



一种新型 FM-DCSK 保密通信系统

张 刚,王 源,王 颖

(重庆邮电大学信号与信息处理重庆市重点实验室 重庆 400065)

摘 要:为解决 DCSK 系统中混沌信号比特能量的不恒定会引起估计干扰从而造成误码率下降,同时该系统的传输速率较低,保密性较差这一问题。提出 FM 调制与改进型的 DCSK 系统相结合的方法,通过使用 FM 调制使混沌信号能量保持恒定从而提高了系统误码性能,同时结合使用两条信道的改进型 DCSK 的方案进一步提高系统传输效率以及系统安全性能。最后通过理论分析与仿真实验结果比较证明了改进后的系统相关性能得到极大提高。

关键词:混沌保密通信;调频调制;新型调频差分混沌键控

doi: 10.11959/j.issn.1000-0801.2015005

A Novel FM-DCSK Secure Communication System

Zhang Gang, Wang Yuan, Wang Ying

(Chongqing Key Laboratory of Signal and Information Processing,

Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: The bit energy of chaotic signals in DCSK system is not stable, which will cause the estimation interference and the bit error rate decline. At the same time, the system's transmission rate is lower and the security is poorer compared with other system. In order to solve these problems, a novel FM-DCSK secure communication system was proposed which was combined the FM modulation with the modified DCSK system. The bit energy of signals remained stable by using FM modulation so that the BER performance in such system can be improved. Meanwhile, the system was also combined with the modified DCSK system which uses two-channel scheme, therefore it can improve the transmission efficiency and further improve the security performance. Finally, the theoretical analysis and the simulation results prove that the relative performance in this proposed system can be greatly improved.

Key words: chaos secure communication, FM modulation, novel FM-DCSK

收稿日期:2014-06-30;修回日期:2014-09-05

基金项目:国家自然科学基金资助项目(No.61371164, No.61071196, No.61102131),教育部新世纪优秀人才支持计划基金资助项目(No.NCET-10-0927),信号与信息处理重庆市市级重点实验室建设基金资助项目(No.CSTC2009CA2003),重庆市杰出青年基金资助项目(No.CSTC2011jjq40002),重庆市自然科学基金资助项目(No.CSTC2010BB2398, No.CSTC2010BB2409, No.CSTC2010BB2411, No.CSTC2012JJA40008),重庆市教育委员会科研基金资助项目(No.KJ120525, No.KJ130524)

Foundation Items: The National Natural Science Foundation of China (No. 61371164, No.61071196, No.61102131), The Program for New Century Excellent Talents in University (No. NCET-10-0927), The Project of Key Laboratory of Signal and Information Processing of Chongqing (No. CSTC2009CA2003), The Chongqing Distinguished Youth Foundation (No. CSTC2011jjq40002), The Natural Science Foundation of Chongqing (No.CSTC2010BB2398, No.CSTC2010BB2409, No.CSTC2010BB2411, No.CSTC2012JJA40008), The Research Project of Chongqing Educational Commission(No.KJ120525, No.KJ130524)



1 引言

混沌信号作为一种非线性信号,其对系统初值的敏感导致信号具有不可预见性,同时其具有的内在随机行为以及宽带功率谱等特性使其在通信系统中发挥着重要的作用,尤其适用于保密通信系统。

Parlitz 等首先提出采用混沌键控技术^[1]应用于通信系统。键控技术主要根据接收端的不同分为两大类,分别为基于相干技术的混沌键控(CSK)^[2]和基于非相干解调的差分混沌键控(DCSK)^[3]。然而相干解调是基于同步技术,而混沌信号对初值的敏感性会使得在接收时重建混沌同步信号变得异常困难。但采用非相干解调技术的 DCSK 系统就不存在这样的问题,不需要在接收端采用复杂的同步装置。

DCSK 系统解决了 CSK 系统判决门限严重依赖 E_b/N_0 的问题,其接收端采用非相干调制技术简化了系统结构,是目前研究最多的一种混沌键控调制^[4]。但其存在保密性差和传输速率较低等缺陷,同时系统中的混沌信号的比特能量不恒定会引起估计干扰 ζ ,从而造成系统误码率提高的问题^[5]。针对这些问题,从两方面进行改进,首先把传统 DCSK 系统在一条信道传输信号改为在两条信道传输,并且把调制信息交叉到对方信道上传输,这样可以改善 DCSK 系统的保密性能和传输率。同时该方案又加入 FM 调制器到系统的发送端,这样会使混沌信号的比特能量保持恒定从而减小误码率,使方案更加完善。

