中国激光

基于储备池计算的激光混沌同步保密通信研究

刘家跃[1,2]，张建国[1,2*]，李创业[1,2]，王云才[3,4]

[1]太原理工大学新型传感器与智能控制教育部重点实验室，山西 太原 030024；

[2]太原理工大学物理与光电工程学院，山西 太原 030024；

[3]广东省信息光子技术重点实验室，广东 广州 510006；

[4]广东工业大学信息工程学院，广东 广州 510006

摘要 为解决传统混沌同步通信中因收发双方参数难以完全匹配而导致的同步系数较小的问题，本文提出了一种基于储备池计算的激光混沌同步保密通信方法。利用混沌加密信号和部分混沌载波信号对储备池进行训练，使之与发送方同步，实现保密通信；进一步，利用交叉预测算法来降低储备池的预测误差，消除了同步误差积累效应，实现了长期预测与同步通信。此外，本文还探究了系统的同步与通信性能，得到了系统能在保证安全度的前提下实现同步系数为 99.90%的高质量混沌同步与通信的结论。仿真结果表明混沌载波的预测均方误差可达 10^{-4} 量级，通信误码率可达 10^{-9} 量级。最后，通过图像通信仿真实验验证了本系统的可行性。

关键词 光通信；混沌同步；储备池计算；交叉预测算法

中图分类号 TN918.8+1；TN249；TP183 **文献标志码** A **DOI**：10.3788/CJL202249.1806001

1 引 言

基于物理层加密方式的激光混沌通信具有高安全性的特点[1-2]，其以速率高、抗干扰能力强等优点[3-6]成为近年来的研究热点[7-9]。但是，在传统的混沌同步通信中，高质量同步的实现需要通信收发双方参数高度一致，因此，混沌同步通信不仅面临同步系数较小的问题，还增加了硬件实现的难度[2,10-16]。

神经网络具有良好的非线性拟合能力，已有学者利用它来预测混沌载波，进而实现混沌同步通信。2019 年，Ke 等[1]利用全连接神经网络作为通信接收方实现了激光混沌同步通信，相比于传统方法，这一方法降低了对收发双方参数的苛刻要求，简化了通信系统结构。Felix 等[17]、Kim 等[18]分别利用深度神经网络构建了自动编码器和解码器，实现了通信系统的全局优化。尽管上述研究都为神经网络在通信领域的应用进行了有益探索，但为了保证较高同步精度和较低误码率而不得不选择多隐藏层结构的神经网络，由此提高了计算复杂度，降低了工作效率。储备池计算(RC)作为一种新型的神经网络，近年来已被广泛应用于混沌时间序列预测[19-24]、激活介质的时空动力学观察[25]、不稳定周期轨道检测[26]、通信信道的实时均衡[27-28]和光通信中的调制格式识别[29]等。相较于传统的神经网络，RC 的优势在于减少了所需训练的权重参数的数量，因此其训练过程被极大地简化，工作效率得以显著提高。而且，RC 具有的衰减记忆特性及其所使用的岭回归算法使得其计算精度不会因结构简化而有所降低。2021 年，Zhong 等[24]利用半导体激光器构建了并行光子 RC，并使用无模型预测算法实现了激光混沌同步，同步系数可达 0.99，预测误差为 10^{-2} 水平。这一研究为本文利用 RC 实现激光混沌同步通信提供了借鉴。然而，无模型预测算法无法消除误差积累效应，这使得通信双方难以实现长期同步，进而导致通信中断。从应用角度来看，鲁棒的混沌保密通信必须建立在稳定的混沌同步基础之上，这就要求通信双方不但要具有较大的同步系数，还要能维持较长的同步时间。

交叉预测算法是一种可以有效消除误差积累效应的机器学习算法。Zimmermann 等[25]利用基于交叉预测算法的 RC 推断了心脏建模中兴奋介质的动力学特性，其预测误差可达 10^{-4} 量级。Cunillera 等[19]利用三个激光混沌变量(强度、相位和载流子数)中的任一个来交叉预测推断其余两个，其预测误差可达 10^{-3} 量级。可见，交叉预测算法的核心就是用无限已知变量来预测未知变量，这一点与混沌同步通信领域中加密信号已知、混沌载波未知的情况不谋而合。

收稿日期：2021-12-01；**修回日期**：2022-01-03；**录用日期**：2022-01-20

基金项目：国家自然科学基金重大仪器专项项目(61927811)、国家自然科学基金重点项目(61731014)、国家自然科学基金国际合作项目(61961136002)、国家重点研发计划(2019YFB1803505，2018YFB2200900)

通信作者：*zhangjianguo@tyut.edu.cn

本文提出了一种基于 RC 的激光混沌同步保密通信方法，该方法可以解决传统混沌同步通信中因收发双方参数难以完全匹配而导致的同步系数较小的问题；本文进一步利用交叉预测算法降低了 RC 的预测误差，通过仿真实现了通信收发双方长期、稳定同步以及低误码率通信。此外，本文还对比分析了基于交叉预测算法以及基于无模型预测算法的激光混沌同步通信系统的性能，证明了交叉预测算法的优越性。

2 原理及算法研究

2.1 系统的通信原理

激光混沌同步通信系统的结构如图 1 所示。波长为 1550 nm 的半导体激光器 LD1 的部分输出光经外部反射镜反射回激光器有源区，对其形成扰动，进而输出激光混沌载波 $C(t)$。$C(t)$通过光隔离器 ISO 后，再经一个 50∶50 的光耦合器 OC1 分为两束，一束由光电探测器 PD1 接收，另一束与信息光 $M(t)$经光耦合器 OC2 混合生成加密信号 $C(t)+M(t)$，混沌光与信息光的混合比可由光衰减器 VOA 调节。信息光 $M(t)$由有用信息 Message(4 Gbit/s)通过马赫-曾德尔调制器 MZM 调制激光器 LD2(波长与 LD1 一致，为 1550 nm)产生。加密信号 $C(t)+M(t)$经通信信道传输，并受信道噪声 $n(t)$的干扰。在接收端，PD2 接收到的加密信号为 $u(t)=C(t)+M(t)+n(t)$，$u(t)$经 ADC 模数转换后作为 RC 的输入信号。文中 ADC 的采样率为 20 GSa/s。RC 的目标输出信号是由 PD1 接收的混沌载波 $C(t)$，利用加密信号和部分经背对背传输的混沌载波信号对 RC 进行训练，使之成为具有如下功能的非线性结构 $f(x)$：当来自发送方的加密信号 $u(t)$被输入 RC 后，可以自动输出相应的同步混沌载波 $y(t)$，即 $C'(t)$。同步后，信息 $M'(t)$可以通过加密信号 $C(t)+M(t)+n(t)$(以下所述加密信号均为包含噪声的加密信号)和同步混沌载波 $C'(t)$直接相减进行解密。需要说明的是，本文仅考虑短距通信情况，因而忽略了色散对系统性能的影响，在长距离通信中需要在系统中引入相应的色散补偿[1]。

