Chebyshev 映射混沌序列用于图像保密通信

Image Secure Communication Using Chebyshev-Map Chaotic Sequences

彭 军[1,2] 张 伟[1,3] 廖晓峰[1] 吴中福[1] 刘勇国[1] 李学明[1]

(重庆大学计算机学院 重庆400044)[1] (重庆工业高等专科学校计算机系 重庆400050)[2]

(重庆教育学院计算机与现代教育技术系 重庆400067)[3]

Abstract In this paper, two image secure communication schemes based on chebyshev-map chaotic sequences are proposed. The synchronization carrier signals can be retrieved directly from received signals in the first scheme, and the good correlation property of chaotic sequences is employed to realize secure communication in the second scheme. The results obtained by computer simulation indicate that the transmitted source image can be correctly and reliably recovered using each proposed scheme even under the situations of a noisy channel. In addition, the schemes proposed in this paper possess higher security and can be implemented easily. At last, the quality of recovered image is discussed through calculating bit-error rate, and the approximate relationship formula is also obtained respectively.

Keywords Chebyshev-map, Chaotic sequences, Synchronization, Statistical correlation, Image secure communication

1 引言

混沌是一种复杂的非线性动力学系统[1],混沌现象是非线性确定性系统中的一种类似随机的过程,由于对初值条件非常敏感,以及混沌序列具有类似噪声的宽频谱特性,近年来混沌用于保密通信成为人们关注的研究热点。特别是进入90年代,美国的 Pecora 和 Carroll[2,3]提出了关于混沌系统的自同步理论,使得这一课题的研究达到了高潮。

文[4]利用混沌实现了基于模拟电路的语音保密通信,文[5]利用混沌序列实现了直接序列扩频(DS/SS)通信系统,文[6]研究了一类时空混沌的同步问题并成功地将其应用于多用户扩频通信。本文我们则将研究如何利用混沌序列进行图像的保密传输。考虑到若采用模拟电路产生混沌信号,则要求收发两端的电路必须完全匹配,而实现这一点是很困难的,因此我们采用数字方法产生所需的离散时间混沌序列。本文采用低维的 Chebyshev 映射混沌系统,其定义如下

$$x_{n+1}=\cos(4\arccos(x_n)),\ -1\leqslant x_n\leqslant 1 \tag{1}$$

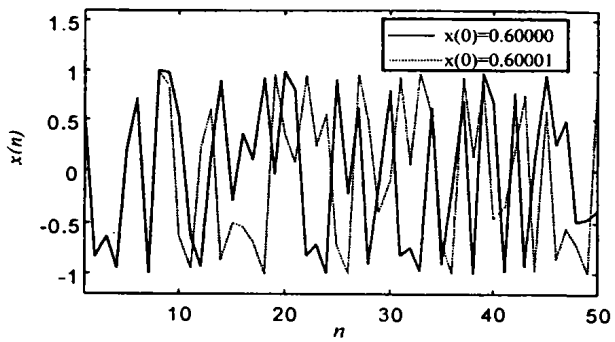

图1 不同初值条件下的系统演化曲线

图1为两条初值相差10^{-5}的系统演化曲线。从图中可看出,初值的微小差异将产生截然不同的混沌信号,这为产生数量众多的满足密码学要求的混沌伪随机序列提供了可能。

本文给出了两种通信方案用于图像保密通信,其中方案一可实现混沌自同步,即接收方根据混沌序列的发生规则直接从接收信号中提取混沌载波,然后恢复出原始信号;方案二则是针对混沌序列具有的优良相关特性而提出的。然后对两种方案进行了计算机仿真实验,结果表明本文给出的方案均能可靠地实现图像的保密通信,并借助误比特率对图像恢复质量进行了讨论。

