



一种改进的 DCSK 保密图像传输方案^{*}

贺利芳, 张 刚, 张天骐

(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: 差分混沌键控(DCSK)采用非相干解调技术,不必在接收端生成混沌同步信号,结构简单,并具有很好的抗噪性能,但保密性不足,较易破解。针对 DCSK 保密性差的问题,提出了一种改进的 DCSK 方案,在保证其性能的同时大大提高保密性。且对此系统进行了深入的理论分析,对误码率、扩频系数和信噪比之间的关系进行了深入研究,并将其运用到图像保密传输中,通过仿真验证该方案的可行性。仿真结果表明,改进的 DCSK 系统在误码性能和保密性上都较原系统有极大提高,因此对实际应用具有重大意义。

关键词: 差分混沌键控;调制;误码率

doi: 10.3969/j.issn.1000-0801.2013.06.015

A Secure Image Transmission Scheme Based on Improved DCSK

He Lifang, Zhang Gang, Zhang Tianqi

(Chongqing Key Laboratory of Signal and Information Processing, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: Non-coherent demodulation technology is applied in the differential chaos shift keying (DCSK) and it's unnecessary for the receiver to generate chaotic synchronous signals at the receiving end. The structure in DCSK is simple and has good performance in anti-noise. However, it is lack of performance in security, and easier to be cracked. A modified DCSK scheme was proposed for the security problems caused by the traditional DCSK scheme. It retains the good performance of the old one and greatly increases security performance at the same time. The theoretical analysis toward the system was deeply carried out. The relationship among the BER, the frequency spread factor and SNR were also deeply analyzed. Finally, it was applied in an image transmission system as an example. The simulation results indicate that the performance of the bit error ratio (BER) and security are greatly improved. The feasibility was also proved by simulations.

Key words: differential chaos shift keying, modulation, bit error ratio

1 引言

混沌键控调制技术具有较强的抗噪声干扰和参数适配的能力,功率谱密度较低、简单易实现,因此广泛应用于

数字保密通信系统^[1]。1992 年,Parlitz 等率先提出了混沌键控技术^[2],其基本原理是在发送端用混沌信号调制数字信号。Dedieu H 和 Kennedy M P 最早提出了混沌移位键控(CSK)^[3]技术,其思想是用不同的混沌信号对数字信号调

^{*} 国家自然科学基金资助项目(No.61071196, No.61102131),教育部新世纪优秀人才支持计划资助项目(No.NCET-10-0927),信号与信息处理重庆市市级重点实验室建设项目(No.CSTC2009CA2003),重庆市杰出青年基金资助项目(No.CSTC2011jjjq40002),重庆市自然科学基金资助项目(No.CSTC2010BB2398, No.CSTC2010BB2409, No.CSTC2010BB2411, No.CSTC2012JJA40008)和重庆市教育委员会科研项目(No.KJ120525, KJ130524),国家留学基金资助项目

制后发送,在接收端采用相干或非相干解调,判断出原始信号。在 CSK 的基础上, Kolumban G 和 Kennedy M P 又进一步提出了混沌开关键控(COOK)^[4]技术。CSK 和 COOK 技术在接收端的门限判决要根据信噪比的变化而变化,否则系统会有较高的误码率,使性能降低。为解决这一问题, Kolumban G 等又提出了基于非相干解调的差分混沌键控(different chaos shift keying, DCSK)^[5]技术,该方法容易实现,且在信噪比上有所改善。此后出现的调频差分混沌键控(FM-DCSK)^[6]技术是为克服符号能量的变化,先将混沌信号进行频率调制,从而使信号能量保持恒定。由于 DCSK 的结构比 FM-DCSK 简单,因而在此仅讨论 DCSK 系统。Kolumban G 等在参考文献[7]中提出的方法避免了估值误差,但要求在接收端有时延网络和良好的同步特性。刘剑波、叶春飞等在参考文献[8]中把混沌多相序列引入 DCSK 系统中,解决了信号本身带来的估值误差问题,提高了系统性能。张刚、张天骐等在参考文献[9,14,15]中对 DCSK 应用于图像传输的误码性能做了进一步的研究。

现有的混沌键控系统中,差分混沌键控具有最好的健壮性和误码性能^[10],但在实际应用中存在保密性问题^[11]。由于 DCSK 在一个码元周期中,发送端发送的参考信号和信息信号相同或相反,通过观察传输信号的频谱,很容易得到系统的比特率,中途被截获后易于破解出原始信息,因此很难达到高保密性。

