物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

一种基于强跟踪滤波的混沌保密通信方法

李雄杰　周东华

A method of chaotic secure communication based on strong tracking filter

Li Xiong-Jie　Zhou Dong-Hua

引用信息 Citation: Acta Physica Sinica, 64, 140501 (2015)　DOI: 10.7498/aps.64.140501
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.140501
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I14

一种基于强跟踪滤波的混沌保密通信方法*

李雄杰[1)2)†] 周东华[1)]

1) (清华大学自动化系, 北京 100084)

2) (浙江工商职业技术学院电子与信息工程系, 宁波 315012)

(2015 年 1 月 31 日收到; 2015 年 3 月 9 日收到修改稿)

提出了一种基于强跟踪滤波器的混沌保密通信方法. 在发送端, 混沌映射和信息符号被建模成非线性状态空间模型, 信息符号被加性混沌掩盖或乘性混沌掩盖调制, 然后通过信道输出. 在接收端, 驱动信号被接收, 使用带有贝叶斯分类器 (信息符号估计) 的强跟踪滤波器算法动态地恢复信息符号. Logistic 混沌映射的仿真表明, 当信息符号为二进制编码时, 不管是加性混沌掩盖调制还是乘性混沌掩盖调制, 强跟踪滤波器均能较好地从混沌信号中恢复信息符号. 与扩展卡尔曼滤波器相比, 由于卡尔曼滤波器对于离散的信息符号跟踪能力差, 混沌映射中信息符号难以恢复, 比特误码率高. 因此, 这种基于强跟踪滤波器的混沌保密通信方法是有效的.

关键词: 保密通信, 强跟踪滤波器, 混沌, 信息估计

PACS: 05.45.Gg, 05.45.Vx, 84.40.Ua **DOI:** 10.7498/aps.64.140501

1 引 言

在过去的几十年中, 混沌是非线性科学中的一个活跃的研究领域. 由于混沌系统具有初值敏感性, 在频域上具有白噪声的特性, 因而混沌系统常常作为调制信号应用于保密通信系统中. 迄今为止, 已先后提出了很多处理混沌保密通信的思想和方法, 如逆系统方法 [1]、观测器方法 [2,3]、系统论方法 [4]。文献 [5, 6] 采用卡尔曼滤波恢复隐藏在混沌中的信号; 文献 [7, 8] 采用粒子滤波恢复隐藏在混沌中的信号; 文献 [9] 利用 Duffing 振子在混沌载波掩蔽中提取周期信号; 文献 [10, 11] 研究了非相干光反馈、注入下两半导体激光器间的双向混沌通信; 文献 [12—14] 分析了光纤混沌通信及色散补偿对通信性能的影响; 文献 [15] 提出了基于正交混沌序列的多用户混沌通信; 文献 [16] 使用等价控制法直接恢复隐藏在混沌系统中的信号; 文献 [17] 提出了保密性能良好的分数阶混沌系统耦合同步方法; 文献 [18] 采用混沌导频信号实现混沌通信收发两端的同步; 文献 [19] 采用混沌系统部分序列参数辨识来实现保密通信; 文献 [20] 讨论了基于四翼混沌系统受到扰动输入的保密通信; 文献 [21] 讨论了混沌替代扩频调制后的发送信号的混沌性质.

信号处理领域的另一个进展同样引人注目. Zhou 和 Frank 曾提出了一种强跟踪滤波 (strong tracking filtering, STF) 算法 [22], 它可用于非线性过程的状态估计. 该算法主要有以下两个特点: 1) 无论在状态平稳运行还是剧烈变化时, 也无论系统是否达到稳定状态, 它都具有很强的状态跟踪能力; 2) 它具有较强的克服模型不确定度的鲁棒性. STF 在本质上是一种具有次优渐消因子的扩展卡尔曼滤波器, 特别适用于非线性时变随机系统的状态与参数估计.

本文应用 STF 处理混沌保密通信问题. 首先提出基于混沌映射和 STF 的保密通信系统的实现方案; 然后提出用于解决混沌保密通信问题的带有

* 国家自然科学基金 (批准号: 61210012) 资助的课题.

† 通信作者. E-mail: lixiongjie@tsinghua.org.cn

信息符号估计的STF算法; 最后采用Logistic混沌映射仿真, 当信息符号为二进制编码时, STF能较好地从噪声混沌信号中恢复信息的编码值.

