基于矩阵低秩估计的可靠多载波差分混沌键控接收机

张 琳*① 陈炳均① 吴志强②
①(中山大学电子与信息工程学院 广州 510006)
②(西藏大学珠峰研究院 拉萨 850000)

摘 要：在多载波差分混沌键控(MC-DCSK)系统中，经由无线信道传输在接收端进行检测时，参考混沌信号的传输差错将降低承载信息的检测性能，降低传输可靠性。为了提高可靠性，该文基于承载信息的调制信号因共享参考混沌信号的低秩特性，提出了一种基于矩阵低秩估计(LRAM)的MC-DCSK接收机，增强系统可靠性。该接收机将接收信号矩阵表示为秩1矩阵和噪声矩阵之和，然后对接收信号矩阵进行低秩估计，以得到参考信号的最优估计，并进而将其用于承载信息的调制信号的检测和解调，从而提升系统传输可靠性。继而，该文证明了LRAM检测可等效于最大似然估计检测，并对信息泄露率理论安全性能进行了分析，分析结果表明所提方案安全性与基准MC-DCSK系统一致。仿真结果验证了该接收机在加性高斯白噪声(AWGN)和多径衰落信道下可有效提升MC-DCSK系统的可靠性。

关键词：多载波差分混沌键控系统；矩阵低秩估计；可靠性；接收机
中图分类号：TN914.42 **文献标识码**：A **文章编号**：1009-5896(2021)01-0037-08
DOI: 10.11999/JEIT200349

Reliable Multi Carrier Differential Chaos Shift Keying Receiver Based on Low Rank Approximation of Matrices Estimation

ZHANG Lin① CHEN Bingjun① WU Zhiqiang②
①(*School of Electronics and Information Technology*, *Sun Yat-sen University*, *Guangzhou* 510006, *China*)
②(*Everest Research Institute*, *Tibet University*, *Lhasa* 850000, *China*)

Abstract: In Multi-Carrier Differential Chaos Shift Keying (MC-DCSK) systems, after transmitted over wireless channels, the transmission errors in the reference chaotic signal will degrade the detection performances of the information-bearing signals at the receiver. In order to address this issue, in this paper, a Low Rank Approximation of Matrices (LRAM) aided MC-DCSK receiver is proposed based on the low rank characteristics of the information-bearing chaotic modulated signals sharing the same reference chaotic signal, with the aim to enhance the reliability performances. In the design, the received signal matrix is evaluated by the sum of a rank one matrix and a Gaussian noise matrix, and then the LRAM method is applied to derive the estimates of received signals to attain the optimal estimate of the reference chaotic sequence, which is subsequently used to recover the user data, thereby improving the reliability performances of MC-DCSK systems. Subsequently, the proposed LRAM detection is proved that is equivalent to the maximum likelihood estimation detection, then the theoretical security performances in terms of the information leakage is analyzed. The analysis shows that the security performances of the proposed system keep the same as those of the benchmark MC-DCSK systems. Simulation results demonstrate the superior Bit Error Rate (BER) performances of the proposed LRAM aided MC-DCSK systems over Additive White Gaussian Noise (AWGN) and multipath fading channels.

Key words: Multi-Carrier Differential Chaos Shift Keying (MC-DCSK); Low Rank Approximation of Matrices (LRAM); Reliability performances; Receiver

收稿日期：2020-04-30；改回日期：2020-08-04；网络出版：2020-08-07
*通信作者： 张琳 isszl@mail.sysu.edu.cn
基金项目：国家自然科学基金(61602531)，广东省自然科学基金(2020A1515010703)，西藏自治区科技计划项目-重点研发与转化计划(XZ201901-GB-16)
Foundation Items: The National Natural Science Foundation of China (61602531), The Natural Science Foundation of Guang Dong Province (2020A1515010703), The Key Research and Development and Transformation Plan of Science and Technology Program for Tibet Autonomous Region (XZ201901-GB-16)

1 引言

混沌序列具有初值敏感性、非周期性、良好的相关性等特性，可增强传输安全性[1]及抗干扰性能，在数字通信系统中得到了广泛的应用。在混沌通信系统中，根据是否要将参考混沌信号从发射端传输到接收端，可以进一步将混沌调制系统分为相干混沌调制系统和非相干混沌调制系统[1,2]。其中非相干混沌调制通过将参考混沌信号从发射端传输到接收端，尽管恶意用户可利用广播无线信道接收到的参考混沌信号恢复用户数据信息，降低了混沌通信系统的安全性能，但避免了在接收端使用同步电路恢复混沌信号的需求，提高了混沌调制系统的实用性，因而得到了广泛地关注。