2 改进的 DCSK 系统方案

针对上述情况,提出了一种改进的 DCSK 系统,如图 1 所示,其保密性得到了极大增强,不易被破解,并且误码性能也有所提高,其调制和解调部分原理如图 2 所示。

传统 DCSK 系统中,参考信号和调制信号在一条信道上传输;改进系统在原有 DCSK 基础上引入了一条信道,使参考信号和已调信号分别在两条信道中传输。调制时,一条信道传输混沌参考信号 x_n ,另一条信道传输式(1)的已调信号 s_n ,前半部分为迷惑信号,后半部分为 CSK 信号。

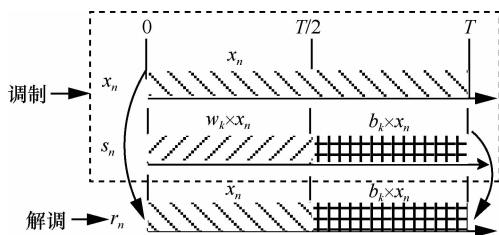
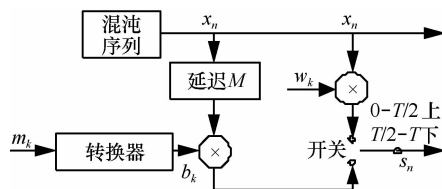
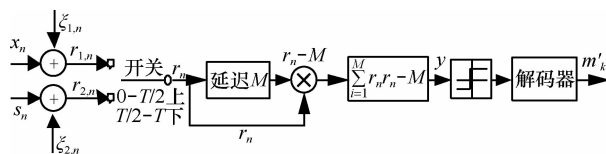


图 1 改进 DCSK 系统调制示意图



(a) 调制原理



(b) 解调原理

图 2 DCSK 系统调制解调原理

其中, x_n 是混沌信号, w_k 是随机信号, b_k 是双极性信号, M 是扩频系数, 即每个符号用 M bit 混沌信号调制, R_n 表示长度为 M 的门函数。解调时, x_n 和 s_n 同时传输到接收端后,在前一个 $T/2$,取混沌信号 x_n 的前 M 位,在后一个 $T/2$,取 s_n 的后 M 位,然后将两个序列合并为一个序列 r_n ,如式(2),其中 T 为一个码元周期。可看出,该序列和传统 DCSK 序列恢复一致,从而可以用相关解调法成功解调。这样,信息在传输过程中分散在两条信道上,且采用了混沌信号传输,频谱得到扩展,保密性得到极大增强。即使监听者截获到 s_n 序列,经过分析解码后恢复的也是随机信号 w_k ,这样,就能够实现完全的保密通信。接收到的信号为 $r_{1,n} = x_n + \xi_{1,n}$, $r_{2,n} = w_k x_n \cdot R_n + b_k x_{n-M} \cdot R_{n-M} + \xi_{2,n}$, 其中, $\xi_{1,n}$, $\xi_{2,n}$ 为信道噪声,合并后的序列如式(2)所示。假设 ξ_n 是一个固定的随机过程且均值为 0,服从高斯白噪声分布,且 $i \neq j$,则 $\xi_{i,n}$ 和 $\xi_{j,n}$ 是统计独立的,这样就能保持很好的位同步和相干性。那么,相关器的输出如式(3)所示。在式(3)中,第 1 项是有用的信号,第 2 项是均值为 0 的随机量,则 y_k 和 b_k 的极性一致,即可判断 m'_k 如式(4)所示。

$$s_n = w_k x_n \cdot R_n + b_k x_{n-M} \cdot R_{n-M} \quad (1)$$

$$r_n = r_{1,n} \cdot R_n + r_{2,n} \cdot R_{n-M} \quad (2)$$

$$\begin{aligned} y_k &= \text{cor}_M(r_n) \\ &= \text{cor}_M(r_{1,n}, r_{2,n}) \\ &= \sum_{n=1}^M r_{1,n} r_{2,n+M} \\ &= \sum_{n=1}^M (x_n + \xi_{1,n})(b_k x_n + \xi_{2,n+M}) \\ &= b_k \sum_{n=1}^M x_n^2 + \sum_{n=1}^M [x_n(\xi_{2,n+M} + b_k \xi_{1,n}) + \xi_{1,n} \xi_{2,n+M}] \quad (3) \end{aligned}$$



$$m'_k = \begin{cases} 1, & \exists y > 0 \\ 0, & \exists y < 0 \end{cases} \quad (4)$$