2 基于混沌序列的图像保密通信

2.1 保密通信方案一

设$\{b_n\}$为需要发送的图像二进制信号,取值0和1。令:

$$x_{n+1}=f[g(x_n)+b_n] \tag{2}$$

$$x_{n+2}=f[g(x_{n+1})+b_{n+1}] \tag{3}$$

其中$g(x_n)$为 Chebyshev 映射,$f(x)=-\frac{1}{6}x^2+\frac{5}{6}x$。函数$f(x)$将区间$[-1,2]$非线性地映射到区间$[-1,1]$,目的是保证下次迭代点落在混沌区。

假设信道为理想信道,即没有噪声干扰,此时接收信号就是发送信号。设第n和$n+1$时刻的发送信号为$s_n=g(x_n)+b_n$,$s_{n+1}=g(x_{n+1})+b_{n+1}$,则经过简单推导就可得到第$n+1$时刻的原始信号为:

$$\tilde{b}_{n+1}=b_{n+1}=s_{n+1}-g(x_{n+1})=s_{n+1}-g[f(s_n)] \tag{4}$$

这种通信方案的优点是,传送的载波含有自同步信息,不需要额外的同步开销。接收方只根据前后两个接收信号s_n和s_{n+1},就可恢复出下一个原始信号b_{n+1},并且同步误差没有传播性,也就是说即使在某一时刻由于失步产生同步误差,但这不会影响以后的解码工作,说明这种自同步具有很高的可靠性。由于函数$f(x)$是非线性的,且有多种选取方法,加之原始信号的随机性,使得每次迭代初值都不同,并且这些迭代初值点构成的序列又不同于直接使用混沌映射产生的原始混沌序列。该方案不同于混沌参数调制,即使采用文[7]中的回归映射(return map)也难以重构混沌系统从而解码出原始信号。

彭 军 博士研究生,研究方向为网络安全,混沌保密通信等。张 伟 博士研究生,主要研究方向为远程教育,数据挖掘。廖晓峰 教授,博士后,主要研究方向为神经网络,数据挖掘。吴中福 教授,博士生导师,主要研究方向为远程教育,网络通信。

因此，通信的保密性能是相当高的。

2.2 保密通信方案二

我们知道，扩频通信中经常采用的基于线性反馈移位寄存器(LFSR)的线性码如 m-序列、Gold 码等尽管都具有良好的统计相关性，但安全性却很差。原因在于只需知道2n 个比特(n 为寄存器级数)的码元就能破译该系统[8]。而混沌序列则不同，由于混沌源和系统参数是保密的，使得任意截取一段序列，均不能预测出整个序列。加之 Chebyshev 映射混沌序列具有 δ-函数形式的自相关和零值互相关及序列数量众多(初值不同即可)等特点，因此用于保密通信具有更好的性能和安全性。图2给出了混沌序列的统计相关特性曲线。