2 基于混沌映射和STF的保密通信系统方案

在发送端, 假定传递的信息符号为$s(k)$, 考虑混沌映射如下:

$$x(k+1)=f_1(x(k),\eta), \tag{1}$$

其中η为系统参数, 用于控制系统的混沌区域. 利用混沌信号$x(k)$对信息符号$s(k)$进行调制, 当信息符号$s(k)$叠加到混沌信号$x(k)$上时, 即

$$z(k)=x(k)+s(k) \tag{2}$$

称为加性混沌掩盖(additive chaos masking, ACM); 当信息符号$\boldsymbol{s}(k)$与混沌信号$\boldsymbol{x}(k)$相乘时, 即

$$z(k)=x(k)\times s(k) \tag{3}$$

称为乘性混沌掩盖(multiplicative chaos masking, MCM). 系统方案如图1所示. 方案中$s(k)$为信息符号, $k=1,2,3,\cdots$, 第k步$s(k)$的取值属于集合$\boldsymbol{S}=\{\boldsymbol{\theta}_1,\boldsymbol{\theta}_2,\cdots,\boldsymbol{\theta}_M\}$, $\boldsymbol{\theta}_1,\boldsymbol{\theta}_2,\cdots,\boldsymbol{\theta}_M$是已知的常数向量. 这里假设向量$\boldsymbol{\theta}_1,\boldsymbol{\theta}_2,\cdots,\boldsymbol{\theta}_M$的取值足够小, 不会影响混沌映射(1)的性质.

由于信息符号$s(k)$为时变信号, 利用自回归模型[8] (auto-regressive, AR)对其建模为

$$s(k)=\sum_{i=1}^{p}a_i s(k-i)+w(k), \tag{4}$$

其中p为AR模型的阶数, $w(k)$为加性高斯白噪声. 考虑采用一阶AR模型对$s(k)$建模, 则(1)式可以等效为

$$\begin{bmatrix}x(k)\\ s(k)\end{bmatrix}=\begin{bmatrix}f_1(x(k-1),\lambda)\\ s(k-1)\end{bmatrix}+\begin{bmatrix}0\\ w(k)\end{bmatrix}. \tag{5}$$

考虑信道中的加性高斯白噪声的影响, 在接收端, 接收信号为

$$y(k)=z(k)+v(k). \tag{6}$$

基于(5)和(6)式构成了本文的状态空间模型如下:

$$\left.\begin{aligned}\boldsymbol{x}(k+1)&=\boldsymbol{f}(\boldsymbol{x}(k))+\boldsymbol{w}(k),\\ y(k+1)&=\boldsymbol{h}(\boldsymbol{x}(k+1))+v(k+1)\end{aligned}\right\}, \tag{7}$$

其中$\boldsymbol{x}(k)$为混合状态向量, $\boldsymbol{x}(k)=[x(k)\ s(k)]^{\mathrm{T}}$; $\boldsymbol{w}(k)$为均值为零、协方差矩阵为$\boldsymbol{Q}(k)$的高斯白噪声; $v(k)$为方差为$R(k)$的高斯白噪声; $\boldsymbol{h}(\boldsymbol{x}(k))$为非线性输出方程, 当调制方式为ACM时, $\boldsymbol{h}(\boldsymbol{x}(k))$如(2)式所示; 当调制方式为MCM时, $\boldsymbol{h}(\boldsymbol{x}(k))$如(3)式所示.

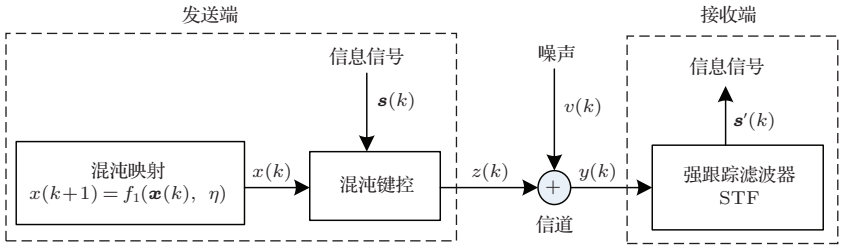

图1 基于STF的混沌保密通信系统框图

Fig. 1. Block diagram of chaotic secure communication system based on STF.

在混沌保密通信领域中, 混沌映射(1)式处于发射端, 输出信号$y(k)$又被称作驱动信号, 用于在公共信道中传输. 因此, 本文所考虑的问题是: 如何在获得驱动信号$y(k)(k=1,2,3,\cdots)$后, 在线地估计信息符号$s(k)$, $k=1,2,3,\cdots$, 并考虑到噪声和输出方程非线性的影响. 为了解决上述问题, 首先给出基于STF处理混沌保密通信问题的方案如图1, 然后在下面将给出能用于在线估计信息符号的STF算法, 以满足混沌保密通信的特殊要求.