3 改进的 DCSK 系统性能

改进 DCSK 系统的输出可表示成:

$$y_k = b_k A + b_k \zeta + \eta, \quad \forall A > 0 \quad (5)$$

其中, $A = \langle x_n^2 \rangle M$, $\langle * \rangle$ 代表自相关函数, $\zeta = \sum_{n=1}^M x_n^2 - A$,

$$\eta = \sum_{n=1}^M x_n \xi_{2,n+M} + b_k \sum_{n=1}^M x_n \xi_{1,n} + \sum_{n=1}^M \xi_{1,n} \xi_{2,n+M} \circ$$

对于 DCSK 系统, $A = E_b/2$ 。

在混沌系统中, 混沌信号 x_n 与 x_{n+M} 之间的相关性随着 M 的增大快速衰减。假设 M 远大于相关特征衰减时间, 则随着 M 的增加, ζ 和 η 更接近于高斯分布^[12]。由于在任何 (i, j) 条件下, x_i 统计独立于第 j 个噪声信号 ξ_j , 并且在任何 $i \neq j$ 条件下, ξ_i 和 ξ_j 也是统计独立的, ζ 和 η 的互相关性为 0, 由此可得, $\sigma_{\eta\zeta}^2 = \sigma_\eta^2 + \sigma_\zeta^2$ 。同理, η 中的各项间的互相关性也为 0, 所以 η 的方差为:

$$\begin{aligned} \sigma_\eta^2 &= \sum_{n=1}^M x_n^2 \sigma_1^2 + \sum_{n=1}^M x_n^2 \sigma_2^2 + \sigma_1^2 \sigma_2^2 M \\ &= \frac{1}{2} E_b \sigma_1^2 + \frac{1}{2} E_b \sigma_2^2 + \sigma_1^2 \sigma_2^2 M \\ &= \frac{1}{4} E_b N_1 + \frac{1}{4} E_b N_2 + \frac{1}{4} N_1 N_2 M \end{aligned} \quad (6)$$

其中, σ_1^2 为 ξ_1 的方差, σ_2^2 为 ξ_2 的方差, N_1, N_2 分别为两个信道的噪声平均功率谱密度, 因此有 $\sigma_1^2 = N_1/2$, $\sigma_2^2 = N_2/2$ 。 ζ 的方差取决于采用何种混沌映射, 在此采用 Logistic 混沌映射产生混沌信号, 如式(7)所示:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (7)$$

Schuster^[13] 给出了 Logistic 映射的概率密度函数, 如式(8)所示:

$$\rho(x) = \begin{cases} \frac{1}{\pi \sqrt{1-x^2}}, & x \in (-1, 1) \\ 0, & \text{其他} \end{cases} \quad (8)$$

通过计算 ζ 的方差, 可得 $\sigma_\zeta^2 = M/8 = E_b^2/8M$, 进而可计算出 $\eta + \zeta$ 的方差, 如式(9)所示:

$$\sigma_{\eta+\zeta}^2 = \frac{E_b^2}{8M} + \frac{1}{4} E_b N_1 + \frac{1}{4} E_b N_2 + \frac{N_1 N_2}{4} M \quad (9)$$

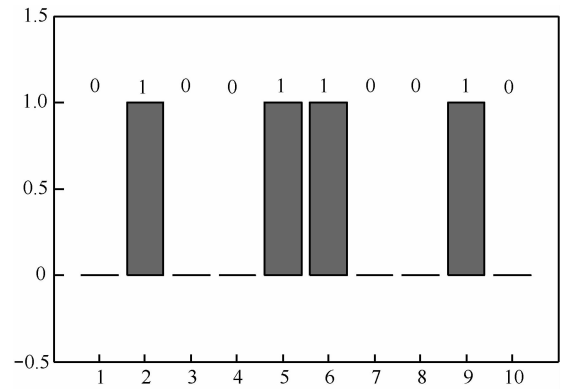
所以, 改进 DCSK 系统的误码率式可写为:

$$\begin{aligned} BER &= P((\zeta + \eta) > A) = \frac{1}{2} \operatorname{erfc}\left(\frac{A}{\sqrt{2\sigma}}\right) \\ &= \frac{1}{2} \operatorname{erfc}\left[\left(\frac{1}{M} + 2 \frac{N_1 + N_2}{E_b} + 2M \frac{N_1 N_2}{E_b^2}\right)^{-\frac{1}{2}}\right] \end{aligned} \quad (10)$$