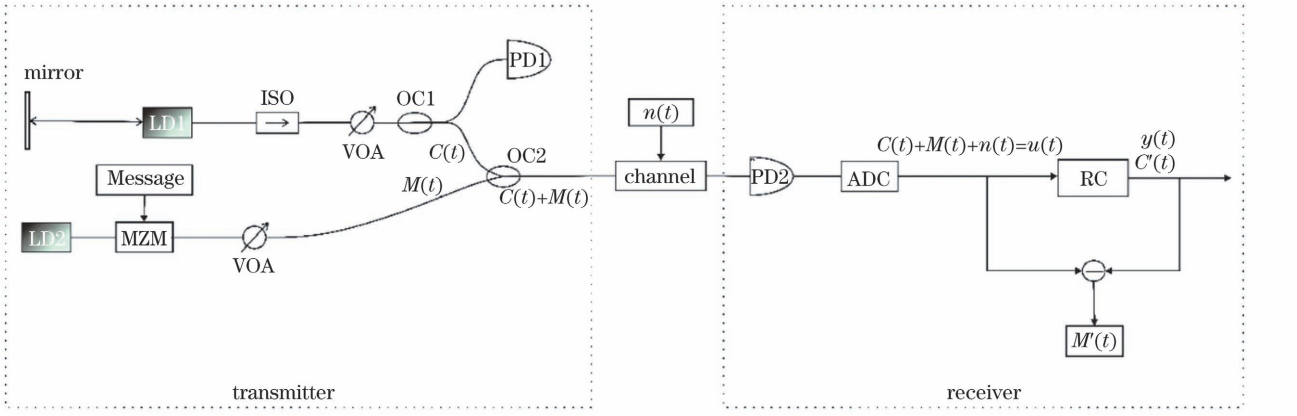

图 1 基于 RC 的激光混沌同步通信系统的原理图。$C(t)$：激光混沌载波；$M(t)$：原始信息；$n(t)$：噪声；$C(t)+M(t)$：加密信号；$C'(t)$：同步混沌载波；$M'(t)$：解密信息；$u(t)$：RC 的输入变量；$y(t)$：RC 的预测输出变量；LD_1/LD_2：激光二极管；ISO：光隔离器；MZM：马赫-曾德尔调制器；Message：有用信息；VOA：可变光衰减器；OC_1/OC_2：光耦合器；ADC：模数转换器；PD_1/PD_2：光电探测器

Fig. 1 Schematic of laser chaos synchronization communication system based on reservoir computing (RC). $C(t)$: laser chaotic carrier; $M(t)$: original message; $n(t)$: noise; $C(t)+M(t)$: encrypted signal; $C'(t)$: synchronized chaotic carrier; $M'(t)$: decrypted message; $u(t)$: input variables of RC; $y(t)$: predicted output variables of RC; LD_1/LD_2: laser diode; ISO: optical isolator; MZM: Mach - Zehnder modulator; Message: useful message; VOA: variable optical attenuator; OC_1/OC_2: optical coupler; ADC: analogue-to-digital converter; PD_1/PD_2: photodetector

发送端光反馈激光器的 Lang-Kobayashi 单模速率方程为

$$\frac{\mathrm{d}E(t)}{\mathrm{d}t}=\frac{1}{2}(1+\mathrm{i}\alpha')\left\{G\left[N_{\mathrm{C}}(t)-N_0\right]-\frac{1}{\tau_{\mathrm{p}}}\right\}\cdot E(t)+kE(t-\tau)\exp(-\mathrm{i}\omega\tau),\tag{1}$$

$$\frac{\mathrm{d}N_{\mathrm{C}}}{\mathrm{d}t}=\frac{I(t)}{qV}-\frac{1}{\tau_{\mathrm{n}}}N_{\mathrm{C}}(t)-G\left[N_{\mathrm{C}}(t)-N_0\right]|E(t)|^2,\tag{2}$$

式中：E 为激光器腔内复电场强度的幅值；α'为线宽增强因子；G 为微分增益系数；N_{C} 为激光器腔内的载流子密度；N_0 为透明载流子密度；τ_{p} 为光子寿命；k 为反馈系数；τ 为光在外谐振腔的往返时间；ω 为激光器输出角频率；$I(t)$为激光器的抽运电流密度；q 为电荷电量；V 为激光器的有源区体积；τ_{n} 为载流子寿命。

在 MATLAB 软件中，使用四阶 Runge-Kutta 法对上述 Lang-Kobayashi 单模速率方程进行求解，求解过程中使用的仿真参数如表 1 所示。光反馈激光器 LD1 产生的激光混沌载波带宽为 8.3 GHz(用 80%能量带宽定义)。

表 1 仿真参数值

Table 1 Values of parameters used in simulation

Symbol and unit	Parameter	Value
α'	Linewidth enhancement factor	3.5
G	Differential gain coefficient	7.0×10^{3}
N_0	Transparent carrier density	1.5×10^{8}
τ_p/ps	Photon lifetime	2.0
τ_n/ns	Carrier lifetime	2.0
τ /ns	Round-trip time of light in the external cavity	5
I_{th}/mA	Threshold current	17.7
V /m^3	Active area volume of the laser	1.2×10^{-16}
q /C	Charge quantity	1.6×10^{-19}
k	Feedback coefficient	3.5×10^{10}
λ /nm	Operation wavelength of LD1 and LD2	1550
h /ps	Time stepping	2.5

2.2 RC 及交叉预测算法

在接收端，RC 的原理如图 2 所示，其包含一个输入层、一个具有 N 个节点的储备池和一个输出层。

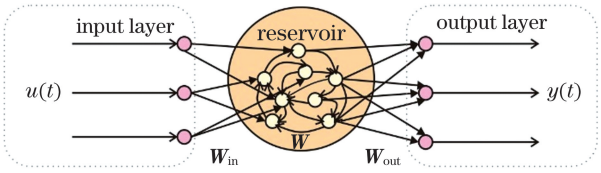

图 2 RC 的结构图

Fig. 2 Principle diagram of reservoir computing

RC 的迭代公式为

$$\boldsymbol{r}(t+\Delta t)=(1-a)\boldsymbol{r}(t)+a\tanh\left\{\boldsymbol{W}\boldsymbol{r}(t)+\boldsymbol{W}_{\text{in}}\begin{bmatrix}b_{\text{in}}\\ u(t+\Delta t)\end{bmatrix}\right\},\tag{3}$$

$$y(t)=\boldsymbol{W}_{\text{out}}\boldsymbol{R}=\boldsymbol{W}_{\text{out}}\begin{bmatrix}b_{\text{out}}\\ u(t)\\ \boldsymbol{r}(t)\end{bmatrix},\tag{4}$$

式中：$\boldsymbol{r}\in\mathbb{R}^{N}$ 是储备池内部 N 个节点的状态向量，其随着输入变量的更新而更新；$\boldsymbol{W}_{\text{in}}\in\mathbb{R}^{N\times(1+M)}$ 是介于输入层和储备池之间的元素随机均匀分布在[−1,1]范围内的输入权重矩阵；$\boldsymbol{W}\in\mathbb{R}^{N\times N}$ 是储备池内部节点之间的稀疏随机连接矩阵，其元素均匀分布在[−1,1]范围内[19-20,28]；泄漏率 a 代表储备池先前状态对当前状态的影响[19]，其取值范围是[0,1]；$\boldsymbol{W}_{\text{out}}\in\mathbb{R}^{M\times(1+M+N)}$ 是介于储备池和输出层之间的唯一需要被训练的权重矩阵；激活函数 tanh 将非线性因素引入节点，以便于 RC 可以逼近任何非线性函数和模型；b_{in}（b_{out}）是伴随 $\boldsymbol{W}_{\text{in}}$（$\boldsymbol{W}_{\text{out}}$）的输入（输出）偏置，本文将它们设置为 1；$\boldsymbol{R}$ 为储备池节点状态矩阵。$\boldsymbol{y}\in\mathbb{R}^{M\times P}$ 由 $y(t)$ 组成，它是要预测的目标输出变量，其在有限时间 $0<t<T$ 内已知；$\boldsymbol{u}\in\mathbb{R}^{M\times P}$ 由 $u(t)$ 组成，它是自 $t\geqslant0$ 便可无限获得的输入变量。根据文献[19-20,25]，$\boldsymbol{W}_{\text{out}}$ 通过岭回归算法确定。岭回归算法的表达式为

$$\boldsymbol{W}_{\text{out}}=\boldsymbol{Y}\boldsymbol{R}^{\mathrm{T}}(\boldsymbol{R}\boldsymbol{R}^{\mathrm{T}}+\xi\boldsymbol{\eta})^{-1},\tag{5}$$

式中：$\boldsymbol{\eta}\in\mathbb{R}^{(1+M+N)\times(1+M+N)}$ 是单位矩阵；ξ 是为了避免过拟合而设置的岭回归参数，本文取其为 10^{-6}；储备池节点状态矩阵 $\boldsymbol{R}\in\mathbb{R}^{(1+M+N)\times S}$ 和有限已知目标输出变量矩阵 $\boldsymbol{Y}\in\mathbb{R}^{M\times S}$ 的第 i 列分别为[b_{out}；$u(i)$；$\boldsymbol{r}(i)$]和[$y(i)$]。

