



一种面向移动无线信道的混沌交织算法

王先平¹, 曹卉²

(1. 重庆文理学院软件工程学院, 重庆 402160;

2. 河南广播电视大学现代教育技术中心, 河南 郑州 450000)

摘要: 交织是抵抗移动无线衰落信道突发差错的有效技术。为了抵抗二维突发差错, 提出了一种新的基于 Baker 映射的混沌交织算法。该算法首先将二进制信源序列转化为数据矩阵, 再使用混沌 Baker 映射方法将其随机离散化, 从而实现二维长突发差错在解交织后变为一维短突发差错。再者, 将该算法和基于 Viterbi 解码的卷积码联合使用, 分别应用于 (2,1,3) 和 (2,1,7) 两种卷积码场景下进行性能比较。仿真结果显示, 当移动信道传输图像画面时, 该算法相比传统方案具有显著优势; 该算法的抗衰落性能随着分组长度的增加而更加优越, 并且有效降低了算法复杂度; 该算法通过使用不同的密钥能够增强每个传输分组的安全性。

关键词: 卷积码; 混沌交织器; 无线信道; 移动性

中图分类号: TN913.21

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016156

A novel chaotic interleaving algorithm for mobile wireless channels

WANG Xianping¹, CAO Hui²

1. School of Software Engineering, Chongqing University of Arts and Sciences, Chongqing 402160, China

2. Center of Modern Educations, Henan Radio & Television University, Zhengzhou 450000, China

Abstract: Interleaving technique is an efficient technique to resist serious burst errors over mobile wireless fading channels. To resist 2 dimensionality burst errors effectively, a novel chaotic interleaving algorithm based on Baker map was proposed. In the proposed scheme, the binary source sequence was converted to the data matrix, and then the data matrix was dispersed randomly by using the chaotic Baker map approach, in order to realize the function of transforming 2 dimensionality long burst error into the short 1 dimensionality short burst error after de-interleaving. In addition, the proposed algorithm was combined with the convolution code based on Viterbi decoding, and was applied into the scenario of convolutional codes (2,1,3) and the scenario of (2,1,7) separately for a performance comparison. The simulation results show that the performance of the proposed algorithm outperforms better than the traditional algorithms under image transmission over mobile wireless channel. Moreover, the anti-fading capability of the proposed algorithm grows as the packet length increases, while reducing the complexity significantly. Finally, the chaotic interleaver can also enhance every transmitted packet's security with different secret keys.

Key words: convolutional code, chaotic interleaving, wireless channel, mobility

收稿日期: 2016-02-29; 修回日期: 2016-06-06

基金项目: 河南省科技厅项目“基于云存储的河南省终身教育海量数字化资源公共服务基础平台建模研究”(No.152102210304); 河南省教育厅项目“面向河南省社区远程教育的海量数字化教学资源存储管理研究”(No.ZJA15172)

Foundation Items: Henan Provincial Department of Science and Technology Project “the Public Service Platform of Massive Digital Resources of Henan Lifelong Education Based on Cloud Storage”(No.152102210304), Henan Provincial Department of Education Project “Research on Storage Management of Massive Digital Teaching Resources for Community Distance Education in Henan”(No.ZJA15172)

1 引言

在移动无线通信环境下,信道的多径衰落会使通信系统产生长串突发差错。目前,应用于移动通信的纠错技术不能完全处理长串突发差错^[1]。因此,需要设计有效的差错分散技术来提高纠错技术的纠错能力。

无线通信系统常使用卷积码(convolutional code, CC)^[2]提高系统纠错能力。Viterbi 译码算法是一种性能较优的译码算法,但其性能受限于码长,计算复杂度和内存需求都会随码长的增加呈指数性增长^[3]。通常会使用交织技术联合卷积码以提高系统纠错性能。其中,块交织技术通过将码序列重新组合排序的方式把长串突发差错离散成多个单突发差错,但其并不能有效离散化图像传输中出现的二维长串突发差错^[4,5]。

为了解决图像传输过程中无线信道产生的二维长串突发差错,本文提出了一种新的基于 Baker 映射^[6]的混沌交织算法。该算法联合卷积码和 Viterbi 译码算法,能够有效提高系统纠错能力,同时降低计算复杂度。仿真结果显示,在无线通信信道中,该混沌交织算法性能优于传统块交织算法。