3 带信息符号估计的强跟踪滤波器算法

本节将首先给出基于贝叶斯分类器的信息符号估计方法, 然后利用此方法, 提出带有信息符号估计的STF算法, 以便应用于混沌保密通信.

3.1 基于贝叶斯分类器的信息符号估计

信息集合$\boldsymbol{S}$中的每个元素的概率, 用$\Pr(\boldsymbol{s}(k)=\theta_l)$, $l=1,2,\cdots,M$表示, 假设作为先验知识已知. 在通信系统的实际应用中, 一旦编码方式确定后, 一般$\Pr(\boldsymbol{s}(k)=\theta_l)$, $l=1,2,\cdots,M$也可以获得. 而且, 为了提高信道的传输效率, 往往在设计编码方式时, 人为地将$\Pr(\boldsymbol{s}(k)=\theta_l)$, $l=1,2,\cdots,M$设计为等概率的, 即$\Pr(\boldsymbol{s}(k)=\theta_l)=1/M$, $l=1,2,\cdots,M$, 因为这时编码可以达到熵的最大值, 从而可以传递更多的信息, 提高信道的利用率. 在得到驱动信号$\boldsymbol{y}(k+1)$后, 根据贝叶斯公式[7], 有

$$\begin{aligned}&\Pr[\boldsymbol{s}(k)=\theta_l\,|\boldsymbol{y}\,(k+1)]\\&=\frac{p[\boldsymbol{y}(k+1)\big|\boldsymbol{s}(k)=\theta_l]\Pr(\boldsymbol{s}(k)=\theta_l)}{\sum\limits_{j=1}^{M}p[\boldsymbol{y}(k+1)\big|\boldsymbol{s}(k)=\theta_j]\Pr(\boldsymbol{s}(k)=\theta_j)},\end{aligned}\tag{8}$$

式中$l=1,2,\cdots,M$, 其中$p[\boldsymbol{y}(k+1)\big|\boldsymbol{s}(k)=\theta_l]$近似为

$$\begin{aligned}&p[\boldsymbol{y}(k+1)\,|\boldsymbol{s}(k)=\theta_l]\\&\approx p_v\{\boldsymbol{y}(k+1)-h[\boldsymbol{x}_{\theta_l}(k+1|k)]\},\end{aligned}\tag{9}$$

其中,

$$\begin{aligned}&\boldsymbol{x}_{\theta_l}(k+1|k)=\boldsymbol{f}[\boldsymbol{x}(k|k)]+\theta_l,\\&l=1,2,\cdots,M.\end{aligned}$$

$p_v(\cdot)$是观测噪声的概率密度. 从而, 后验概率近似为

$$\begin{aligned}&\Pr[\boldsymbol{s}(k)=\theta_l|\boldsymbol{y}(k+1)]\\&=\frac{p[\boldsymbol{y}(k+1)|\boldsymbol{s}(k)=\theta_l]\Pr(\boldsymbol{s}(k)=\theta_l)}{\sum\limits_{j=1}^{M}p[\boldsymbol{y}(k+1)|\boldsymbol{s}(k)=\theta_j]\Pr(\boldsymbol{s}(k)=\theta_j)}\\&\approx\frac{p_v\{\boldsymbol{y}(k+1)-h[\boldsymbol{x}_{\theta_l}(k+1|k)]\}\Pr(\boldsymbol{s}(k)=\theta_l)}{\sum\limits_{j=1}^{M}p_v\{\boldsymbol{y}(k+1)-h[\boldsymbol{x}_{\theta_j}(k+1|k)]\}\Pr(\boldsymbol{s}(k)=\theta_j)}\\&\propto p_v\{\boldsymbol{y}(k+1)-h[\boldsymbol{x}_{\theta_l}(k+1|k)]\}\\&\quad\times\Pr(\boldsymbol{s}(k)=\theta_l),\end{aligned}\tag{10}$$

式中$l=1,2,\cdots,M$. 因此, 用于恢复信息符号的贝叶斯分类器$\boldsymbol{s}'(k)$可以近似地表示为

$$\begin{aligned}\boldsymbol{s}'(k)=&\mathop{\arg\max}_{\theta_l,l=1,2,\cdots,M}p_v\{\boldsymbol{y}(k+1)\\&-h[\boldsymbol{x}_{\theta_l}(k+1\,|k)]\}\Pr(\boldsymbol{s}(k)=\theta_l).\end{aligned}\tag{11}$$