2 DCSK 通信系统原理

DCSK 由 CSK 和 COOK 系统发展而来,它解决了和系统判决门限严重依赖于信噪比的问题。DCSK 系统发送端发送每一位信息的前半段信号作为参考信号,后半段携带传输的信息。根据参考信号与后一段信号相同或相反来判断发送的信息是“1”还是“-1”。由此可看到缺点比较明显,信号被截获后容易破解^[6],并且只使用一个信道导致信息传输效率低下^[7]。传统 DCSK 系统调制解调模型如图 1、图 2 所示。

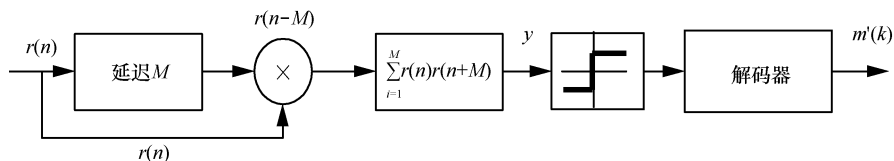


图 2 DCSK 系统解调原理

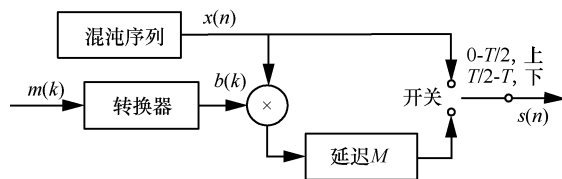


图 1 DCSK 系统调制原理

3 新型 FM-DCSK 调制原理

传统的 DCSK 只使用一条信道传输信号^[8],传输率和保密性不强,而经过改进后的 DCSK 同时采用两条信道进行传输,达到提高信道利用率和保密性能的目的。同时为了减小经过“混沌”扩频后的信息比特能量变化引起的估计干扰 ζ ,把频率调制与经过改进后的 DCSK 结合起来,有别于以前的系统,提出一种新型 FM-DCSK 通信系统,其原理如图 3 所示。

首先把经过 FM 调制过的信息同时通过两条信道传输信息每个周期先传输参考信号,随后把得到的信号分别放到对方信道上,这样就把参考信号和经过调频后信息相互分离到不同的信道中进行传输,即使拦截到其中任意一条信道的信息也无法破译。

新型 FM-DCSK 通信系统中接收端采用非相干解调方式来恢复信号。每个混沌映射在每个比特时间周期 $[t_i, t_i+T]$ 内发送 $2M$ 个混沌离散样值。各自先发送长为 M 的混沌序列 x_1 、 x_2 作为参考信号,随后在发送端将待传输的信息 m_i 经过串并转换后变成两路双极性信号 $b_{1,k}$ 和 $b_{2,k}$,分别与两路先经过 FM 调制随后延迟 M 时间的混沌信号 $x_{1,n-M}$ 和 $x_{2,n-M}$ 进行相乘,之后得到 $b_{1,k} x_{1,n-M}$ 和 $b_{2,k} x_{2,n-M}$ 。为了达到保密的目的,需把经过调制的两组信号交换,随后得到各自信息比特信号 $s_{1,n}$ 和 $s_{2,n}$ 。

两条信道输出信息比特 $s_{1,n}$ 和 $s_{2,n}$ 为:

$$s_{1,n} = \begin{cases} x_{1,n} & , 0 < n \leq M \\ b_{2,k} x_{2,n+M} & , M < n \leq 2M \end{cases} \quad (1)$$

$$s_{2,n} = \begin{cases} x_{2,n} & , 0 < n \leq M \\ b_{1,k} x_{1,n+M} & , M < n \leq 2M \end{cases} \quad (2)$$