下面我们给出的保密通信方案则利用了混沌序列的这种相关特性。设要传送的信息为 $b(k)\in\{0,1\}$，每一个信息比特分配 N 个序列码片。

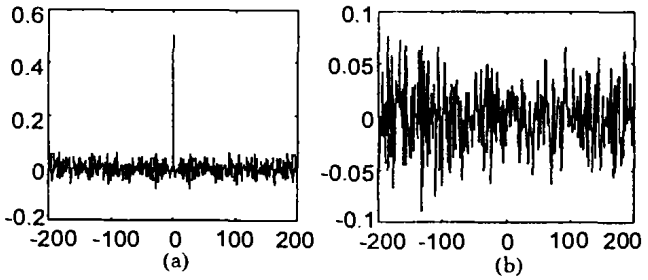

图2 序列的统计相关特性曲线 (a)初值为0.60000时混沌序列自相关曲线
(b)初值分别为0.60000和0.60001时两个混沌序列的互相关曲线

传输信号 $s(n)$做如下定义：

$$s(n)=\begin{cases}x(n), b(k)=1\\ -x(n), b(k)=0\end{cases} \tag{5}$$

其中 $n=1+(k-1)N,\cdots,kN; k=1,2,\cdots$，令 $\tilde{b}(k)=2b(k)-1$，则有

$$s(n)=\tilde{b}(k)x(n) \tag{6}$$

设信道噪声为 $w(n)$，则接收信号 $r(n)$为

$$r(n)=s(n)+w(n) \tag{7}$$

一般 $w(n)$取为零均值的 Gaussian 型白噪声。

在收发双方同步之后，就可以进行图像传输了。受计算精度的影响，因此我们首先给出信号 $r(n)$与 $x(n)$的非周期互相关函数表达式，定义如下：

1)如果$0\leqslant m<N$，$C_{r(n),x(n),k}(m)=\frac{1}{N}\sum_{i=1+(k-1)N}^{kN-|m|-1}(r(i)-\mu_r)(x(i)-\mu_x)$； (8a)

2)如果$1-N\leqslant m<0$，$C_{r(n),x(n),k}(m)=C_{r(n),x(n),k}(-m)$； (8b)

3)其余情况，$C_{r(n),x(n),k}(m)=0$。 (8c)

其中，$n=1+(k-1)N,\cdots,kN; k=1,2,\cdots,N$ 为码片长度，μ_r 为 $r(n)$的均值，μ_x 为 $x(n)$的均值。

由于混沌序列相关函数具有快速衰减特性，并且函数在相关间隔为零处时达到模极大值，因此接收方在收到信号 $r(n)$后，利用本地产生的同步混沌序列 $x(n)$计算 $C_{r(n),x(n),k}(0)$，然后根据下式进行判决，就可恢复出原始二进制信号 $\hat{b}(k)$。

$$\hat{b}(k)=\begin{cases}1, C_{r(n),x(n),k}(0)>0\\ 0, C_{r(n),x(n),k}(0)\leqslant 0\end{cases} \tag{9}$$

为了测试该通信方案的可行性，我们针对以下二进制序列作了预备实验

$b=\{1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1\}$

混沌映射初值选为0.60000，信道中加入了分布为 N(0, 0.05)的高斯白噪声。实验结果如图3所示。结果表明，收发双方使用相同初值均能进行正常通信，而初值的微小差异(实验中误差仅为10^{-5})都将导致错误的结果，并且由于两个不同混沌序列具有的零值互相关性，加之信道噪声的影响，使得相关曲线在相关间隔为零处的取值符号是随机的，因而每次得到的结果也是随机的。从本例可看出，根据混沌序列的相关特性原理进行信号检测是可行的也是可靠的，同时文中给出的算法具有很强的鲁棒性。

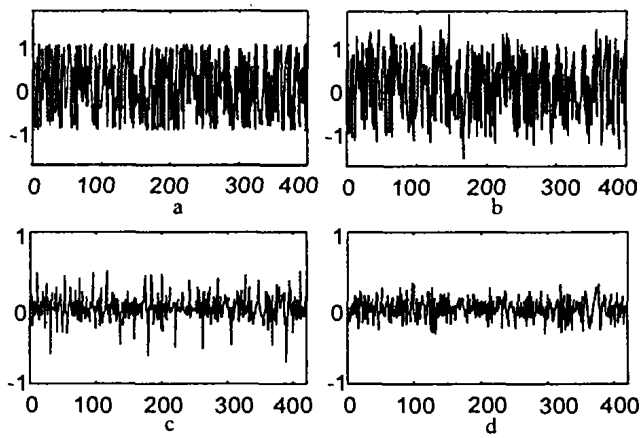

图3 (a)为发送信号 (b)为接收信号 (c)为接收方使用初值0.60000时得到的相关曲线
(d)为接收方使用初值0.60001时得到的相关曲线

图4是通信方案二的系统实现框图。图中 PN 为混沌系统产生的伪随机序列，$\tilde{b}(k)$为原始信号，$w(n)$为信道噪声，$\hat{b}(k)$为检测出的信号。收发两端通过一个同步信号进行同步，这样在经历一暂态后就可产生完全相同的混沌序列。关于该方案中混沌伪随机序列的同步问题，我们将另文报道。