不同于目前已广泛使用的无模型预测算法[20,27,30-32]，本文提出的基于混沌同步通信的交叉预测算法致力于实现长期通信。目前关于交叉预测算法的研究较少，仅文献[19,25]有所涉及，但它们都没有将该算法应用于混沌同步通信领域。在方案的选择问题上，本文将加密信号和混沌载波（而不是有用信息）分别作为输入变量和目标输出变量，这不仅有利于交叉预测算法的实施，还可以保证系统的安全度。无模型预测和交叉预测的原理图如图 3 所示。无模型预测用同一时间序列的历史变量来预测未来变量。在同步通信中，输入变量 $u(t)$ 和目标输出变量 $u'(t+\Delta t)$ 分别是混沌载波 $C(t)$ 的历史数据和未来数据，它们只具有有限可观测时间。如图 3(a)所示，在训练阶段，随着输入变量 $u(t)$ 的更新，RC 通过随机确定的连接矩阵 $\boldsymbol{W}_{\text{in}}$ 和 $\boldsymbol{W}$ 来迭代生成储备池节点状态矩阵 $\boldsymbol{R}$；然后，目标输出变量 $u'(t+\Delta t)$ 结合矩阵 $\boldsymbol{R}$ 训练输出连接权重矩阵 $\boldsymbol{W}_{\text{out}}$，训练完成后便不再改变。在测试阶段，连接权重矩阵 $\boldsymbol{W}_{\text{in}}$、$\boldsymbol{W}$ 和 $\boldsymbol{W}_{\text{out}}$ 都被确定，继续输入历史数据 $u(t)$，RC 会迅速预测并输出未来数据 $u(t+\Delta t)$，并将此未来数据反馈回输入端，作为下一时刻的历史输入数据。由此，RC 便能自动运转起来。值得注意的是，无模型预测的误差来源有两个：一方面，RC 训

练的本质相当于从输入变量到输出变量的非线性映射，即输入变量被用来预测（估计）输出变量，因此，预测本身会因为所训练的网络精度而有误差；另一方面，预测输出数据需要被反馈回输入端作为下一时刻的输入数据，因此，输入数据本身就是有误差的估计值，而不是真实值。当它被用来预测输出变量时，这种误差会随着迭代次数的增多而逐渐积累，预测精度会逐渐下降。误差积累效应会随着迭代次数的增加而愈发明显，直至不能预测。这就是无模型预测不能实现长期预测的原因。

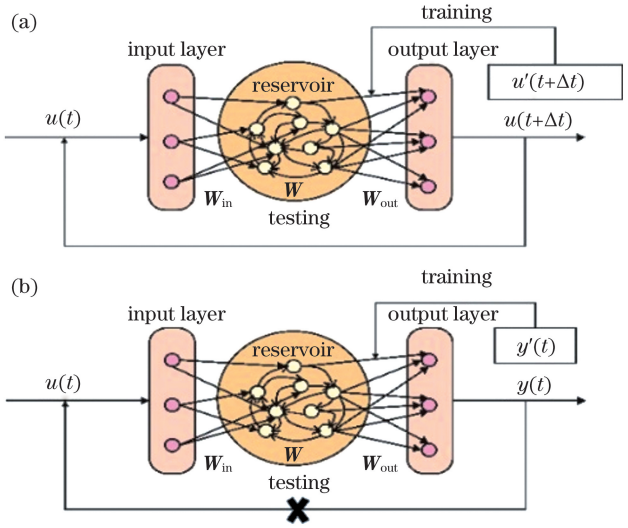

图 3 无模型预测和交叉预测原理图。(a)无模型预测；(b)交叉预测

Fig. 3 Schematics of model-free prediction and cross-prediction. (a) Model-free prediction; (b) cross-prediction

交叉预测的本质是基于无限可观测的输入变量和有限可观测的目标输出变量来构建非线性网络，使RC可以根据输入变量自动推断出不可观测阶段的目标输出变量。图3(b)展示了交叉预测原理图，这里，$u(t)$是输入变量，$y(t)$是RC的预测输出变量，$y'(t)$是与$y(t)$对应的目标输出变量。交叉预测和无模型预测的差异在于两点：其一是在预测原理上，交叉预测的输入变量和目标输出变量分别来自两列时间序列，在本文中，它们分别是加密信号$C(t)+M(t)+n(t)$和混沌载波$C(t)$。加密信号$u(t)$源自叠加了信息$M(t)$和噪声$n(t)$的混沌载波$y'(t)$，$u(t)$和$y'(t)$具有较高的相关性，并且交叉预测的精度与它们的相关性有关；此外，$u(t)$可以通过调整信息的幅度来控制。因此，$y'(t)$的预测精度是可控的。同时，加密信号$u(t)$可以长期获得，因此，交叉预测不必再像无模型预测那样将混沌载波的历史数据作为输入来预测混沌载波的未来数据，而是将加密信号作为输入来预测混沌载波。其二是在预测流程上，交叉预测的输出变量$y(t)$不必再反馈回输入端，RC的输入数据一直是加密信号，它是精确的真实值而不是被预测出来的估计值，所以，误差不会随着迭代次数的增多而逐渐积累，误差积累效应被消除。因此，交叉预测算法的误差来源仅有一个，即RC网络本身的训练精度。这样一来，预测误差被大幅降低，长期同步与长期通信得以实现。

为了便于数值分析，这里采用式(6)来说明。高斯噪声$n(t)$被用来模拟通信信道的噪声，RC的实际输入变量$u(t)$是混沌载波、信息及噪声三者的混合，如式(6a)所示。在RC的整个工作过程中，输入变量$u(t)$的每次迭代都对应生成了储备池节点状态向量$\boldsymbol{r}(t)$。在训练阶段，RC首先根据式(3)经历一个初始化过程($0<t<\tau$)，以消除瞬态，并且在此期间状态向量$\boldsymbol{r}(t)$只生成而不存储到状态矩阵$\boldsymbol{R}(t)$中；然后，在$\tau<t<T$期间继续向RC注入输入变量，但此时将$\boldsymbol{r}(t)$存储到$\boldsymbol{R}(t)$中，以使低维输入向量映射到高维状态矩阵；最后，将状态矩阵$\boldsymbol{R}$与目标输出变量矩阵$\boldsymbol{Y}$代入式(5)来计算$\boldsymbol{W}_{\text{out}}$。$\boldsymbol{Y}$由发送方经过背对背传输至合法接收方，并仅用于训练阶段，这样，即使第三方RC获得了加密信号，但由于没有目标混沌载波，仍然无法对RC进行训练，也就无法实现混沌载波的预测以及混沌同步通信。因此，本系统的安全性得到了保障。在测试阶段($t>T$)，$\boldsymbol{W}_{\text{out}}$已固定，当$u(t)$被注入RC后，RC会迅速地通过式(3)、(4)计算出预测输出变量$y(t)$，它也是同步混沌载波$C'(t)$。最后，信息$M'(t)$通过式(6b)所示的直接相减解调得出。

$$u(t)=C(t)+M(t)+n(t), \tag{6a}$$

$$M'(t)=C(t)+M(t)+n(t)-y(t)=C(t)+M(t)+n(t)-C'(t)。 \tag{6b}$$

3 仿真结果

3.1 同步及通信性能研究

在发送端，混沌载波采用光反馈半导体激光器产生的激光混沌，伪随机码作为有用信息叠加至混沌载波上，成为混沌加密信号。掩盖系数α的计算公式为

$$\alpha=\frac{M_{\text{P-P}}}{C_{\text{P-P}}}\times 100\%, \tag{7}$$

式中：$M_{\text{P-P}}$是信息$M(t)$的峰峰值；$C_{\text{P-P}}$是混沌载波$C(t)$的峰峰值。

在接收端，经过训练的RC接收到来自发送方的加密信号后，会预测输出及与之对应的同步混沌载波。为量化预测性能，本文计算了同步混沌载波$C'(t)$的预测归一化均方误差(NMSE，记为e_{NMSE})，计算公式为

$$e_{\text{NMSE}}=\frac{1}{L}\frac{\sum_{t>T}[y'(t)-y(t)]^2}{\text{var}(y')}, \tag{8}$$