在接收端,接收到的信号首先进行信息的交换:每个比特时间周期 T 内,前 $T/2$ 取 $r_{1,n}$ 和 $r_{2,n}$ 的前 M 位,后 $T/2$

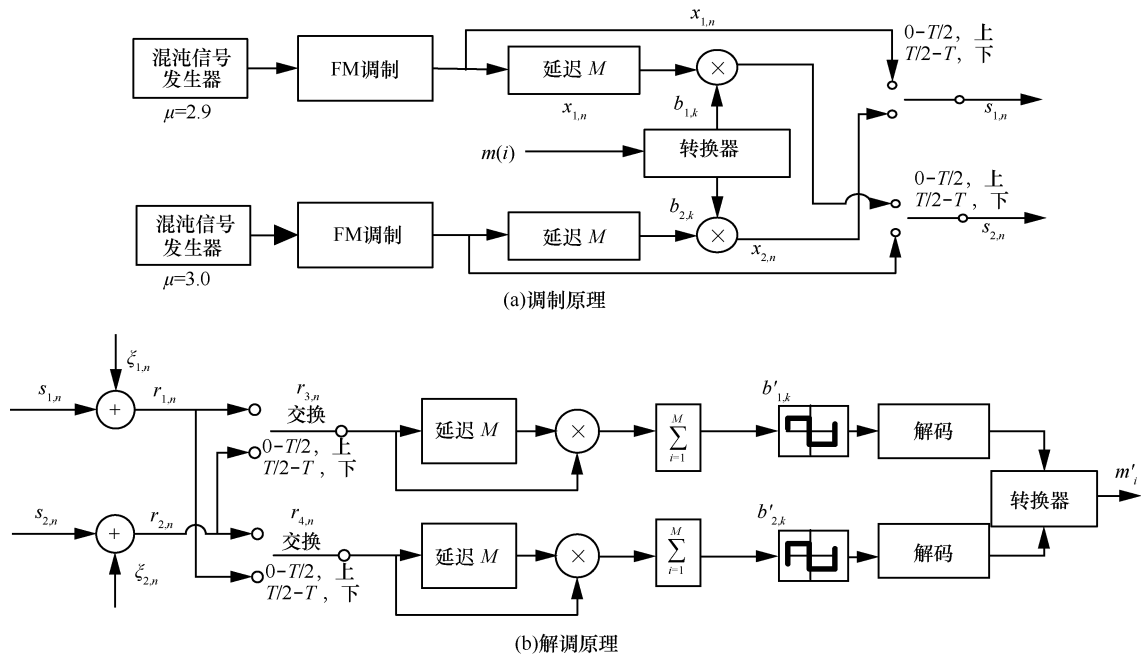


图3 新型 FM-DCSK 调制解调原理

取 $r_{1,n}$ 和 $r_{2,n}$ 的后 M 位并交换信道后,随后送到相关器恢复码元信息。 $r_{k,n}=s_{k,n}+u_{k,n}$ ($k=1,2$), $u_{k,n}$ 代表零均值加性高斯白噪声(AWGN)。在接收端合并后的序列为:

$$r_{3,n} = \begin{cases} r_{1,n}, & 1 < n \leq M \\ r_{2,n}, & M < n \leq 2M \end{cases} \quad (3)$$

$$r_{4,n} = \begin{cases} r_{2,n}, & 1 < n \leq M \\ r_{1,n}, & M < n \leq 2M \end{cases} \quad (4)$$

在这里计算第一路相关器输出表达式为:

$$\begin{aligned} S &= \sum_{n=1}^M r_{3,n} r_{3,n+M} \\ &= \sum_{n=1}^M (s_{1,n} + u_{1,n})(b_{1,l} s_{2,n+M} + u_{2,n+M}) \\ &= \sum_{n=1}^M (x_{1,n} + u_{1,n})(b_{1,l} x_{1,n+M} + u_{2,n+M}) \\ &= b_{1,l} \sum_{n=1}^M x_{1,n}^2 + \sum_{n=1}^M [x_{1,n} u_{2,n+M} + b_{1,l} x_{1,n+M} u_{1,n}] + u_{1,n} u_{2,n+M} \end{aligned} \quad (5)$$

r_3 代表接收端经过转换后的信号,则相关器的输出可写为:

$$S = b_{1,l} A + b_{1,l} \zeta + \eta, A > 0 \quad (6)$$

其中, $A = E[x_{1,n}^2]M$ ($E[\cdot]$ 表示求均值) 代表所携带的信息, $\zeta = \sum_{n=1}^M x_{1,n}^2 - A$ 是由每比特能量所引起的干扰项^[9], 而式(7)是信道噪声产生的干扰项,并且均值为0:

$$\eta = \sum_{n=1}^M x_{1,n} u_{2,n+M} + b_{1,l} \sum_{n=1}^M x_{1,n+M} u_{1,n} + \sum_{n=1}^M u_{1,n} u_{2,n+M} \quad (7)$$