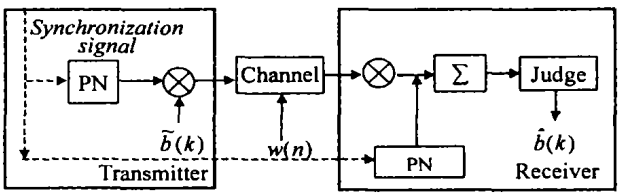

图4 基于 Chebyshev 映射的混沌通信系统框图

3 计算机仿真实验

对前面给出的两种保密通信方案分别进行了计算机仿真实验。图像选用大小为100×100的 Lenna 位图。图5为使用方案一并在不同信噪比情况下的实验结果。此处，信噪比 SNR (dB)计算公式如下：

$$SNR=10\log\left[\sum_{n=1}^{kN}(s(n)-\bar{s})^2/\sum_{n=1}^{kN}(w(n)-\bar{w})^2\right] \tag{10}$$

其中，$s(n)$为发送信号，$w(n)$为高斯噪声，$\bar{s}$ 和 $\bar{w}$ 分别是 $s(n)$和 $w(n)$的均值。

表1 使用通信方案一在不同信噪比下的误比特率

图5	(a)	(b)	(c)	(d)	(e)	(f)
SNR	43.6	36.7	33.7	26.7	23.7	16.7
BER	0	3.75E-5	1.20E-3	3.85E-2	6.96E-2	1.28E-1

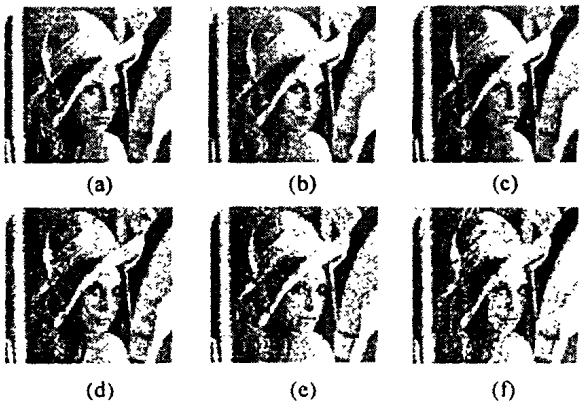

图5 使用通信方案一在不同信噪比情况下的实验结果

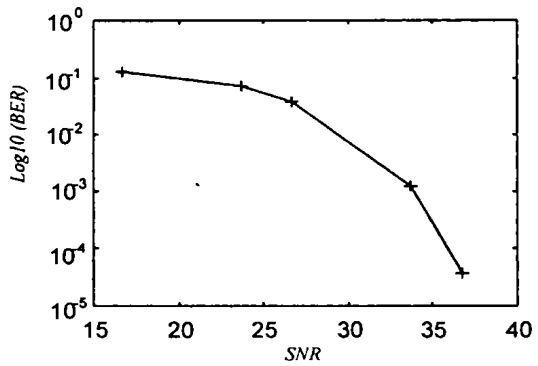

图6 误比特率 BER 与信噪比 SNR 之间的关系曲线

我们注意到，虽然方案一能够实现自同步通信，但对噪声却比较敏感。表1给出了不同信噪比情形下的误比特率（*BER*）。图6还给出了 *BER* 与 *SNR* 之间的关系曲线，对曲线进行拟合得到如下近似公式

$$BER(SNR)=a\exp(-b10^{SNR/10}) \tag{11}$$

其中 $a=0.1462$，$b=0.0030$。实验结果表明，在通信信道比较理想（如光纤）或信噪比较高（如 $SNR>35$）时，仍然是一种可靠的保密通信方案。