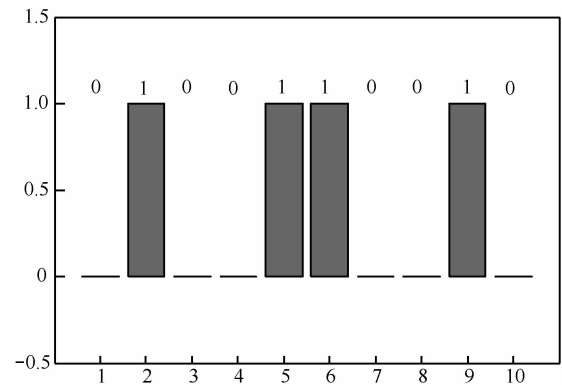
其中, $\operatorname{erfc}(x)$ 为补误差函数, 即 $\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty \exp(-t^2) dt$ 。

4 仿真结果及性能分析

采用 Logistic 混沌序列, 初值 $x_1=0.11$, $\mu=3.5$, 并做 50 次迭代后产生混沌信号作为载波对原始信号进行调制。假设要传输的原始信号为 $m_k=\{0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0\}$, 则经过变换后的双极性信号为 $b_k=\{-1 \ 1 \ -1 \ -1 \ 1 \ 1 \ -1 \ -1 \ 1 \ -1\}$, 并令扩频系数 $M=50$ 。模拟在无线信道中传输过程, 假设信道噪声服从 AWGN 分布, 则得到原始信号和经过解调后的信号如图 3 所示, 两者一致。而经过传统 DCSK 系统调制和改进 DCSK 系统调制之后的信号如图 4 所示, 可看出, 经过传统 DCSK 系统调制的信号, 具有很强的规律性, 每隔半个码元周期, 信号会发生重复或者反向重复, 若被截获, 很容易破译; 而经过改进 DCSK 系统调制的信号, 虽会重复, 但前半个码元周期的参考信号被加权了 w_k , 即使

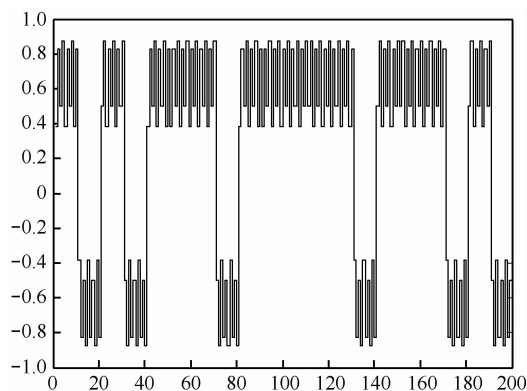


(a) 原始信号

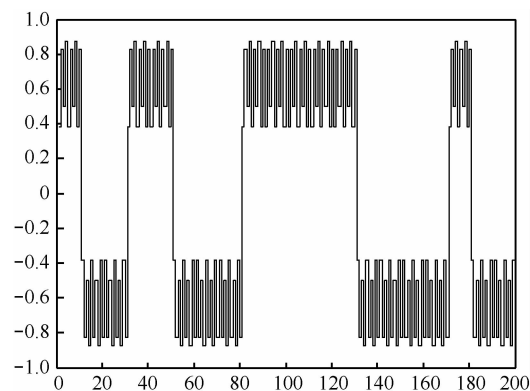


(b) 恢复后的信号

图 3 原始信号与恢复后的信号



(a)传统 DCSK 系统调制信号



(b)改进 DCSK 系统调制信号

图4 传统 DCSK 系统和改进 DCSK 系统

被截获,破译出的也为 $w_k \oplus b_k$,因此该系统保密性得到了极大增强。从图3可知,改进的 DCSK 系统能够将信号正确解调出来,其仿真结果与理论分析一致,从而验证了该方案的正确性。