3.2 带信息符号估计的强跟踪滤波器算法

众所周知, 扩展卡尔曼滤波器(extended kalman filtering, EKF)关于模型不确定性的鲁棒性很差, 而且当系统达到平稳状态时, EKF的增益阵$\boldsymbol{K}(k+1)$将趋于极小值, 此时系统状若发生突变, 预报残差$\boldsymbol{\gamma}(k+1)$将随之增大. 然而增益阵不会随预报残差的增大而增大. 于是EKF将丧失对突变状态的跟踪能力. STF在EKF中引入时变的次优渐消因子$\boldsymbol{\lambda}(k+1)$, 实时调整状态预报误差协方差阵$\boldsymbol{P}(k+1|k)$和相应的增益阵, 强迫残差序列处处保持相互正交. 无论在状态平稳运行还是剧烈变化时, STF都具有很强的状态跟踪能力, 并具有较强的克服模型不确定度的鲁棒性. 在混沌保密通信中, 通常信息符号$\boldsymbol{s}(k)$是一种离散信号, 混沌信号$\boldsymbol{x}(k)$是一种伪随机信号, 对这两种调制信号进行自适应滤波, 当然滤波器的状态跟踪能力越强越好.

为了应用STF算法解决混沌保密通信问题, 根据问题的特殊要求, 对原始的STF算法做一些必要的改进. 针对混沌映射(1)式的状态空间模型(7)式, 带有信息符号估计的STF算法能在线恢复被调制的信息符号$\boldsymbol{s}(k)$, 并同时给出混沌系统的状态估计. 算法步骤如下.

1) 初始化:

设定初始值$\hat{\boldsymbol{x}}(0\,|0)$, $\boldsymbol{P}(0\,|0)$.

2) 状态预报与信息符号估计: 状态的一步预报值为

$$\hat{\boldsymbol{x}}(k+1\,|k)=\boldsymbol{f}[\hat{\boldsymbol{x}}(k\,|k)],\tag{12}$$

在接收到驱动信号$\boldsymbol{y}(k+1)$后, 用如下近似的贝叶斯分类器估计信息符号

$$\begin{aligned}\boldsymbol{s}'(k)=&\mathop{\arg\max}_{\theta_l,l=1,2,\cdots,M}p_v\{\boldsymbol{y}(k+1)\\&-h[\boldsymbol{x}_{\theta_l}(k+1\,|k)]\}\Pr[\boldsymbol{s}(k)=\theta_l].\end{aligned}\tag{13}$$

3) 计算:

$$\boldsymbol{F}[\hat{\boldsymbol{x}}(k\,|k)]=\frac{\partial\boldsymbol{f}(\boldsymbol{x}(k))}{\partial\boldsymbol{x}}\Big|_{\boldsymbol{x}(k)=\hat{x}(k|k)},\tag{14}$$

$$\begin{aligned}&\boldsymbol{H}[\hat{\boldsymbol{x}}(k+1\,|k)]\\&=\frac{\partial\boldsymbol{h}[\boldsymbol{x}(k+1)]}{\partial\boldsymbol{x}}\Big|_{\boldsymbol{x}(k+1)=\hat{x}(k+1|k)}.\end{aligned}\tag{15}$$

4) 求残差序列:

$$\boldsymbol{\gamma}(k+1)=\boldsymbol{y}(k+1)-\boldsymbol{h}[\hat{\boldsymbol{x}}(k+1\,|k)]\,.\tag{16}$$

5) 求次优渐消因子矩阵 $\boldsymbol{\lambda}(k+1) = \mathrm{diag}\{\lambda_1(k+1), \lambda_2(k+2), \cdots, \lambda_n(k+1)\}$, 其中

$$\boldsymbol{\lambda}_i(k+1) = \begin{cases} \lambda_0 & \lambda_0 > 1, \\ 1 & \lambda_0 \leqslant 1, \end{cases} \tag{17}$$