图7 使用通信方案二的实验结果

(a)和(b)为接收方使用相同初值时的恢复图像，(a)对应码片长度 N=6，(b)对应码片长度 N=10

(c)和(d)为接收方使用不同初值时的恢复图像，(c)对应初值0.61000，(d)对应初值0.60001

图7为使用方案二的实验结果。各参数取值如下：初值 $x_0=0.60000$，码片长度分别取 $N=2,4,6,8,10$。并在信道中加入了分布为 $N(0,0.05)$ 的高斯白噪声。结果表明，当通信双方取相同的参数值时，接收方能正确地恢复出原始图像。如果接收方的初值不同于发送方，得到的图像则面目全非，其误比特率接近于0.5。这说明通信方案二具有极好的保密性能，只要参数稍有差异，就不能正确地恢复信号，同时也说明收发双方的同步是非常关键的。表2给出了相应的实验数据。从表2我们发现，*BER* 与码片长度 *N* 有关，对于有固定信噪比的通信信道，增加码片的长度可降低误比特率，从而有效地提高图像恢复质量。图8是 *BER* 与 *N* 的关系曲线。通过曲线拟合，我们还得到它们之间的函数关系式：

表2 使用通信方案二在不同码片长度下的实验结果（SNR=10.09*dB*）

N	2	4	6	8	10
BER	1.07*E*-1	9.20*E*-3	1.20*E*-3	1.50*E*-4	2.50*E*-5

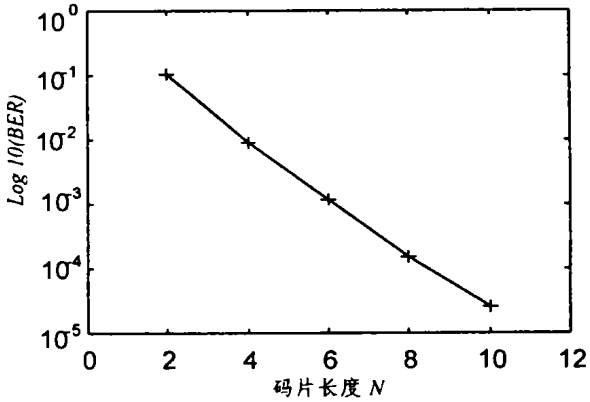

图8 码片长度 *N* 与误比特率 *BER* 的关系曲线

$$BER(N)=a10^{-bN} \tag{12}$$

其中 $a=1.2349$，$b=0.5311$。公式(12)表明，在信噪比固定的前提下，误比特率将随着码片长度的增大而以指数速率衰减。

结论 混沌在保密通信中具有非常广阔的应用前景，本文提出了基于混沌序列的两种方案用于图像保密通信。除此之外，通过增大码片长度，或采用超混沌系统的混沌序列，可进一步提高抗破译能力。本文提出的图像保密通信方案，同样可扩展到其他方面。如将不同的初值分配给不同的用户，以同时传输图像、语音、文本等内容，从而实现多用户的保密通信。

参 考 文 献

1 郝柏林. 从抛物线谈起——混沌动力学引论. 上海科技教育出版社，1993

2 Pecora L M, Carroll T L. Synchronization in chaotic systems. Phys. Rev. Lett.,1990, 64: 821～823

3 Pecora L M, Carroll T L. Driving systems with chaotic signals. Phys. Rev. A,1991, 44: 2374～2383

4 Cuomo K M, Oppenheim A V. Circuit implementation of synchronized chaos with applications to communication. Phys. Rev. Lett.,1993, 71(1): 65～68

5 Heidari-Bateni G, McGillem C D. A Chaotic Direct-Sequence Spread-Spectrum Communication System. IEEE transactions on communications, 1994, 42(2/3/4): 1524～1527

6 Xiao J H, Hu G, Qu Zhilin. Synchronization of Spatiotemporal Chaos and Its Application to Multichannel Spread-Spectrum Communication. Phys. Rev. Lett.,1996,77(20): 4162～4165

7 Pérez G, Cerdeira H A. Extracting Messages Masked by Chaos. Phys. Rev. Lett.,1995, 74(11): 1970 ～1973

8 王育民，刘建伟编著. 通信网的安全——理论与技术. 西安电子科技大学出版社，1999