比较相同扩频系数 M 下,改进前、后 DCSK 系统的误码性能,图5是 M 分别为20和30时,两种系统的误码性能仿真。从图中可以看出,信噪比较低时,两个系统误码率相差不大,当 E_b/N_0 大于5 dB时,误码率的差别开始增大,改进 DCSK 系统比传统 DCSK 系统低。在相同的 E_b/N_0 下,改进 DCSK 系统比传统 DCSK 系统误码率要低1~2个数量级;在相同的 BER 下,信噪比也有所不同,当 $BER=10^{-3}$ 时,改进 DCSK 系统比传统 DCSK 系统大约提高了2.5 dB。

如图6所示,DCSK 系统误码性能和 M 有很大关系。当 M 在一定范围内时,随着 M 增大,系统 BER 将减小,误码性能也越好。在 $E_b/N_0 < 15$ dB 时, M 对系统 BER 影响不大;而当 $E_b/N_0 > 15$ dB 时,BER 得到极大改善,如 E_b/N_0 在30 dB 时,BER 基本改善1个数量级左右。当 BER 为 10^{-3} 时, M 为5和15时 E_b/N_0 大约改善了20 dB。

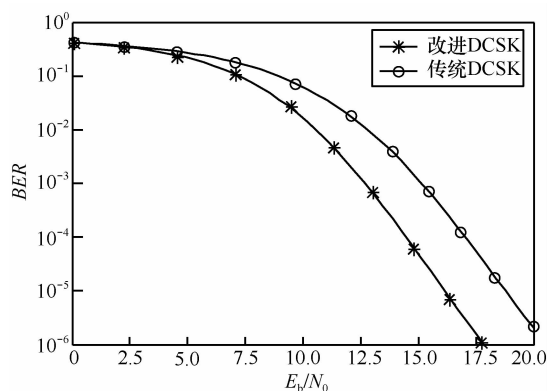
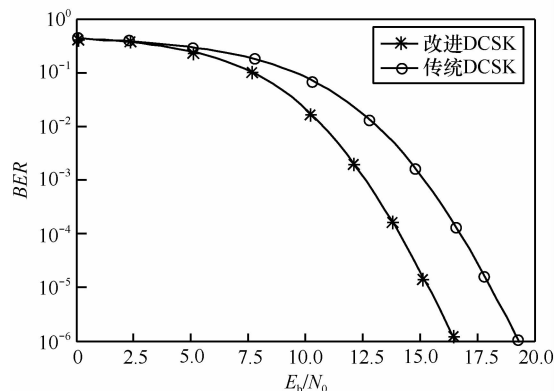
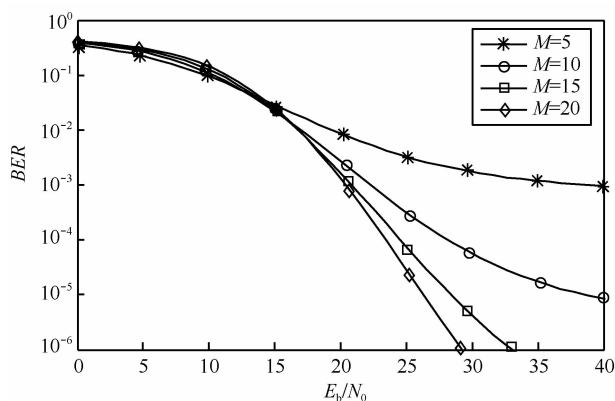
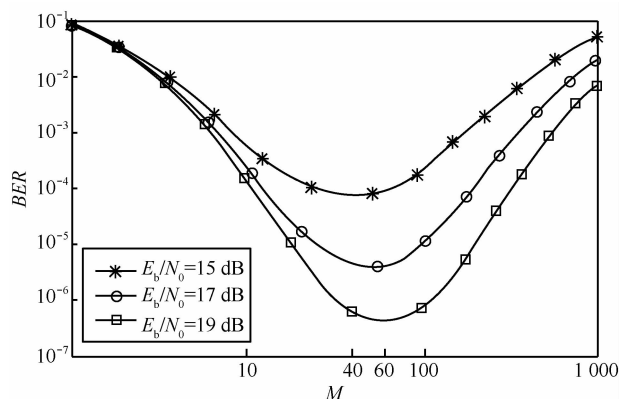