2 算法设计

2.1 传统交织算法

块交织算法^[7]常被用于纠正无线链路传输图像过程中出现的突发差错。首先将图像信源编码后变成二进制数字序列,再将该序列以行排列的方式排列为矩阵,最后再逐列读取矩阵恢复成数字序列,完成块交织。图 1 给出了 8 bit×8 bit 数据矩阵和块交织过程中的不同版本。假设一个突发差错会影响 4 个连续比特发生差错,成为一维突发差错,见图 2 中的阴影部分。解交织后的网格见图 3,突发差错有效地被扩展到 4 个不同的行中,减小了一维突发差错对图像的影响。

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

图 1 传统交织算法的原始数据矩阵

1	9	17	25	33	41	49	57
2	10	18	26	34	42	50	58
3	11	19	27	35	43	51	59
4	12	20	28	36	44	52	60
5	13	21	29	37	45	53	61
6	14	22	30	38	46	54	62
7	15	23	31	39	47	55	63
8	16	24	32	40	48	56	64

图 2 传统交织算法的交织数据矩阵

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

图 3 传统交织算法的解交织数据矩阵

由于解码算法具有单个误比特纠错能力,一维突发差错不会影响解码的正确性。由图 1 可知,块交织可以有效解决一维突发差错。但对于图 2 中的二维突发差错,由图 3 可知,二维突发差错影响的差错比特并没有被扩展分散开,因此解交织后的差错比特仍然是二维突发差错。由于传统单个差错比特纠错机制不能纠正二维突发差错,因此,块交织算法不能解决二维突发差错。

2.2 混沌交织算法

为了有效解决二维突发差错,本文设计了一种基于离散二维混沌 Baker 映射的混沌交织算法。将二进制信源序列以行方式排列为数据矩阵后,使用混沌 Baker 映射离散化此数据矩阵。离散化后的 Baker 映射是离散方阵的理想工具之一。设 $B_{(m_1, m_2, \dots, m_k)}$ 代表离散 Baker 映射,其中, $[m_1, m_2, \dots, m_k]$ 代表密钥 S_{key} 。设 M 为矩阵行元素的数目,有 $m_1 + m_2 + \dots + m_k = M$ 。因此,映射后的元素新位置为:

$$B_{(m_1, m_2, \dots, m_k)}(r, s) = \left[\frac{M}{m_i} (r - M_i) + s \bmod \frac{M}{m_i}, \frac{m_i}{M} \left(s - s \bmod \frac{M}{m_i} \right) + M \right] \quad (1)$$

其中, r 和 s 分别表示离散方阵中元素的行和列位置, $M_i \leq r \leq M_i + n_i$, $0 \leq s < M$, $M_i = 0$ 。本文提出的混沌交织算法步骤如下所示。

步骤 1 $M \times M$ 阶二维矩阵分解为 M 个宽为 m_i 、元素



数目为 M 的子矩阵。

步骤 2 每个子矩阵中的元素被重新排列成置换矩阵中的一行,子矩阵是依次从上到下、从右到左读取。

步骤 3 每个子矩形内部,依次从左下角向上扫描读取数据。

图 4~图 6 给出了 8×8 方阵使用本文的混沌交织算法的示例。其中,密钥为 $S_{key}=[n_1, n_2, n_3]=[2, 4, 2]$ 。相比块交织机制,混沌交织机制更为有效地解决了一维和二维突发差错。误码在解交织后会被分散扩展开,变成多个单突发差错。因此,混沌交织算法能够提供更好的接收图像的峰值信噪比(peak signal to noise ratio, PSNR)。再者,混沌交织算法的密钥增强了图像传输安全性。在通信系统接收机端,使用步骤相反的混沌解交织算法完成比特流的解交织。

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

图 4 混沌交织算法的原始数据矩阵

31	23	15	7	32	24	16	8
63	55	47	39	64	56	48	40
11	3	12	4	13	5	14	6
27	19	28	20	29	21	30	20
43	35	44	36	45	37	46	38
59	51	60	52	61	53	62	54
25	17	9	1	26	18	10	2
57	49	41	33	58	50	42	34