式中 $i = 1, 2, \cdots, n$, 文献 [22] 给出了 λ_0 的计算式子为

$$\lambda_0 = \frac{\mathrm{tr}[\boldsymbol{N}(k+1)]}{\mathrm{tr}[\boldsymbol{M}(k+1)]}, \tag{18}$$

$$\begin{aligned} &\boldsymbol{M}(k+1) \\ &= \boldsymbol{H}(\hat{\boldsymbol{x}}(k+1|k))\boldsymbol{F}(\hat{\boldsymbol{x}}(k|k))\boldsymbol{P}(k|k) \\ &\quad \times \boldsymbol{F}^{\mathrm{T}}(\hat{\boldsymbol{x}}(k|k))\boldsymbol{H}^{\mathrm{T}}(\hat{\boldsymbol{x}}(k+1|k)), \end{aligned} \tag{19}$$

$$\begin{aligned} &\boldsymbol{N}(k+1) \\ &= \boldsymbol{V}_0(k+1) - \boldsymbol{H}(\hat{x}(k+1|k))\boldsymbol{Q}(k) \\ &\quad \times \boldsymbol{H}^{\mathrm{T}}(\hat{\boldsymbol{x}}(k+1|k)) - \beta\boldsymbol{R}(k+1), \end{aligned} \tag{20}$$

残差序列协方差阵 $\boldsymbol{V}_0(k+1)$ 可由下式计算

$$\begin{aligned} &\boldsymbol{V}_0(k+1) \\ &= \begin{cases} \boldsymbol{\gamma}(1)\boldsymbol{\gamma}^{\mathrm{T}}(1) & k = 0, \\ \dfrac{\rho\boldsymbol{V}_0(k) + \boldsymbol{\gamma}(k+1)\boldsymbol{\gamma}^{\mathrm{T}}(k+1)}{1+\rho} & k \geqslant 1, \end{cases} \end{aligned} \tag{21}$$

(21) 式中 ρ 为遗忘因子, 一般取 $\rho = 0.95$. (20) 式中, $\beta \geqslant 1$ 为一个选定的弱化因子, 引入的目的是使得状态估计值更加平滑. 此值可以凭经验选择, 也可以通过仿真, 由下面准则确定

$$\beta : \min_{\beta} \left[\sum_{k=0}^{L} \sum_{i=1}^{n} |x_i(k) - \hat{x}_i(k|k)| \right], \tag{22}$$

式中 L 为仿真步数, 此准则反映了滤波器的累计误差.

6) 求带次优渐消因子的预报误差协方差阵:

$$\begin{aligned} &\boldsymbol{P}(k+1|k) \\ &= \boldsymbol{\lambda}(k+1)\boldsymbol{F}(\hat{\boldsymbol{x}}(k|k))\boldsymbol{P}(k|k)\boldsymbol{F}^{\mathrm{T}}(\hat{\boldsymbol{x}}(k|k)) \\ &\quad + \boldsymbol{Q}(k). \end{aligned} \tag{23}$$

7) 求增益阵

$$\begin{aligned} &\boldsymbol{K}(k+1) \\ &= \boldsymbol{P}(k+1|k)\boldsymbol{H}^{\mathrm{T}}(\hat{\boldsymbol{x}}(k+1|k))\Big\{\boldsymbol{H}[\hat{\boldsymbol{x}}(k+1|k)] \\ &\quad \times \boldsymbol{P}(k+1|k)\boldsymbol{H}^{\mathrm{T}}[\hat{\boldsymbol{x}}(k+1|k)] + \boldsymbol{R}(k+1)\Big\}^{-1}. \end{aligned} \tag{24}$$

8) 更新

$$\begin{aligned} &\hat{\boldsymbol{x}}(k+1\,|k+1) \\ &= \hat{\boldsymbol{x}}(k+1\,|k) + \boldsymbol{K}(k+1)\boldsymbol{\gamma}(k+1). \end{aligned} \tag{25}$$

9) 求状态估计误差协方差阵

$$\begin{aligned} &\boldsymbol{P}(k+1|k+1) \\ &= \{\boldsymbol{I} - \boldsymbol{K}(k+1)\boldsymbol{H}[\hat{\boldsymbol{x}}(k+1|k)]\}\boldsymbol{P}(k+1|k). \end{aligned} \tag{26}$$

最后令 $k = k+1$, 转到步骤 2), 继续循环.

4 仿真实验

利用 Logistic 混沌映射为仿真实例来验证改进的 STF 算法的有效性. Logistic 混沌映射可以用下列的状态方程描述:

$$x(k+1) = \eta \times x(k)(1 - x(k)), \tag{27}$$

其中, 当 $\eta \in [3.57, 4]$ 时, 该映射是混沌的, 在仿真实验中, 选取参数 $\eta = 4$. 信息符号 $s(k)$ 的建模均采用一阶 AR 模型 (5) 式, $s(k)$ 的取值均为二进制编码集合 $\boldsymbol{S} = \{\theta_1, \theta_2\}$, 整个混沌保密通信的方案如图 1 所示, 表示的状态空间模型如 (7) 式所示.