式中：t表征输出变量索引，取值范围是$t>T$；$y(t)$是RC的预测输出变量，它无限接近目标输出变量$y'(t)$；var(•)代表参数的方差；L是目标值以及与之对应的预测值二者的组合个数。NMSE用来衡量预测的精准度，它指的是混沌载波的预测值与真实值之间的近似程度[18,33-34]，NMSE越小，表示预测精度越高。

同步功能实现后，信息可由加密信号和 RC 输出的同步混沌载波直接相减进行解调恢复。通信质量可以通过解调信息 $M'(t)$ 的误码率(BER，记为 r_{BER})来定量计算，本文采用 Q 因子法计算 BER，计算公式为

$$r_{\mathrm{BER}}=\frac{1}{\sqrt{2\pi}}\frac{1}{Q}\exp\left(-\frac{Q^2}{2}\right), \tag{9a}$$

其中，

$$Q=\frac{I_1-I_0}{\sigma_1+\sigma_0}。 \tag{9b}$$

当发送端传输有用信息为二进制序列“1”和“0”时，由于预测同步精度及噪声等的影响，接收端解调出来的信息不是精确的“1”和“0”比特数据，而是围绕它们上下微小随机波动的数值。I_1 和 I_0 分别是恢复信息 $M'(t)$ 中与原始信息 $M(t)$ 中的“1”和“0”相对应的二进制序列的平均值；σ_1 和 σ_0 分别是恢复信息 $M'(t)$ 中与原始信息 $M(t)$ 中的“1”和“0”相对应的二进制序列的标准差[35]。BER 越小，表示解密效果越好，通信质量越高。

接下来，以掩盖系数 $\alpha=5.56\%$、信噪比 $R_{\mathrm{SN}}=20$ dB 为例展示原始信息、混沌载波及加密信号的时序波形图，如图 4 所示。混沌载波和加密信号的波形十分相似，这说明信息被很好地隐藏在载波中。

进一步，图 5 给出了掩盖系数 $\alpha=5.56\%$、信噪比 $R_{\mathrm{SN}}=20$ dB 及储备池节点数 $N=1200$ 时的目标载波、预测载波的时序波形图，以及相对应的预测误差和载波同步关联点图。由图 5(a)可知预测载波和目标载波高度重合，每一点的预测误差为 10^{-3} 量级；同时，图 5(b)显示 RC 预测的同步载波和来自发送方的目标载波大部分都拟合在 $y=x$ 直线上，同步系数为 99.90%，说明系统实现了高质量的混沌同步[38]。经计算可知 NMSE 为 1.94×10^{-3}，即系统的预测精度是良好的。经过直接相减解调，恢复信息被量化为比特“1”和“0”。原始信息和量化解调信息的时序波形如图 6(a)所示，可见，二者高度重合。计算后可知 BER 为 1.19×10^{-9}，此值低于 3.8×10^{-3} 这一硬判决前向纠错阈值标准(HD-FEC 标准)[1]，这表明系统达到了通信标准，实现了通信功能。图 6(b)给出了掺杂噪声的原始信息和未经量化的解调信息，二者波形相似，表明 RC 具有混沌通滤波效应[16,36-37]。这一点与传统混沌同步通信中接收机的作用是一致的。

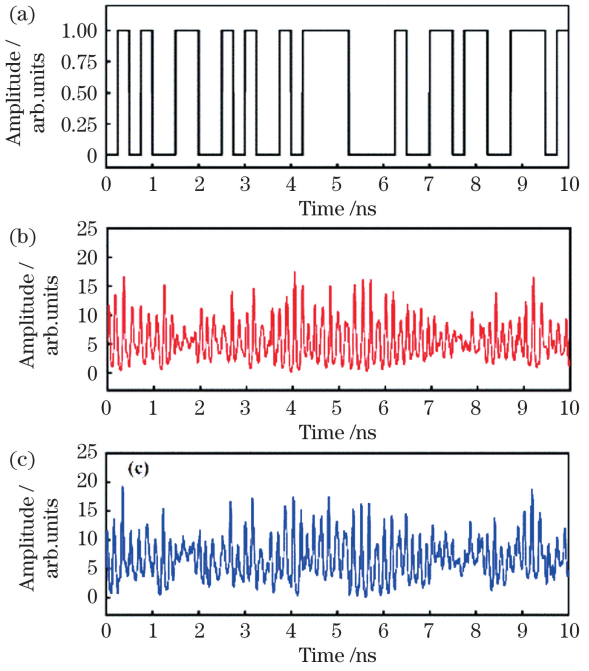

图 4　掩盖系数 $\alpha=5.56\%$、信噪比 $R_{\mathrm{SN}}=20$ dB 时的时序波形图。(a)原始信息；(b)混沌载波；(c)加密信号

Fig. 4　Temporal waveforms when mask coefficient α is 5.56% and signal-to-noise ratio R_{SN} is 20 dB. (a) Original message; (b) chaotic carrier; (c) encrypted signal

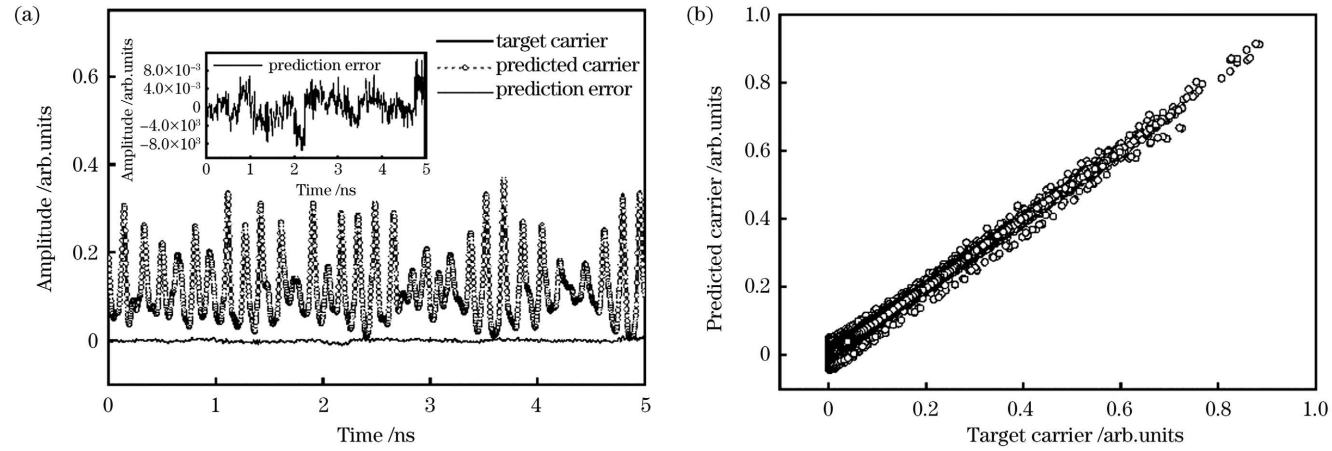

图 5　掩盖系数 $\alpha=5.56\%$、信噪比 $R_{\mathrm{SN}}=20$ dB 时的载波同步结果。(a)目标载波和预测载波的时序图以及相对应的同步误差，插图是预测误差的细节放大图；(b)RC 预测的同步载波和来自发送方的目标载波的混沌同步关联点图

Fig. 5　Carrier synchronization results when mask coefficient α is 5.56% and signal-to-noise ratio R_{SN} is 20 dB. (a) Temporal waveforms of target carrier and predicted carrier, as well as the corresponding synchronization error, the inset shows the detail of prediction error; (b) chaotic synchronization plot of predicted synchronization carrier by RC and target carrier received from transmitter