 (a) $M=20$

 (b) $M=30$

 图5 相同 M 值下,改进前后 DCSK 的误码性能

 图6 不同 M 值下误码率

不同信噪比下, M 和 BER 之间的关系如图7所示。从图中可以看出,信噪比越大,相同 M 值下的 BER 越低。随着扩频系数 M 的增大,误码性能并非越来越好,当 M 为50左右的时候,BER 达到最小值。随后, M 越大,BER 反而随之增加,而且 M 的增大会使得信号的传输效率降低。因而选取合适的 M 值对性能改善有很大的影响。总体看来,改进的 DCSK 系统性能明显要优于传统系统,在数据传输的误码性能和保密性上都有很大改善。

图 7 不同 E_b/N_0 下误码率

可将该方案用于图像保密传输,信噪比和 M 在不同取值情况下的仿真结果如图 8 所示。从式(10)中可以看出,影响误码率的因素有两个:一个是扩频系数 M ,一个是信噪比 E_b/N_0 。因此通过选取不同的 M 和 E_b/N_0 ,比较对图像传输的影响。当信道噪声固定不变时,随着 M 的增大,图像的清晰度逐渐变好;当 M 固定不变时,随着 E_b/N_0 的增大,图像也逐渐变得清晰;当 M 和一个信道的 E_b/N_0 固定不变,另一个信道的 E_b/N_0 逐渐增大时,图像逐渐变得清晰。也就是说 E_b/N_0 和 M 逐渐增大时,图像清晰度就会出

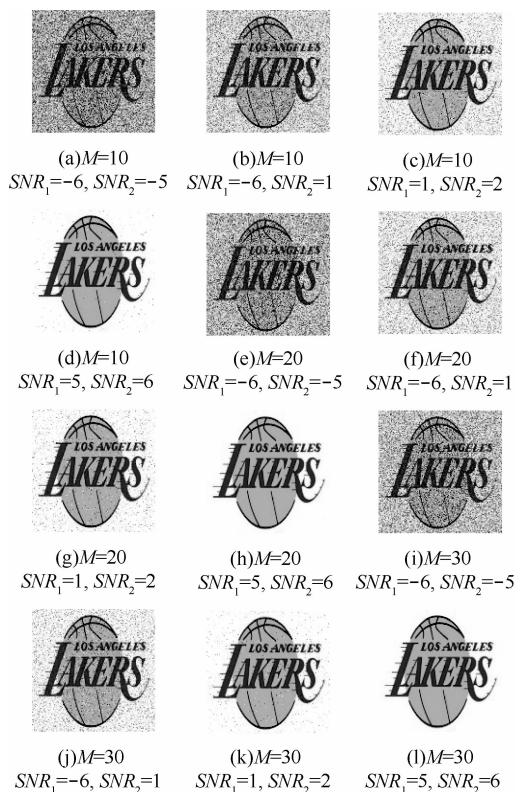
现很大改善,这与理论分析结果一致,可见改进 DCSK 系统同样可应用于图像保密传输。

5 结束语

DCSK 是目前研究最多的差分混沌键控保密通信系统,系统结构简单、误码率低、抗干扰能力强。但是该系统发送的信息信号和参考信号只有同相和反相的区别,所以信道保密性较低,发送的信息被截获后通过数据分析很容易破译出传输信号。针对 DCSK 的保密性问题,经过改进,使信息分散在两条信道上传输,在传输调制信号的信道中加入随机序列,这样即使信息在传输过程中被截获,也无法破译原始信号。通过改进前、后系统误码率的对比,发现改进的 DCSK 系统与传统系统相比,在数据传输中的误码率更低,性能更好。将该方案应用到图像保密传输中,随着信道噪声的减小,扩频系数的增大,图像逐渐变清晰。通过仿真可以看出,仿真结果与理论分析一致,保密性得到极大增强,从而验证了该方案的正确性。但改进系统的信道利用率有所降低,因此下一步工作将针对此问题进行深入的研究。