4.1 ACM 仿真

驱动信号 $\boldsymbol{y}(k)$ 选为

$$y(k) = x(k) + s(k) + v(k), \tag{28}$$

其中混沌映射 (27) 式的初始状态 $x(0) = 0.3$; 观测噪声 $v(k)$ 是零均值高斯白噪声, 方差 $R = 0.0005^2$; 二进制 θ_1, θ_2 的取值应足够小, 这样不会影响系统混沌映射的性质, 令二进制编码 $\theta_1 = 0.01$, $\theta_2 = -0.01$. STF 算法的初值为: $\hat{x}(0\,|0) = 0$, $p(0\,|0) = 10000I_n$, $\rho = 0.95$, $\beta = 1$. 仿真结果如图 2 所示. 图 2 (a) 给出了 Logistic 混沌映射状态的真实值与估计值, 为了清楚地表示 STF 算法的跟踪性能, 图 2 (a) 仅给出了对混沌映射估计的 50 步仿真. 图 2 (b) 给出了二进制信息符号的真实值与估计值. 由图 2 可知, 由于 STF 具有优良的跟踪能力, 所以对 Logistic 混沌映射的状态 $x(k)$ 跟踪良好, 被调制的信息符号 $s(k)$ 也非常精确地得到恢复.

图 3 给出了仿真过程中的 STF 算法的渐消因子 $\boldsymbol{\lambda}(k+1)$ 值的变化情况, 每当二进制信息符号发生变化时, 渐消因子 $\boldsymbol{\lambda}(k+1)$ 值会突增, 实时调整状态预报误差的协方差阵以及相应的增益阵, 从而保持超强的信息符号跟踪能力. 尤其是当刚开始滤波时, 由于初始状态设置的差异, 渐消因子 $\boldsymbol{\lambda}(k+1)$ 值特别大, 确保了对信息符号的快速跟踪.

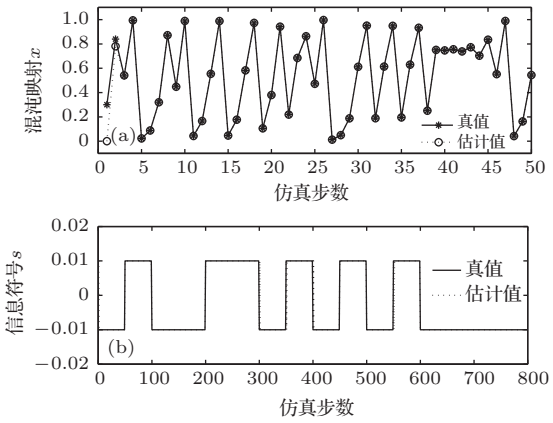

图 2 采用 ACM 和 STF 的混沌保密通信仿真 (a) 混沌映射; (b) 二进制信息符号

Fig. 2. The simulation of chaotic secure communication using ACM and STF: (a) chaotic mapping; (b) binary information symbols.

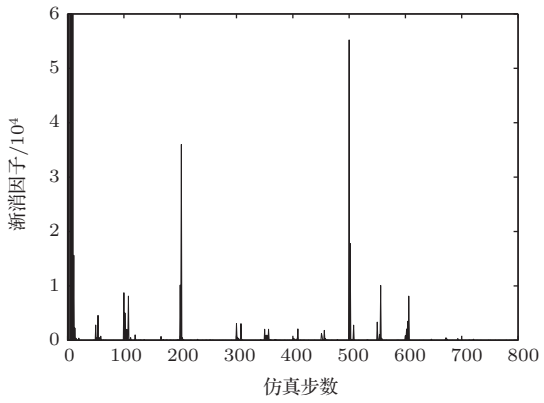

图 3 强跟踪滤波器中的渐消因子

Fig. 3. The fading factor of strong tracking filter.

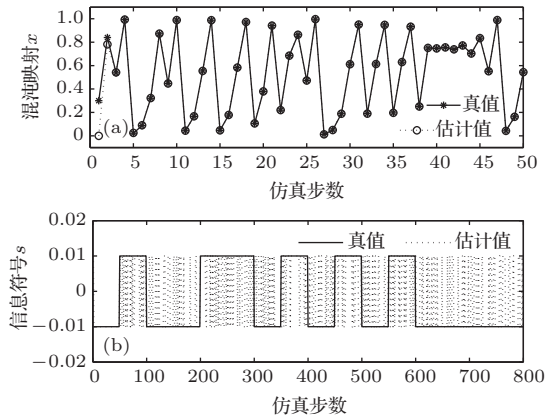

图 4 采用 ACM 和 EKF 的混沌保密通信仿真 (a) 混沌映射; (b) 二进制信息符号

Fig. 4. The simulation of chaotic secure communication using ACM and EKF: (a) chaotic mapping; (b) binary information symbols.