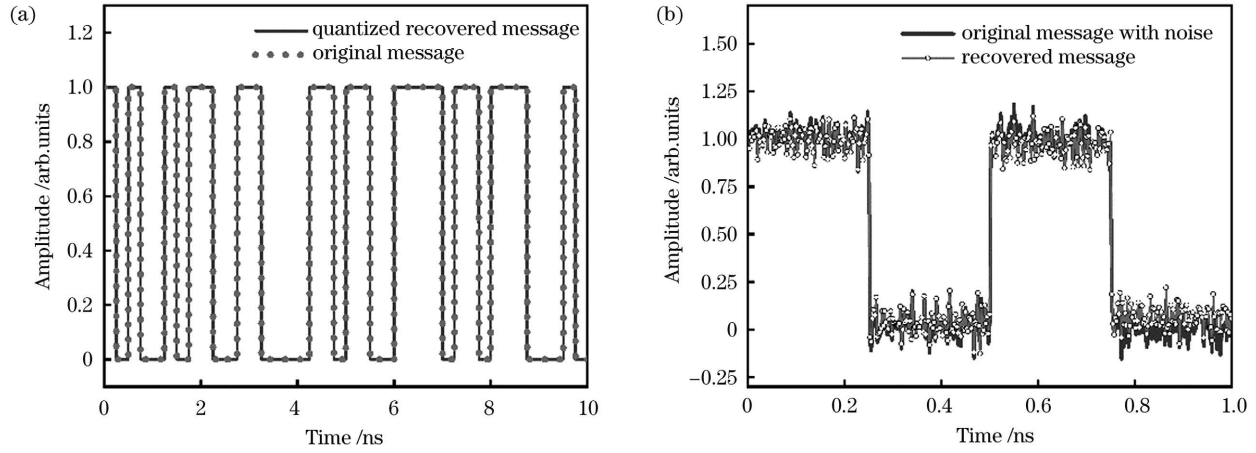

图 6　掩盖系数 $\alpha=5.56\%$、信噪比 $R_{SN}=20$ dB 时，信息解调的时序波形图。(a)原始信息以及量化解调信息；(b)原始加噪信息以及未经量化的解调信息

Fig. 6　Temporal waveforms of message decryption when mask coefficient α is 5.56% and signal-to-noise ratio R_{SN} is 20 dB. (a) Original message and quantized recovered message; (b) original message with noise and recovered message before quantizing

储备池节点数量是影响 RC 预测精度的重要因素，因此，本文探究了节点数量 N 对混沌同步及通信性能的影响。下面以掩盖系数 $\alpha=5.56\%$、$R_{SN}=20$ dB 为例，探究 RC 的最优节点数。由图 7(a)可知：随着节点数增多，BER 和 NMSE 整体呈先下降后趋于稳定的趋势，相应的同步系数 β 整体呈先上升后趋于稳定的趋势；当节点数小于 1000 时，系统同步及通信性能随着节点数增多而明显提高。当节点数介于

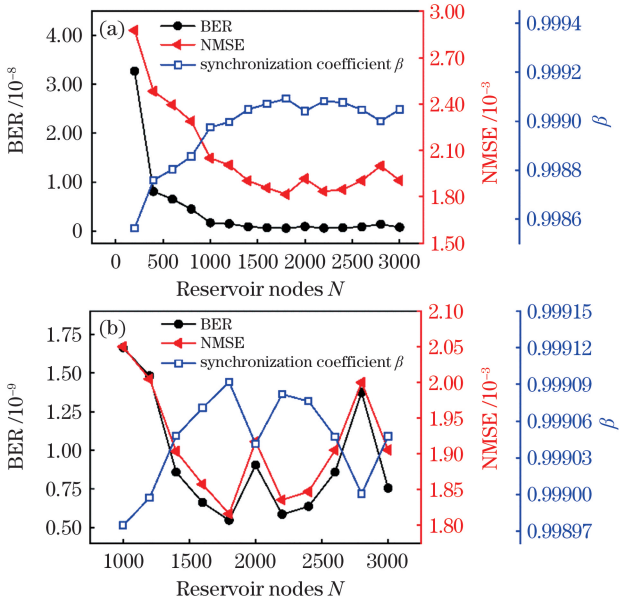

图 7　掩盖系数 $\alpha=5.56\%$、信噪比 $R_{SN}=20$ dB 时，BER、NMSE 及同步系数 β 随节点数 N 的变化。(a) $N=200\sim3000$，间隔 200；(b)细节放大图($N=1000\sim3000$，间隔 200)

Fig. 7　BER, NMSE and synchronization coefficient β versus reservoir nodes N when mask coefficient α is 5.56% and R_{SN} is 20 dB. (a) N ranges from 1000 to 3000 in intervals of 200; (b) enlarged details (N ranges from 1000 to 3000 in intervals of 200)

1000 到 3000 时，系统同步及通信性能呈现小幅波动，且在 $N=1800$ 时取得最优性能，如图 7(b)所示。

当掩盖系数为 5.56%时，RC 解密的 NMSE 和 BER 随着信噪比的变化如图 8 所示。由图 8 可知，NMSE 和 BER 都随着信噪比的增大而单调降低，当 $R_{SN}=3.6$ dB 时，BER 开始越过 HD-FEC 标准线，通信质量合格。当信噪比较大时，BER 可达到 10^{-9} 量级，NMSE 可达到 10^{-3} 量级。同时，为验证系统抗攻击的安全度，本团队还绘制了窃听者使用截止频率等于信息比特率的五阶巴特沃斯低通滤波器对信道中传输的加密信号进行直接解调[也称为直接线性滤波(DLF)攻击[2]]的 BER 结果。在不同的信噪比下，DLF 攻击的 BER 都在 0.29 以上，远高于 HD-FEC 标准，即系统具有较高的安全度。

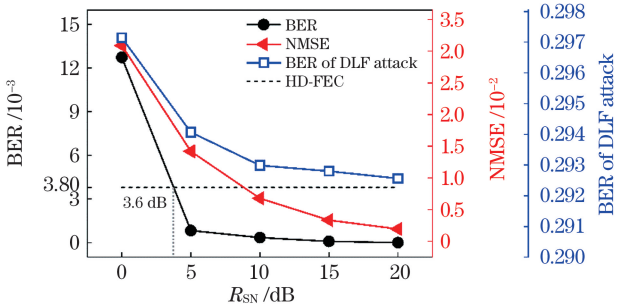

图 8　掩盖系数 α 为 5.56%时，RC 解密的 NMSE 和 BER 以及 DLF 攻击的 BER 随信噪比 R_{SN} 的变化

Fig. 8　NMSE and BER of RC decryption and BER of direct linear filtering (DLF) attack versus R_{SN} for the case with mask coefficient α of 5.56%

3.2　结果对比

本节分别对基于交叉预测算法和基于无模型预测算法的系统的通信性能进行对比。目前对无模型预测算法的研究较多，但这些算法都面临着无法长期预测的难题[20,27,30-32]。然而，混沌同步通信的特殊性不仅

要求预测精度足够高，还要求预测时间足够长，这样才能保证长期可靠的同步与通信质量。在 2.2 节，本文针对交叉预测相比无模型预测能实现长期预测（即同步保持时间 Syn-time 更长）的原因进行了理论分析。下面将通过仿真实验来证明理论分析的正确性。首先，引入预测同步均方误差（SMSE，记为 e_{SMSE}）指标，其计算公式为

$$e_{\mathrm{SMSE}}=\frac{\sum_{t>T}\left[y'(t)-y(t)\right]^2}{L},\tag{10}$$

式中：t 表征输出变量索引，取值范围是 $t>T$；$y(t)$ 是 RC 的预测输出变量；$y'(t)$ 是与 $y(t)$ 对应的目标输出变量。同步保持时间定义为当 $e_{\mathrm{SMSE}}\leqslant 0.001$ 时对应的最大 t 值，即

$$e_{\mathrm{SMSE}}=\frac{\sum_{t>T}\left[y'(t)-y(t)\right]^2}{L}\leqslant 0.001。\tag{11}$$