针对 DCSK 系统, $A = E_b/2$, $E_b = E[\sum_{n=1}^M x_{1,n}^2]$ 表示信号能量。 η 代表噪声, ζ 表示经过“混沌”扩频后引起的信息比特能量变化而导致的估计干扰^[10]。当 N 逐渐增加时, $\eta\zeta$ 逐渐趋于高斯分布^[11], 在这里需要确定 $\eta+\zeta$ 的均值与方差。对于任意正整数 $i, j, i \neq j$, u_i, u_j 统计独立, u_1, u_2 的方差分别为 σ_1^2, σ_2^2 , N_1, N_2 分别是两信道噪声平均功率, 可得 $\sigma_1^2 = E[u_{1,n}^2] = N_1/2, \sigma_2^2 = E[u_{2,n}^2] = N_2/2$ 。由此得到 $\eta\zeta$ 的均值 $E[\eta\zeta] = 0$ 。因为 η, ζ 之间相互独立, 从而由两者间的不相关就知道了 η, ζ 之间的协方差为0, 同时由 η, ζ 相互独立可得 $\sigma_{\zeta+\eta}^2 = \sigma_{\zeta}^2 + \sigma_{\eta}^2, \sigma_{\zeta+\eta}^2$ 为 $\eta+\zeta$ 方差。 η 的方差表达式为:

$$\begin{aligned} \sigma_{\eta}^2 &= E\left[\sum_{n=1}^M x_{1,n}^2\right](\sigma_1^2 + \sigma_2^2) + M\sigma_1^2\sigma_2^2 \\ &= \frac{E_b(N_1 + N_2)}{4} + \frac{MN_1N_2}{4} \end{aligned} \quad (8)$$

为了讨论方便, 假设两条信道噪声条件一致, 这样 $N_0 = N_1 = N_2$, 可得到:

$$\sigma_{\eta}^2 = \frac{E_b N_0}{2} + \frac{MN_0^2}{4} \quad (9)$$

σ_{ζ}^2 是由“混沌”引起的比特能量变化造成的干扰 ζ 的方差, 与具体采用的混沌映射类型相关。当采用 logistic 混



沌映射时,其估计干扰 ζ 的方差较小,为 $\sigma_{\zeta}^2=E_b^2/(8M)^{[12]}$ 。而当改进型 DCSK 保密通信系统加入 FM 调制器后,系统会将振幅随机变化的混沌信号变为频率随机变化而振幅恒定的信号,从而使每比特混沌信号能量保持恒定,同时干扰项 $\zeta=\sum_{n=1}^M x_{k,n}^2-A$ 忽略不计,混沌调幅变成混沌调频。从而可以得到:

$$\sigma_{\zeta+\eta}^2=\sigma_{\zeta}^2+\sigma_{\eta}^2=\frac{E_b N_0}{2}+\frac{N_0^2}{4}M \quad (10)$$

故新型 FM-DCSK 的误码率为:

$$P_e=P((\zeta+\eta)>A)=\frac{1}{2}\operatorname{erfc}\left(\frac{A}{\sqrt{2\sigma_{\zeta+\eta}^2}}\right) \quad (11)$$

$$P_e=\frac{1}{2}\operatorname{erfc}\left(\sqrt{\frac{E_b}{4N_0}\left(1+\frac{N_0}{2E_b}M\right)^{-1}}\right) \quad (12)$$

作为对比,传统 DCSK 系统在 AWGN 信道中的误码率为^[13]:

$$\begin{aligned} BER &= \frac{1}{2}\operatorname{erfc}\left[\left(\frac{1}{M}+\frac{4N_0}{E_b}+2M\frac{N_0^2}{E_b^2}\right)^{\frac{1}{2}}\right] \\ &= \frac{1}{2}\operatorname{erfc}\left[\sqrt{\frac{E_b}{4N_0}\left(1+\frac{1}{4M}\frac{E_b}{N_0}+M\frac{N_0}{2E_b}\right)^{\frac{1}{2}}}\right] \end{aligned} \quad (13)$$