参考文献

- Li H, Si F F. UWB DCSK system design and simulation. IEEE International Conference on Test and Measurement, HongKong, 2009: 311~314
- Parlitz U, Chua L O, Kocarev L, *et al.* Transmission of digital signals by chaotic synchronization. International Journal Bifurcation Chaos, 1992, 2(4): 973~977
- Dedieu H, Kennedy M P, Hasler M. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit. IEEE Transactions on Circuits and Systems II, 1993, 40(10): 634~642
- Kolumban G, Kennedy M P, Kis G. Performance improvement of chaotic communications systems. European Conference on Circuit Theory and Design, Budapest, 1997: 284~289
- Kolumban G, Vizvari B, Schwarz W, *et al.* Differential chaos shift keying: a robust coding for chaos communication. International Specialist Workshop of Nonlinear Dynamics of Electronic Systems, Seville, Spain, 1996: 87~93
- Kolumban G, Kennedy M P. Recent results for chaotic modulation schemes. Circuits and Systems, ISCAS, 2001, 3(2): 141~144
- Kolumban G, Jako Z, Kennedy M P. Enhanced versions of DCSK and FM-DCSK data transmission system. IEEE-ISCAS, 1999: 475~478

图 8 在不同 M 及 E_b/N_0 情况下的图像清晰度

- 8 刘剑波, 叶春飞, 张树京等. 基于混沌多相序列的差分混沌键控方案. 铁道学报, 2001, 23(1): 52~55
- 9 贺利芳, 张刚, 张天骐. 一种基于 DCSK 的数字保密通信系统. 电子技术应用, 2012, 38(7): 103~106
- 10 Chen S Y, Wang L, Chen G. Data-aided timing synchronization for FM-DCSK UWB communication systems. IEEE Transactions on Industrial Electronics, 2010, 57(5): 1538~1545
- 11 Jako Z, Kis G. On the effectiveness of noise reduction methods in DCSK systems. IEEE International Symposium on Circuits and Systems, 2000, 4(1): 437~440
- 12 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
- 13 Schuster H G, Wolfram J. Deterministic Chaos: an Introduction. Wiley-VCH, Germany, 1998
- 14 Zhang G, He L F, Zhang T Q. A secure communication system based on DCSK. International Journal of Communications in Computer and Information Science (CCIS), 2012, 288(1): 140~147
- 15 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

[作者简介]



贺利芳, 女, 硕士, 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。



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。



张天骐, 男, 博士后, 重庆邮电大学、教授, 信号与信息处理重庆市重点实验室主任, 主要研究方向为宽带微弱无线电信号处理、盲信号检测与信息处理、无线通信的智能信号处理等。

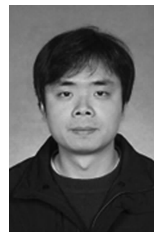
(收稿日期: 2013-03-22)

(上接第 88 页)

- IEEE 802.11p/WAVE vehicular networks. IEEE Communications Letters, 2011, 15(2): 199~201
- 13 Stanica R, Chaput E, Beylot A L. Enhancements of IEEE 802.11p protocol for access control on a VANET control channel. Proceedings of 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 2011: 1~9
 - 14 Deng D, Chen H, Chao H, *et al.* A collision alleviation scheme for IEEE 802.11p VANETs. Wireless Personal Communications, 2011, 56(3): 1~13
 - 15 Jang Hung Chin, Feng Wen Chieh. Network status detection-based dynamic adaptation of contention window in IEEE 802.11p. Proceedings of 2010 IEEE 71st Vehicular Technology Conference (VTC 2010-Spring), Taipei, Taiwan, China, 2010: 1~5
 - 16 Alapati J, Pandya B, Merchant S N, *et al.* Backoff and retransmission strategies for throughput enhancement of broadcast transmissions in IEEE 802.11p. Proceedings of 2010 IEEE Intelligent Vehicles Symposium (IV), Sandgo, CA, 2010: 700~705
 - 17 Ma X M, Chen X B. Performance analysis of IEEE 802.11 broadcast scheme in Ad Hoc wireless LAN. IEEE Transactions on Vehicular Technology, 2008, 57(6): 3757~3768
 - 18 VanetMobiSim. <http://vanet.eurecom.fr/>
 - 19 Network Simulator 2 (NS2). <http://nsnam.isi.edu/nsnam/index.php/>

Main Page

[作者简介]



李大鹏, 男, 南京邮电大学讲师, 主要研究方向为无线通信、认知无线电、移动自组织网络。



袁涛, 男, 南京邮电大学硕士研究生, 主要研究方向为移动通信、车载自组织网络。

赵海涛, 男, 南京邮电大学讲师, 主要研究方向为无线通信与网络编码。

(收稿日期: 2013-03-28)