图 9(a1)、(a2)分别是无模型预测和交叉预测的载波预测同步时序图，它们是在相同的参数设置（掩盖系数 $\alpha=2.23\%$，信噪比 $R_{\mathrm{SN}}=20$ dB，训练样本数为 20000，测试样本数为 3000）下获得的结果。由图 9(a1)可知，当同步保持时间的 time step 为 50 时，无模型预测的载波预测值和目标值有明显的分离现象，此时，SMSE 为 0.001，NMSE 为 0.1640。相应地，从图 9(b1)中可以看到，当同步保持时间的 time step 为 50 时，SMSE 开始越过标准线 0.001。但由图 9(a2)可以看到此时交叉预测的 SMSE 和 NMSE 值分别仅为 5.53×10^{-7} 和 2.75×10^{-4}，在整个测试集样本上，载波同步时序都高度重合，整个测试集上的 NMSE 值仅为 6.09×10^{-4}，即实现了较高的预测精度和良好的同步效果。相应地，图 9(b2)显示交叉预测的 SMSE 值在整个测试集内都远小于标准值 0.001，长期通信得以实现。

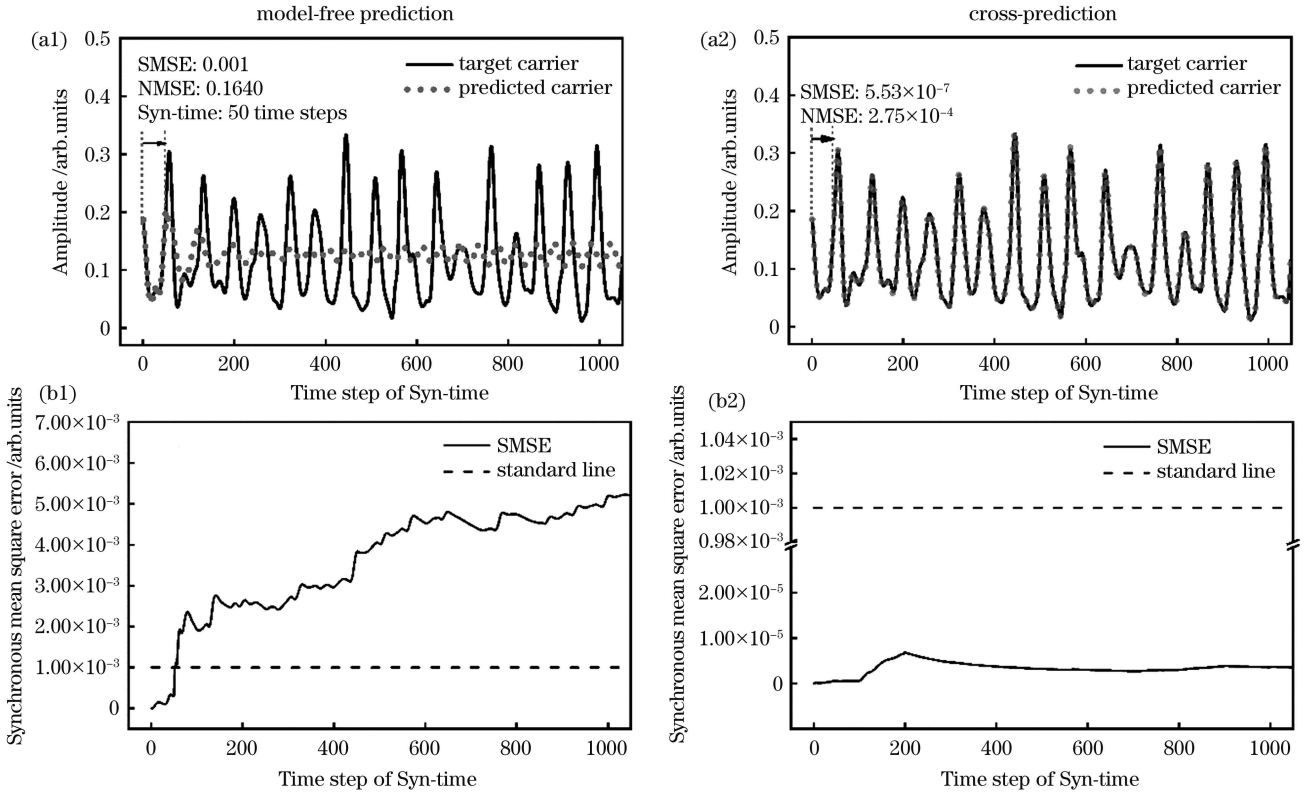

图 9　掩盖系数 $\alpha=2.23\%$、信噪比 $R_{\mathrm{SN}}=20$ dB、训练样本数为 20000、测试样本数为 3000 时的载波同步时序以及与之对应的 SMSE。(a1)(a2)载波同步时序；(b1)(b2)SMSE

Fig. 9　Temporal waveforms of carrier synchronization and the corresponding SMSE when mask coefficient $\alpha=2.23\%$, signal-to-noise ratio $R_{\mathrm{SN}}=20$ dB, training sample quantity is 20000, and testing sample quantity is 3000. (a1)(a2) Temporal waveforms of carrier synchronization; (b1)(b2) SMSE

3.3　同步通信系统仿真实验

为了验证系统的可行性，本节将所提出的基于 RC 的激光混沌同步保密通信系统用于图像传输实验。图 10 所示是不同掩盖系数下的原图、加密图、DLF 攻击图及 RC 解密图。由图 10(d1)、(d2)、(d3)可知，随着掩盖系数 α 增大，解密图的质量明显提高。同时由图 10(b1)、(b2)、(b3)可知，加密图质量几乎不变，都较好地隐藏住了有用信息。图 10(c1)、(c2)、(c3)是窃听者用截止频率等于信息比特率的五阶巴特沃斯低通滤波器对信道中传输的加密信号进行 DLF 攻击的解密图，该图与加密图相似，证明本系统具有良好的抗攻击性能和较高的安全度。因此，本系统的通信质量和安全度能够同时得以保证。