如果令次优渐消因子 $\boldsymbol{\lambda}(k+1) = \boldsymbol{I}_n$(单位矩阵), 则 STF 算法退化为 EKF 算法. 为了进行性能比较, 将带有信息符号估计的 EKF 算法也用于混沌保密通信, 仿真结果如图 4 所示. 由图 4 可知, 由于 EKF 对于离散的二进制信息符号跟踪能力差, 虽然对 Logistic 混沌映射的状态 $x(k)$ 跟踪良好, 但是, 被调制的信息符号 $s(k)$ 不能恢复, 即比特误码率大.

4.2 MCM 仿真

驱动信号 $y(k)$ 选为

$$y(k) = x(k) \times s(k) + v(k). \tag{29}$$

对于乘性混沌掩盖方案, 由于信息符号对系统混沌性质的影响较大, 二进制 θ_1, θ_2 的取值应更小一些, 所以取 $\theta_1 = 0.0001$, $\theta_2 = -0.0001$. 由于 θ_1, θ_2 取值小, 同观测噪声 $v(k)$ 的方差 R 也相应小些, 取 $R = 0.00005^2$. 混沌映射 (27) 式的初始状态 $x(0) = 0.2$; STF 算法的初值为: $\hat{x}(0\,|0) = 0$, $p(0\,|0) = 10000\boldsymbol{I}_n$, $\rho = 0.95$, $\beta = 1$. 图 5 (a) 给出了 Logistic 混沌映射状态的真实值与估计值, 为了清楚地表示, 图 5 (a) 仅给出了对混沌映射估计的 50 步仿真, 图 5 (b) 给出了二进制信息符号的真实值与估计值. 由图 5 可知, 估计值对真实值的跟踪良好, 这说明对于乘性混沌掩盖的混沌保密通信, STF 仍然具有优良的跟踪能力, 所以对 Logistic 混沌映射的状态 $x(k)$ 跟踪良好, 被调制的信息符号 $s(k)$ 也较精确地得到恢复.

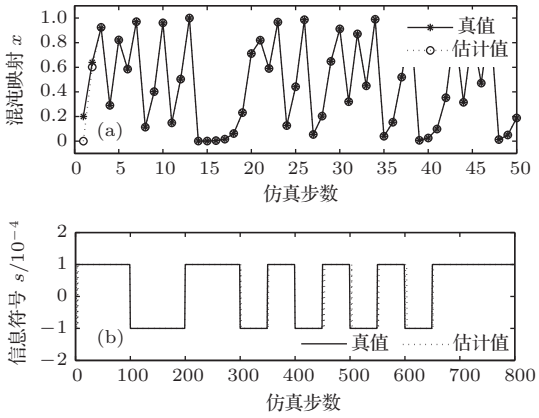

图 5 采用 MCM 和 STF 的混沌保密通信仿真 (a) 混沌映射; (b) 二进制信息符号

Fig. 5. The simulation of chaotic secure communication using MCM and STF: (a) chaotic mapping; (b) binary information symbols.

5 结 论

本文提出了一种基于 STF 算法解决混沌保密通信的方案, 并且根据混沌保密通信系统的特殊要

求, 提出了一种带有信息符号估计(贝叶斯分类器)的STF算法. 这种基于STF算法的混沌保密通信系统易于在线实现, 并且可以有效地处理驱动信号非线性的影响. 对Logistic混沌映射的数值仿真验证了STF算法有效性, 不管是加性混沌掩盖调制还是乘性混沌掩盖调制, STF算法均能实现混沌保密通信, 而且恢复信息符号的能力强于传统的卡尔曼滤波算法.