图 5 混沌交织算法的交织数据矩阵

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

图 6 混沌交织算法的解交织数据矩阵

3 复杂度分析

卷积码在无线通信系统中的应用受限于不同的码长。码长越大,卷积码纠错性能越好,其计算复杂度随码长增加而迅速增大^[8]。在某码长为 K 的一般卷积码中,输入信息序列包含 $k \times L$ bit, 其中, k 表示单位时间间隔内并行处理的信息比特数目, L 指时间间隔的数目。因此,此卷积码有 $m+1$ 阶网格图, m 指解码器中的移相寄存器数目, 且有 $K=m+1$ 。由于网格图中有 $2^k \times L$ 个不同路径, 则其最大似然序列(maximum likelihood, ML)的计算复杂度为 $O(2^k \times L)$ 。Viterbi 算法对每个节点的网格图进行最大似然搜索来降低 ML 序列的计算复杂度。网格图中每阶所包含的节点数目为 2^m 。因此, Viterbi 算法的计算复杂度为 $O((2^k)(2^m)(m+L))^m$ 。当 m 和 k 增大时,复杂度会呈指数式急剧增长。

因此,为了降低复杂度,在算法仿真过程使用基于二进制非递归卷积编码,其卷积编码器采用的分量码主要参数为: $K=3, 5, 7$, 码速率为 $1/2$, 生成多项式分别为 $G=(5, 7)$ 、 $G=(23, 35)$ 、 $G=(133, 171)^{[10-12]}$ 。本文使用混沌交织算法和传统交织算法来提高短码编码器的纠错能力。

4 仿真结果分析

本节使用 MATLAB 软件对提出的混沌交织算法进行了实验仿真。仿真环境采用 Jaker 模型,其载波频率为 $F_c=2.46$ GHz。本节仿真提出了多个不同的移动图像传输场景,主要仿真参数:节点移动速率为 $v=30$ km/h,图像被划分为 512 个分组,每个分组长度为 1 024 bit,卷积码为 $(2, 1, 7)$ 和 $(2, 1, 3)$,交织器为混沌交织器和块交织。同时仿真了分组长度分别为 2 048 bit、4 096 bit、8 192 bit 和 16 384 bit 条件下的图像传输性能,其他参数设置同上。仿真结果见图 7~图 9。图 7 给出了在信噪比 $SNR=10$ dB、分组长度为 16 384 bit 时,不同卷积码长度下本文的混沌交织算法的性能比较。图 8 给出了不同卷积码长度和分组长度条件下使用新混沌交织算法时图像的 PSNR 性能比较。图 9 给出了不同交织算法条件下图像 PSNR 值。

据图 7 可知,卷积码码字长度越长,图像去噪效果越好;图 7(c)和图 7(d)比较可知,使用混沌交织算法的 PSNR 性能优于使用块交织算法;图 7(a)、图 7(b)、图 7(c)比较可知,如果不使用交织算法,接收图像噪点多,质量差。