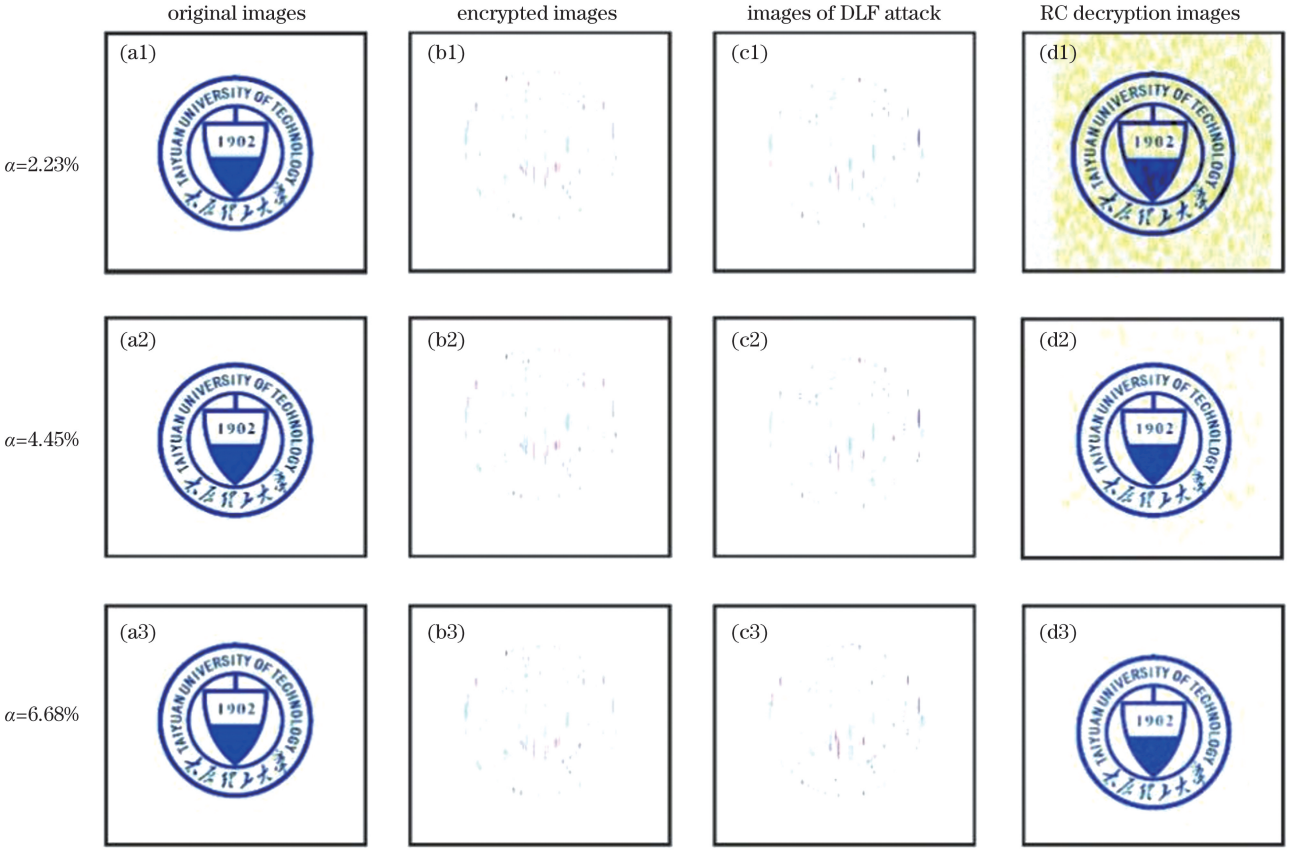

图 10 掩盖系数 α 分别为 2.23%、4.45%及 6.68%时的原图、加密图、DLF 攻击图及 RC 解密图

Fig. 10 Original images, encrypted images, images of DLF attack, and RC decryption images when mask coefficient α is 2.23%, 4.45%, and 6.68%, respectively

4 结 论

本文利用基于交叉预测算法的 RC 实现了激光混沌同步保密通信。其优势在于：1)与传统的混沌同步通信相比，用 RC 作为接收方，避免了传统同步通信中因收发双方参数难以完全匹配而导致的同步系数较小的问题，可在保证系统安全度的前提下实现收发双方的高质量同步，同步系数可达 99.90%；2)相比于无模型预测算法，交叉预测消除了误差积累效应，使预测精度提高了 3 个数量级，预测均方误差 NMSE 可达 10^{-4} 量级，进而长期混沌同步与通信得以实现，误码率 BER 仅为 10^{-9} 量级。此外，通过图像通信仿真实验证明了本系统的安全度和通信质量能够同时得以保证。

参 考 文 献

[1] Ke J X, Yi L L, Yang Z, et al. 32 Gb/s chaotic optical communications by deep-learning-based chaos synchronization [J]. Optics Letters, 2019, 44(23): 5776-5779.

[2] Jiang N, Zhao A K, Wang Y J, et al. Security-enhanced chaotic communications with optical temporal encryption based on phase modulation and phase-to-intensity conversion [J]. OSA Continuum, 2019, 2(12): 3422-3437.

[3] 米乐, 胡思奇, 周田华, 等. 基于低密度奇偶校验码和脉冲位置调制的水下长距离光通信系统设计[J]. 中国激光, 2018, 45(10): 1006002.
Mi L, Hu S Q, Zhou T H, et al. Long distance underwater laser communication system based on low-density parity check codes and pulse-position modulation [J]. Chinese Journal of Lasers, 2018, 45(10): 1006002.

[4] 刘伟达, 罗忠宝, 李响, 等. 地球静止轨道激光通信系统的遮光罩优化设计[J]. 中国激光, 2019, 46(2): 0206005.
Liu W D, Luo Z B, Li X, et al. Optimized design of baffle for laser communication system on geostationary orbit[J]. Chinese Journal of Lasers, 2019, 46(2): 0206005.

[5] 李小明, 王隆铭, 李响, 等. 激光通信天线一体化的摆镜面形优化[J]. 中国激光, 2021, 48(1): 0106006.
Li X M, Wang L M, Li X, et al. Optimization of integrated tilt-mirror for laser communication antenna[J]. Chinese Journal of Lasers, 2021, 48(1): 0106006.

[6] 孙晶, 黄普明, 幺周石. 大气湍流与平台微振动影响下的星地激光通信性能[J]. 激光与光电子学进展, 2021, 58(3): 0301003.
Sun J, Huang P M, Yao Z S. Performance of satellite-to-ground laser communications under the influence of atmospheric turbulence and platform micro-vibration [J]. Laser & Optoelectronics Progress, 2021, 58(3): 0301003.

[7] 颜森林. 激光混沌交叉发射与交替并行接收在保密通信中应用的基本理论与技术[J]. 中国激光, 2020, 47(9): 0906001.
Yan S L. Theory and technique of cross transmittance and alternate parallel reception of laser chaos in secure communication[J]. Chinese Journal of Lasers, 2020, 47(9): 0906001.

[8] 孙宇川, 毛晓鑫, 王安帮. 开环单向耦合半导体激光器的相位混沌同步[J]. 中国激光, 2020, 47(10): 1001003.
Sun Y C, Mao X X, Wang A B. Phase chaos synchronization of semiconductor laser with open-loop unidirectional coupling configuration[J]. Chinese Journal of Lasers, 2020, 47(10): 1001003.

[9] 吴梅, 王龙生, 王云才, 等. 垂直腔面发射激光器的混沌同步恢

复时间研究[J]. 激光与光电子学进展, 2020, 57(21): 210607.
Wu M, Wang L S, Wang Y C, et al. Research on chaos resynchronization time of vertical-cavity surface-emitting lasers [J]. Laser & Optoelectronics Progress, 2020, 57(21): 210607.
[10] Cuomo K M, Oppenheim A V, Strogatz S H. Synchronization of Lorenz-based chaotic circuits with applications to communications[J]. IEEE Transactions on Circuits and Systems Ⅱ: Analog and Digital Signal Processing, 1993, 40(10): 626-633.
[11] Alvarez J. Synchronization in the Lorenz system: stability and robustness[J]. Nonlinear Dynamics, 1996, 10(1): 89-103.
[12] Chen H C, Liau B Y, Hou Y Y. Hardware implementation of Lorenz circuit systems for secure chaotic communication applications[J]. Sensors, 2013, 13(2): 2494-2505.
[13] Argyris A, Syvridis D, Larger L, et al. Chaos-based communications at high bit rates using commercial fibre-optic links[J]. Nature, 2005, 438(7066): 343-346.
[14] Cui S Y, Zhang J Z. Chaotic secure communication based on single feedback phase modulation and channel transmission[J]. IEEE Photonics Journal, 2019, 11(5): 18900883.
[15] Fischer I, Vicente R, Buldú J M, et al. Zero-lag long-range synchronization via dynamical relaying [J]. Physical Review Letters, 2006, 97(12): 123902.
[16] Jiang N, Pan W, Yan L S, et al. Chaos synchronization and communication in mutually coupled semiconductor lasers driven by a third laser[J]. Journal of Lightwave Technology, 2010, 28(13): 1978-1986.
[17] Felix A, Cammerer S, Dörner S, et al. OFDM-autoencoder for end-to-end learning of communications systems[C]//2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications, June 25-28, 2018, Kalamata, Greece. New York: IEEE Press, 2018: 56-60.
[18] Kim M, Lee W, Yoon J, et al. Toward the realization of encoder and decoder using deep neural networks [J]. IEEE Communications Magazine, 2019, 57(5): 57-63.
[19] Cunillera A, Soriano M C, Fischer I. Cross-predicting the dynamics of an optically injected single-mode semiconductor laser using reservoir computing [J]. Chaos: an Interdisciplinary Journal of Nonlinear Science, 2019, 29(11): 113113.
[20] Weng T F, Yang H J, Gu C G, et al. Synchronization of chaotic systems and their machine-learning models[J]. Physical Review E, 2019, 99(4): 042203.
[21] Griffith A, Pomerance A, Gauthier D J. Forecasting chaotic systems with very low connectivity reservoir computers [J]. Chaos, 2019, 29(12): 123108.
[22] Nakayama J, Kanno K, Uchida A. Laser dynamical reservoir computing with consistency: an approach of a chaos mask signal [J]. Optics Express, 2016, 24(8): 8679-8692.
[23] Chen X L, Weng T F, Gu C G, et al. Synchronizing hyperchaotic subsystems with a single variable: a reservoir computing approach[J]. Physica A: Statistical Mechanics and Its Applications, 2019, 534: 122273.
[24] Zhong D Z, Yang H, Xi J T, et al. Predictive learning of multi-channel isochronal chaotic synchronization by utilizing parallel optical reservoir computers based on three laterally coupled semiconductor lasers with delay-time feedback [J]. Optics Express, 2021, 29(4): 5279-5294.
[25] Zimmermann R S, Parlitz U. Observing spatio-temporal dynamics of excitable media using reservoir computing [J]. Chaos: an Interdisciplinary Journal of Nonlinear Science, 2018, 28(4): 043118.
[26] Zhu Q X, Ma H F, Lin W. Detecting unstable periodic orbits based only on time series: when adaptive delayed feedback control meets reservoir computing [J]. Chaos: an Interdisciplinary Journal of Nonlinear Science, 2019, 29(9): 093125.
[27] Antonik P, Duport F, Hermans M, et al. Online training of an opto-electronic reservoir computer applied to real-time channel equalization [J]. IEEE Transactions on Neural Networks and Learning Systems, 2017, 28(11): 2686-2698.
[28] Argyris A, Cantero J, Galletero M, et al. Comparison of photonic reservoir computing systems for fiber transmission equalization[J]. IEEE Journal of Selected Topics in Quantum Electronics, 2020, 26(1): 18964716.
[29] Cai Q, Guo Y, Li P, et al. Modulation format identification in fiber communications using single dynamical node-based photonic reservoir computing[J]. Photonics Research, 2020, 9(1): B1-B8.
[30] Appeltant L, Soriano M C, van der Sande G, et al. Information processing using a single dynamical node as complex system[J]. Nature Communications, 2011, 2: 468.
[31] Pathak J, Hunt B, Girvan M, et al. Model-free prediction of large spatiotemporally chaotic systems from data: a reservoir computing approach [J]. Physical Review Letters, 2018, 120(2): 024102.
[32] Lu Z X, Pathak J, Hunt B, et al. Reservoir observers: model-free inference of unmeasured variables in chaotic systems [J]. Chaos, 2017, 27(4): 041102.
[33] Pyle R, Rosenbaum R. A reservoir computing model of reward-modulated motor learning and automaticity [J]. Neural Computation, 2019, 31(7): 1430-1461.
[34] Antonik P, Gulina M, Pauwels J, et al. Using a reservoir computer to learn chaotic attractors, with applications to chaos synchronization and cryptography[J]. Physical Review E, 2018, 98(1): 012215.
[35] Jiang N, Zhao A K, Liu S Q, et al. Chaos synchronization and communication in closed-loop semiconductor lasers subject to common chaotic phase-modulated feedback[J]. Optics Express, 2018, 26(25): 32404-32416.
[36] Murakami A, Shore K A. Chaos-pass filtering in injection-locked semiconductor lasers[J]. Physical Review A, 2005, 72(5): 053810.
[37] Paul J, Lee M W, Shore K A. Effect of chaos pass filtering on message decoding quality using chaotic external-cavity laser diodes[J]. Optics Letters, 2004, 29(21): 2497-2499.