对两种误码率计算式进行简单对比可以发现,新型的 FM-DCSK 系统的误码率性能比传统 DCSK 系统有提升,并且通过模型简单分析可得出传输的性能由于采用了两条信道,也得到翻倍的提升,传输速率是以前的两倍。下面将通过仿真来验证相关结论。

4 仿真结果

根据推导出来的结果,对 DCSK 系统和新型 FM-DCSK 系统进行仿真。在仿真模型当中,本文采用 Logistic 映射作为混沌序列信号源。从图 1 可以看到两个信号源采用不同的 Logistic 映射调节参数值,分别为 $\mu_1=2.9$ 、 $\mu=3.0$ 。采用的 Logistic 映射方程为:

$$x_{k,n}=\mu_k x_{k,n}(1-x_{k,n}^2), k=1,2 \quad (14)$$

图 4 显示了新型 FM-DCSK 系统与传统 DCSK 系统的误码率随 E_b/N_0 的变化。从图中可以看到当信噪比低于 5 dB 时,两者性能相当,随着 E_b/N_0 的增大,两者的性能差距逐

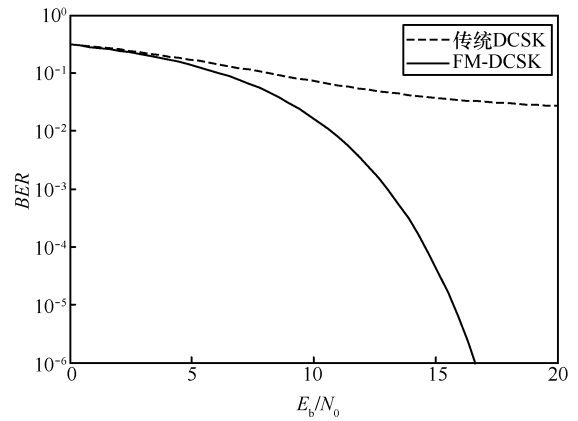


图 4 改进型 FM-DCSK 与 DCSK 误码率比较

渐拉大,新型 FM-DCSK 系统表现出的性能要好于 DCSK 系统。这是由于当 E_b/N_0 值较小时,混沌序列产生的比特能量变化被功率较大的噪声所掩盖;而随着信噪比增大,信道噪声不再成为主要影响系统性能的因素,相反比特能量不均衡引起的方差对系统性能产生较大的影响。可见对改进型 DCSK 进行 FM 调制的效果十分明显。

图 5 显示的是新型 FM-DCSK 与 DCSK 误码率比较,从图中可以看到,随着 E_b/N_0 的增加,误码率在逐渐降低。同时随着 M 值的递增,误码率性能也在逐渐下降,说明不能无限扩大扩频系数 M 。通过理论分析可知 M 的增大会使系统的传输速率下降,所以合理选择一个 M 值非常重要,应尽量选择小一些的值。

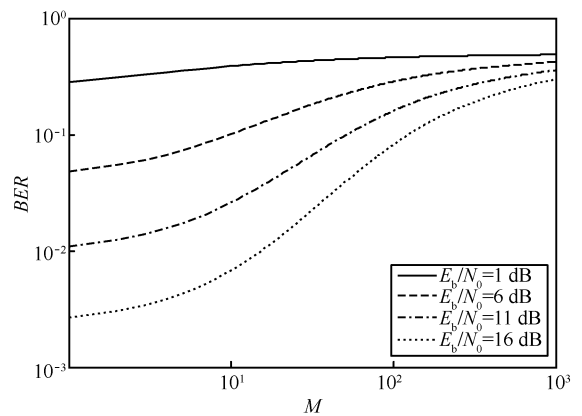
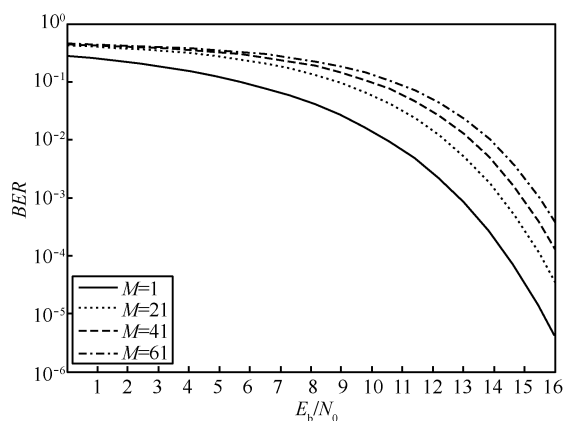