由图 8 可知,在低 SNR 时,混沌交织算法联合码长更

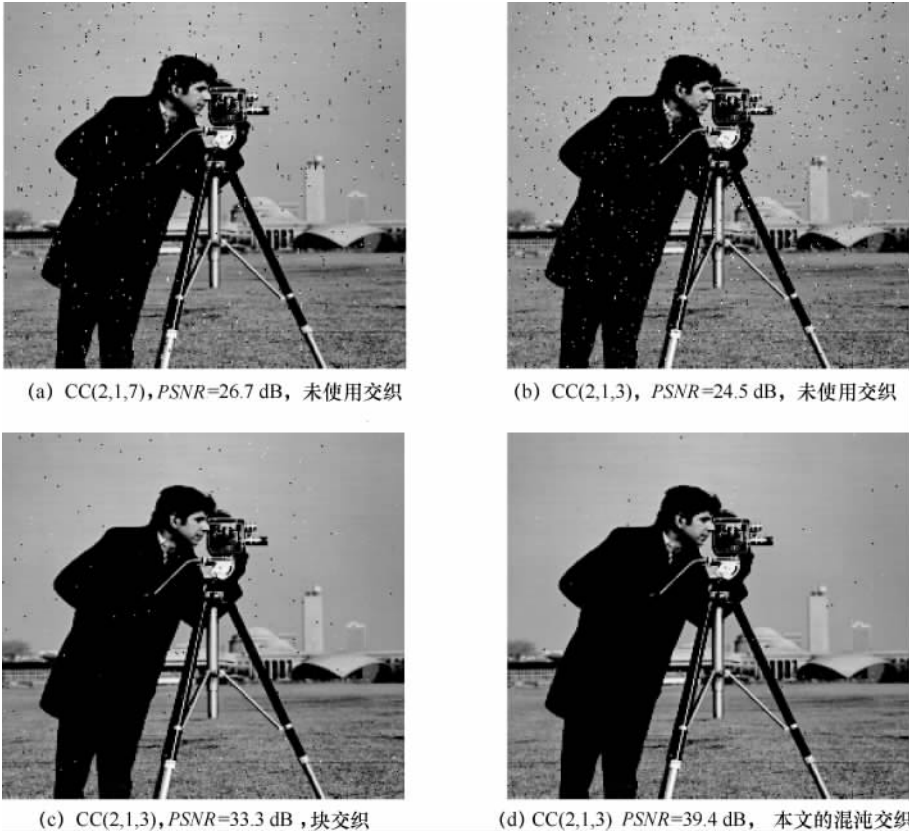


图 7 参数为 $SNR=10$ dB, $v=30$ km/h, 分组长度为 16 384 bit 时接收图像性能比较

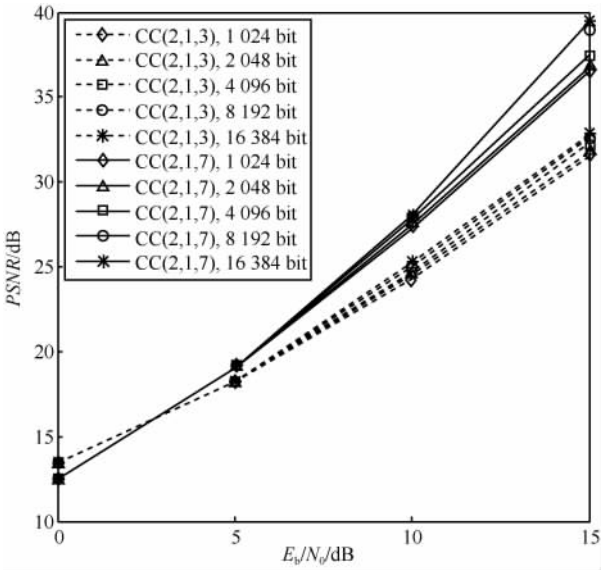


图 8 不同 CC 长度和分组长度条件下接收图像的 PSNR 数值比较

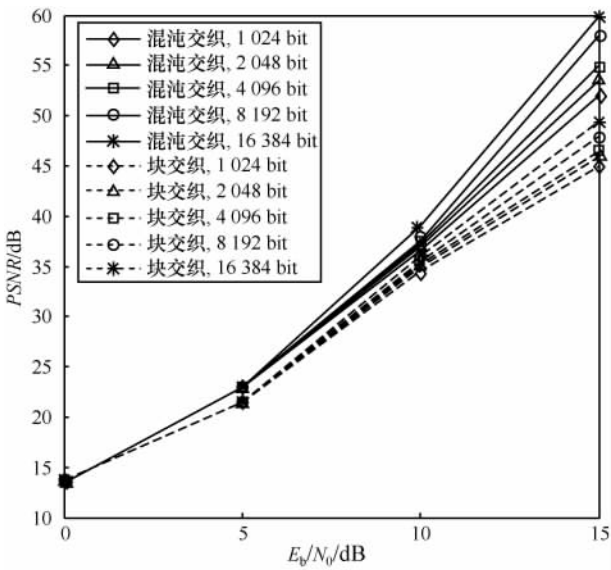


图 9 块交织和本文的混沌交织算法性能比较

短的卷积码可以获得更优的图像传输质量,并且可以降低计算复杂度;高 SNR 时,卷积码越长,图像质量越优;图像使用越长的分组,图像的 PSNR 值越大,传输质量越好。

由图 9 可知,相比传统块交织算法,混沌交织算法能

够提供更好的图像传输质量,这是因为混沌交织算法可以同时弱化一维和二维突发差错。混沌交织算法不受实际通信系统限制,可以被用在如 WLAN 和 WiMAX 的通信网络中,并且能够提升链路安全性能。