Secure Communication via Laser Chaos Synchronization Based on Reservoir Computing

Liu Jiayue[1,2], Zhang Jianguo[1,2*], Li Chuangye[1,2], Wang Yuncai[3,4]

[1] *Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, Taiyuan University of Technology, Taiyuan* 030024, *Shanxi, China*;

[2] *College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan* 030024, *Shanxi, China*;

[3] *Guangdong Provincial Key Laboratory of Photonics Information Technology, Guangzhou* 510006, *Guangdong, China*;

[4] *School of Information Engineering, Guangdong University of Technology, Guangzhou* 510006, *Guangdong, China*

Abstract

Objective National security, economic stability, and people's privacy are affected via information security. In recent decades, laser chaos synchronization communication has realized rapid development because of its enhanced physical security. It is based on the message being mixed with the transmitting end's laser chaotic carrier to generate the encrypted signal, and then the encrypted signal being transmitted to the receiving end as its input signal. The receiver employs its chaos pass filtering effect to output the synchronized chaotic carrier signal, and the message is recovered through subtractive demodulation of the encrypted signal and the synchronized chaotic carrier. Thus, synchronization is the key to chaotic synchronization communication, and achieving high-quality synchronization necessitates the completely matched parameters between the sender and receiver, which not only causes a lower synchronization coefficient but increases the difficulty of hardware implementation. This study proposes a reservoir computing-based secure communication approach to laser chaos synchronization. The reservoir computing, as the chaos synchronization communication system's receiver, is synchronized with the sender's chaotic carrier and then obtains the message by subtracting the output variable synchronized chaotic carrier from the reservoir computing's input variable encrypted signal. The proposed approach overcomes the difficulty of a lower synchronization coefficient in traditional chaotic synchronization communication because the parameters of the transmitter and receiver are difficult to match completely.

Methods One of the machine learning algorithms is cross-prediction, the present study proposes the cross-prediction algorithm based on chaotic synchronization communication. Among them, the encrypted and chaotic carrier signals are employed as the reservoir computing's input and output variables, respectively. Its non-linear structure with the following functions is obtained using the encrypted signal and part of the target chaotic carrier signal, which is transmitted back to back from the sender to receiver to train the reservoir computing. When the encrypted signal from the sender is continued to be input into the reservoir computing, the corresponding synchronized chaotic carrier can be automatically output. After synchronization, subtractive demodulation between the encrypted signal and synchronized chaotic carrier can be employed to decrypt the message. Compared with the currently widely employed model-free prediction algorithm, cross-prediction removes the effect of carrier synchronization error accumulation and enhances the prediction accuracy, then the long-term prediction and communication can be realized.

Results and Discussions Simulation exploration comprises three parts. First, the synchronization performance and communication performance of the proposed system are explored, concluding that the system can realize high-quality chaotic synchronization and communication with the synchronization coefficient of 99.90% under the premise of ensuring security (Figs. 5, 8). The simulation results reveal that the carrier prediction mean square error can reach 10^{-4} orders of magnitude (Fig. 9), and the decryption bit error rate can reach the order of 10^{-9} (Fig. 6). The influences of the signal-to-noise ratio and the number of reservoir nodes on the system synchronization performance and communication performance are explored. The results reveal that the carrier prediction error and bit error rate decrease with increasing signal-to-noise ratio (Fig. 8). The optimal number of reservoir nodes is 1800 when the signal-to-noise ratio is 20 dB and the masking coefficient is 5.56% (Fig. 7). Second, when the cross-prediction and model-free prediction algorithms are applied to the system, the synchronization performance and communication performance are compared, respectively. The results reveal that the cross-prediction eliminates the carrier prediction error accumulation effect, and its prediction error shall not accumulate with the increase of the prediction length. Thus, the prediction accuracy is greatly improved, and long-term synchronization and communication can be realized (Fig. 9). Finally, the system's feasibility is verified using the image communication simulation experiment. The results reveal the proposed system has good anti-attack performance and high decryption quality. Additionally, the security and system's communication quality can be assured at the same time (Fig. 10).

Conclusions In this study, reservoir computing based on the cross-prediction algorithm for laser chaos synchronization

secure communication is proposed. Its advantages are as follows. 1) When compared with traditional chaotic synchronization communication, reservoir computing is employed as the receiver that avoids the difficulty of a lower synchronization coefficient due to the difficulty of completely matched parameters between the sender and receiver. The proposed system can realize high-quality chaotic synchronization and communication with a synchronization coefficient of 99.90% under the premise of ensuring security. 2) The cross-prediction algorithm based on reservoir computing applied to the chaotic synchronization communication realizes long-term prediction and communication. The cross-prediction algorithm removes the effect of carrier synchronization error accumulation, enhancing prediction accuracy by 3 orders of magnitude over model-free prediction. The prediction mean square error can reach 10^{-4} orders of magnitude, and the decryption bit error rate can reach the order of 10^{-9}. Furthermore, the image communication simulation experiment demonstrates that the security and proposed system's communication quality are assured at the same time.

Key words optical communications; chaos synchronization; reservoir computing; cross-prediction algorithm