图 5 不同信噪比下改进型 FM-DCSK 与 DCSK 误码率比较

图 6 显示不同扩频系数 M 下的误码性能仿真。当 M 值较大且不高时,系统的性能差别不大。只有当逐渐提高了, M 值越小的系统性能才越好。当 $M=1$ 时系统性能最好。

图 6 不同 M 值下 FM-DCSK 系统性能

5 结束语

目前对 DCSK 的研究很多,目的是克服其自身的种种缺点以及发挥它潜在的优势,本文通过改进 DCSK 系统的结构提升其系统性能,通过加入 FM 调制克服混沌信号的信息比特能量变化而导致的估计干扰,同时引入两条信道来提升系统的有效性和提高系统安全性。

当然本设计的缺点是相对于传统的 DCSK 系统复杂程度较高,对于接收端对信号的检测和信号的分离提出了较高的要求。而且本设计只是针对较为简单的信道进行分析,可以在以后进行更多信道类型研究。

经过改进后的 DCSK 系统较传统系统有明显的优越性,在系统保密性方面有着天然的优势,同时可改善通信系统的有效性以及误码性能,因此在无线传输、军事和无线通信等领域有着极为广泛的应用潜力。

参考文献

- 1 Dedieu H, Kennedy M P, Hasler M. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *Circuits and Systems II: IEEE Transactions on Analog and Digital Signal Processing*, 1993, 40(10):634~642
- 2 孔龙,陈平平,徐位凯等. FM-DCSK UWB 技术在无线体域网中的性能分析. *重庆邮电大学学报*, 2013, 25(2):265~269
Kong L, Chen P P, Xu W K, *et al.* Performance of FM-DCSK UWB for body area network. *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)*, 2013, 25(2): 265~269
- 3 陈志贵, 徐位凯. CS-DCSK 在 Nakagami-m 衰落信道下的性能分析. *重庆邮电大学学报*, 2012, 24(4):395~399
Chen Z G, Xu W K. Performance analysis of CS-DCSK over Nakagami-m fading channels. *Journal of Chongqing University of*

Posts and Telecommunications (Natural Science Edition), 2012, 24(4): 395~399

- 4 Yang H, Jiang G P. Reference modulated DCSK: a novel chaotic communication scheme. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2013, 60(4):232~236
- 5 Yang H, Jiang G P. High-efficiency differential-chaos-shift-keying scheme for chaos-based noncoherent communication. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2012, 59(5): 312~316
- 6 Xu W, Wang L, Chen G. Performance analysis of the CS-DCSK/BPSK communication system. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2014, 61-1(9): 2624~2633
- 7 Lee D H, Jeong B J. Performance analysis of combining space-time block coding and scheduling over arbitrary Nakagami fading channels. *IEEE Transactions on Wireless Communications*, 2014, 13(5): 2540~2551
- 8 仇洪冰, 王玫. FM-EDCSK 系统性能分析. *通信学报*, 2005, 26(5):113~117
Qiu H B, Wang M. Analysis of the system character of FM-EDCSK. *Journal on Communications*, 2005, 26(5):113~117
- 9 Xia Y X, Tse C K, Lau F C M. Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2004, 51(12): 680~684
- 10 Kaddoum G, Charge P. Performance analysis of differential chaos shift keying over an AWGN channel. *IEEE International Conference on Advances in Computational Tools for Engineering Applications*, 2009(7): 255~258
- 11 Kolumban G, Kennedy M P, Chua L O. The role of synchronization in digital communications using chaos-part II chaotic modulation and chaotic synchronization. *IEEE Trans Circuits Syst Part I: Fundamental Theory and Applications*, 1998, 45(11): 1129~1140
- 12 Deng Y K, Hu Y H, Geng X P. Randomness enhancement using digitalized modified logistic map. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2010, 57(12):996~1000
- 13 Sushchik M, Tsimring L S, Volkovskii A R. Performance analysis of correlation-based communication schemes utilizing chaos. *IEEE Transactions on Circuits and Systems I*, 2000, 47(12): 1684~1691

[作者简介]



张刚,男,博士,重庆邮电大学副教授,主要研究方向为混沌同步、混沌保密通信等。

(2015005-6 接排在 2015044-7 后)