5 结束语

本文提出了一种简单有效的新混沌交织算法,该算法和使用 Viterbi 译码的卷积码联合使用,能够明显提升无线移动信道传输的图像质量和安全性。本文比较了传统块交织算法和混沌交织算法的性能差异,后者可以解决传统块交织不能够离散化的二维突发差错。其次,使用块交织算法可以明显降低卷积码字长度,进而降低计算复杂度,提升算法效率。再者,由于混沌交织算法使用了密钥对信源加密,能够大大提升图像传输安全性。仿真实验证明,本文所提算法更适用于移动通信,能够使无线信道具有优越的图像传输性能。

参考文献:

- [1] 张博, 林伟, 刘春元, 等. 突发差错信道下的多元 LDPC 码设计与性能分析[J]. 通信学报, 2013, 34(7): 98-104.
ZHANG B, LIN W, LIU C Y, et al. On the design and performance of nonbinary LDPC codes on burst error channels[J]. Journal on Communications, 2013, 34(7): 98-104.
- [2] 唐琪. 基于 3G 的卷积码的研究[D]. 武汉: 华中师范大学, 2013.
TANG Q. Research on convolutional code based on 3G [D]. Wuhan: Central China Normal University, 2013.
- [3] 段高攀, 杜慧敏, 韩俊刚, 等. 可编程 Viterbi 译码器设计与实现[J]. 电子技术应用, 2014, 40(3): 29-31.
DUAN G P, DU H M, HAN J G, et al. Design and implementation for programmable Viterbi decoder[J]. Application of Electronic Technology, 2014, 40(3): 29-31.
- [4] KASHBAN H, EI A M, TOKHY M. Interleaved reed-solomon codes with code rate switching over wireless communications channels [J]. International Journal of Information Technology and Computer Science, 2014, 16(1): 1-10.
- [5] EI-BENDARY M A M, AE A, NA E F, et al. Enhancing the image transmission over wireless networks through a novel interleaver[J]. KSII Transactions on Internet and Information Systems, 2011, 5(9): 1528-1543.
- [6] 葛祥友. 基于二维 baker 映射的隐写算法设计 [J]. 广西民族大学学报(自然科学版), 2014, 20(2): 66-69.
GE X Y. The steganography algorithm design based on dimensional baker mapping [J]. Journal of Guangxi University (Natural Science Edition), 2014, 20(2): 66-69.
- [7] 易琛, 张天骐, 胡然, 等. BSP 二维块交织算法结合 RS 纠错码在水印中的应用 [J]. 计算机应用研究, 2012, 29(8): 3029-3032.
- YI C, ZHANG T Q, HU R, et al. Application of BSP two dimensional block interleaving algorithm and RS coding in digital watermark [J]. Application Research of Computers, 2012, 29(8): 3029-3032.
- [8] LIU L T, LV Y B. Construction of irregular photograph-based LDPC convolutional codes with windowed decoding[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2014, 26(1): 74-80.
- [9] 王晓涛, 钱骅, 康凯. 基于 Viterbi 双向搜索的咬尾码最大似然译码算法[J]. 电子与信息学报, 2013, 35(5): 1018-1022.
WANG X T, QIAN H, KANG K. Viterbi-bidirectional searching based ML decoding algorithm for tail-biting codes [J]. Journal of Electronics & Information Technology, 2013, 35(5): 1018-1022.
- [10] XU C L, YANG W, YE W C. Decoding algorithms for shortened-extended turbo product codes in WiMAX systems [J]. Science in China Series F: Information Sciences, 2009, 52(12): 2415-2423.
- [11] 张玉玲, 袁东风, 高新颖. 基于新型距离度量的以卷积码为分量码的 MLC/PDL 性能 [J]. 电子与信息学报, 2005, 27(1): 69-72.
ZHANG Y L, YUAN D F, GAO X Y. Performance of MLC/PDL with convolutional codes as component codes under a new distance metric [J]. Journal of Electronics and Information Technology, 2005, 27(1): 69-72.
- [12] KODURU S C, CHANDRASEKARAN V. Integrated confusion-diffusion mechanisms for chaos based image encryption[C]//The IEEE 8th International Conference on Computer and Information Technology Workshops, July 8-11, 2008, Sydney, Australia. New Jersey: IEEE Press, 2008: 260-264.

[作者简介]



王先平(1972-),男,重庆文理学院软件工程学院讲师,主要研究方向为算法理论和应用。



曹卉(1982-),女,河南广播电视大学现代教育技术中心讲师,主要研究方向为云计算、大数据数据分析。