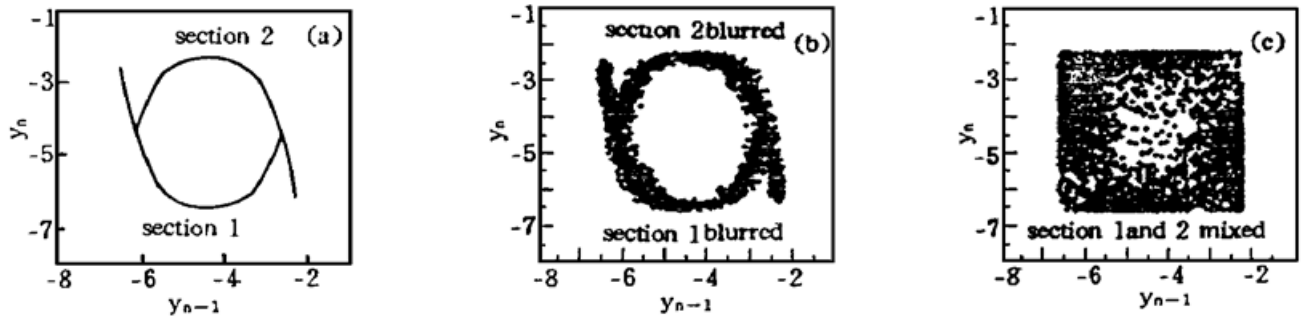

Fig. 6 Reconstructed return map with variables from discrete mapping equation. (a) no noise; (b) 5% noise; (c) 20% noise

讨　论　本文系统研究了利用声光双稳混沌系统进行混沌无同步保密通讯的原理。这种方法要求同时传送混沌驱动信号与加密的混沌信号，这一点与文献[14]相同，但实现起来简单，抗噪声效果好，因此更实用更安全。本文的方法被破译的可能性较小，由于所使用的噪声为宽带噪声，因此带通滤波法无效，且使用重构返回映射法在同频带的噪声覆盖下也无效。

对于可能存在的驱动信号 $x(t)$ 与加密信号 $y(t)$ 同时被截获的情况，窃听者可能直接把二者做相关处理试图破译，这就要求发射者选择驱动系统和调制系统有较大的参数差异(即方程(1)和方程(3)的参数值相差较大)，使得二者相关性丧失(如图 1)而破译失败。同时，发射 $y(t)$ 时人为加入宽带噪声以防止重构法窃听，但 $x(t)$ 不要加入大的噪声，以免接收端产生的 $z(t)$ 与 $y(t)$ 失去相关性导致信息恢复出错。

由于光学双稳系统在光电子技术中的重要性，对它的研究将不局限于开关和存储等功能，本文的研究不仅为它寻找了新的应用场合，也为混沌在光学中的实际应用提供新的参考。

参 考 文 献

[1] L. M. Pecora, T. L. Carroll, Synchronization in Chaotic Systems. *Phys. Rev. Lett.*, 1990, **64**(8): 821~824

[2] L. M. Pecora, T. L. Carroll, Driving systems with chaotic signals. *Phys. Rev.* (*A*), 1991, **44**(4): 2374~2383

[3] T. L. Carroll, L. M. Pecora, Synchronizing chaotic circuits. *IEEE Trans. Circuits Syst.*, 1991, **38**(4): 453~456

[4] R. He, P. G. Vaidya, Analysis and synthesis of synchronous periodic and chaotic systems. *Phys. Rev.* (*A*), 1992, **46**(12): 7387~7392

[5] J. H. Peng, E. J. Ding, M. Ding *et al.*, Synchronizing hyperchaos with a scalar transmitted signal. *Phys. Rev. Lett.*, 1996, **76**(6): 904~907

[6] J. M. Kowalski, G. L. Albert, G. W. Gross, Asymptotically synchronous chaotic orbits of exitable elements. *Phys. Rev.* (*A*), 1990, **42**(10): 6260~6263

[7] A. Maritan, J. R. Banavar, Chaos, Noise, and Synchronzation, *Phys. Rev. Lett.*, 1994, **72**(10): 1451~1454

[8] T. L. Carroll, L. M. Pecora, Cascading synchronized chaotic systems. *Physica*, 1993, **D67**: 126~140

[9] U. Parlitz, S. Ergezinger, Robust communication based on chaotic spreading sequences. *Phys. Lett.* (*A*), 1994, **188**(2): 146~150

[10] Y. H. Yu, K. Kwak, T. K. Lim, Secure communication using small time continuous feedback. *Phys. Lett.* (*A*), 1995, **197**(5): 311~315

[11] H. J. Li, J. L. Chern, Coding the chaos in a semiconductor diode for information transmission. *Phys. Lett.* (*A*), 1995, **206**(3): 217~221

[12] L. Kocarev, U. Parlitz, General approach for chaotic synchronization with application to communication. *Phys. Rev. Lett.*, 1995, **74**(25): 5028~5031

[13] G. Perez, H. A. Cerdeira, Extracting messages masked by chaos. *Phys. Rev. Lett.*, 1995, **74**(11): 1970~1973

[14] A. Oksasoglu, T. Akgul, Chaotic masking scheme with a linear inverse system. *Phys. Rev. Lett.*, 1995, **75**(25): 4595~4597

[15] R. Vallee, C. Delisle, J. Chrostowski, Noise versus chaos in acousto-optic bistability. *Phys. Rev.* (*A*), 1984, **30**(1): 336~342

Study on Mechanism of Secure Communication with Driven Chaos Masking in Optical Bistable System

Liu Jingang[1, 2] He Changshun[3] Shen Ke[2] Zhou Liwei[1]

1, *Optics Engineering Department, Beijing Institute of Technology, Beijing* 100081

2, *Physics Department, Changchun Institute of Optics and Fine Mechanics, Changchun* 130022

(Received 18 July 1996; revised 16 April 1997)

Abstract Based on the dynamic behavior of the acousto-optical bistable system driven chaotically, a secure communication system is proposed. It can be realized by adding message due to the phase property of the system and extracting message due to the chaotic signal produced by chaos driving at the receive end. It is found that message can be securely transmitted even the signal masked by large noise. The message recovery needs no chaotic signal perfectly synchronized with carrier but only depends on the correlation of transmitted signal to the output signal of driven system at the receive end. The scheme is praticable in application.

Key words optical bistable system, chaos, secure communication.