参考文献

[1] Hasler M 1998 *Int. J. Bifur. Chaos* **8** 647

[2] Feki M 2003 *Chaos Soliton. Fract.* **18** 141

[3] Liao T L, Huang N S 1999 *IEEE Trans. Circ. Syst. I* **46** 1144

[4] Grassi G, Mascolo S 1999 *IEEE Trans. Circ. Syst. I* **46** 1135

[5] Sobiski D J, Thorp J S 1998 *IEEE Trans. Circ. Syst. I* **45** 194

[6] Azou S, Burel G 2002 *IEEE Communications Conference* Bucharest, Romania, December 5–7, 2002 p123

[7] Zhang B, Chen M Y, Zhou D H 2006 *Chaos Soliton. Fract.* **30** 1273

[8] Wang S Y, Feng J C 2008 *J. Electron. Inform. Technol.* **30** 89 (in Chinese) [王世元, 冯久超 2008 电子与信息学报 **30** 89]

[9] Wang Y C, Zhao Q C, Wang A B 2008 *Chin. Phys. B* **17** 2373

[10] Cao L P, Xia G Q, Deng T, Lin X D, Wu Z M 2010 *Acta Phys. Sin.* **59** 5541 (in Chinese) [操良平, 夏光琼, 邓涛, 林晓东, 吴正茂 2010 物理学报 **59** 5541]

[11] Wei Y, Fan L, Xia G Q, Chen Y L, Wu Z M 2012 *Acta Phys. Sin.* **61** 224203 (in Chinese) [魏月, 樊利, 夏光琼, 陈于淋, 吴正茂 2012 物理学报 **61** 224203]

[12] Liu H J, Ren B, Feng J C 2012 *Chin. Phys. B* **21** 040501

[13] Zou L, Feng Y, Yang Y B, Wang A B, Yang L Z, Zhang J Z 2011 *Chin. Phys. B* **20** 094209

[14] Zhang J Z, Wang Y C, Wang A B 2008 *Chin. Phys. B* **17** 3264

[15] Li D J, Zhou Z F, Wu C M 2104 *J. Comput. Appl.* **34** 963 (in Chinese) [李杜娟, 周子峰, 吴成茂 2014 计算机应用 **34** 963]

[16] Chen M Y, Zhou D H, Shang Y 2006 *Int. J. Bifurc. Chaos* **16** 419

[17] Yan J, Wei Q Y 2013 *Comput. Technol. Develop.* **23** 199 (in Chinese) [严璟, 韦庆阳 2013 计算机技术与发展 **23** 199]

[18] Li G H 2014 *Appl. Res. Comput.* **31** 2788 (in Chinese) [李国华 2014 计算机应用研究 **31** 2788]

[19] Liu L Z, Zhang J Q, Xu G X, Liang L S, Wang M S 2014 *Acta Phys. Sin.* **63** 010501 (in Chinese) [刘乐柱, 张季谦, 许贵霞, 梁立嗣, 汪茂胜 2014 物理学报 **63** 010501]

[20] Yu F, Wang C H 2014 *Optics* **125** 5920

[21] Candido R, Soriano D C, Silva M T M, Eisencraft M 2015 *Signal Processing* **108** 412

[22] Zhou D H, Xi Y G, Zhang Z J 1990 *Control and Decision* **5** 1 (in Chinese) [周东华, 席裕庚, 张仲俊 1990 控制与决策 **5** 1]

A method of chaotic secure communication based on strong tracking filter*

Li Xiong-Jie[1)2)†] Zhou Dong-Hua[1)]

1) (*Department of Automation, Tsinghua University, Beijing 100084, China*)

2) (*Department of Electronic and Information Engineering, Zhejiang Business Technology Institute, Ningbo 315012, China*)

(Received 31 January 2015; revised manuscript received 9 March 2015)

Abstract

Chaotic secure communication is an active research field of chaotic application. A novel method for chaotic secure communication is proposed based on strong tracking filter (STF) in this study. STF is an extended Kalman filter with suboptimal fading factors, especially suitable for estimating the state and parameter of nonlinear time-varying stochastic systems. The main idea of the proposed method is summarized below. At the emitting end, the chaotic mapping and the information symbol are modeled as a nonlinear state space model, and the information symbol is modulated by additive chaos masking or multiplicative chaos masking and then is outputted through the channel. At the receiving end, the driving signal is received, and the message symbol is recovered dynamically by STF with Bayesian classifier. Simulation tests of the logistic chaotic mapping show that STF can restore the information symbols in chaotic signals when information symbols are binary code, with either additive or multiplicative chaos masking modulation. Compared with STF, the conventional Kalman filter has poor ability to track the discrete information symbol. It is difficult to restore the information symbols in the chaotic mapping, and the bit error rate is high. Therefore, the STF-based chaotic secure communication method is effective.

Keywords: secure communication, strong tracking filtering, chaos, message estimation

PACS: 05.45.Gg, 05.45.Vx, 84.40.Ua **DOI:** 10.7498/aps.64.140501

* Project supported by the National Nature Science Foundation of China (Grant No. 61210012).

† Corresponding author. E-mail: lixiongjie@tsinghua.org.cn