近年来涌现了众多非相干混沌调制技术的研究成果。其中，差分混沌键控调制(Differential Chaos Shift Keying, DCSK)技术因其高可靠性而得到了各国学者的青睐[2–8]。然而，正如文献[2]中所指出的，DCSK技术存在一半时隙用于传送参考混沌信号导致的低频谱效率问题和发射端延时线电路难以实现的应用性弱的问题。多载波差分混沌键控调制(Multi-Carrier Differential Chaos Shift Keying, MC-DCSK)系统[3]能有效解决该问题，通过多路子载波信号共享一路参考混沌信号，有效解决了频谱效率较低的问题，并且去除了DCSK发射端所需的延迟线，因此具有较高的实用性。

然而MC-DCSK系统的传输可靠性仍然受制于参考混沌信号的精度。换言之，由于在接收端，承载了用户信息的多路信号需使用预设子载波通路传送的参考混沌信号恢复信息，因此在无线信道上传输后，参考混沌信号的传输差错将直接导致MC-DCSK系统接收端混沌解调可靠性的下降。

为了提高MC-DCSK系统的传输可靠性，文献[4]中提出了降噪的MC-DCSK(Noise Reduction MC-DCSK, NR-MC-DCSK)系统，该系统在发射端重复发送缩短参考序列，然后在接收端对其取平均值的方法，以此来提升参考信号的信噪比，从而提高参考混沌信号的接收检测精度。文献[5]中提出的子载波分配MC-DCSK(Subcarrier Allocated MC-DCSK, SA-MCDCSK)系统则在多个子载波上传输多个参考序列的副本，并在接收端取平均值的方法来提升参考混沌信号的信噪比，进而降低其接收误比特率。在我们的前期工作中[6]，我们提出了一种MC-DCSK迭代接收机(MC-DCSK Iterative Receiver, MC-DCSK-IR)方案，通过迭代检测，有效提升了接收参考混沌信号的信噪比，提高了传输可靠性，并进而带来了接受信息检测精度的提高，增强了系统的传输可靠性。

不同于以上已有的MC-DCSK增强方案，本文提出利用共享参考混沌信号的多路混沌调制信号矩阵具有低秩特性的特点，在接收端采用矩阵低秩估计的方法检测并恢复参考混沌信号，并进而用于混沌调制信号的解调。

在本文所提矩阵低秩估计混沌接收机的设计中，无需改变发射端的结构，也不需要在接收端增加反馈支路，只需要在MC-DCSK接收端增加矩阵低秩估计模块，通过对接收信号矩阵进行低秩估计检测，可得到参考混沌信号的最大似然估计值，提高了检测精度，从而可有效增强混沌解调的可靠性。同时，因所提方案并未改变发射端结构，因此未影响传输安全性、频谱效率及传输有效性。值得注意的是，本文所提方案不同于传统混沌保密通信的安全传输，因直接传输参考混沌序列，其安全性能与基准MC-DCSK系统类似，即经由广播无线信道传输时，恶意用户可利用接收到的参考混沌序列恢复用户数据信息。更进一步，本文证明了矩阵低秩估计方法等效于最大似然估计检测方法，并对理论安全性能进行了分析，推导了信息泄漏率表示式。继而，对所提方案在加性白高斯噪声(Additive White Gaussian Noise, AWGN)信道和衰落信道下对误比特率(Bit Error Rate, BER)进行仿真，验证了所提方案可有效提高系统的可靠性。

本文将首先在第2节简要介绍矩阵低秩估计原理，进而在第3节详细描述基于矩阵低秩估计的MC-DCSK系统，介绍了收发信机结构以及并在Monte Carlo快速矩阵低秩估计方法，快速、可靠地恢复信息，进而在第4节对检测性能进行分析，以证明矩阵低秩估计方法可提供对参考混沌信号的最大似然估计。随后，第5节对所提方案在AWGN信道、瑞利衰落信道上的误比特率性能进行了仿真验证，并在第6节给出了对本文的理论设计与仿真验证进行了总结。

2 矩阵低秩估计概述

矩阵的低秩估计在实际用于评估信息时，例如在图像分析[9,10]以及子空间分割[11]等应用中，可将数据矩阵表示为低秩矩阵和噪声矩阵之和，然后利用矩阵的低秩估计来对数据矩阵降噪评估。文献[10]中给出了使用低秩估计降噪的数学模型：$\boldsymbol{D}=\boldsymbol{X}+\boldsymbol{E}$，其中，$\boldsymbol{X}$为低秩矩阵，$\boldsymbol{E}$为噪声或者在误差矩阵，$\boldsymbol{D}$则为接收到的数据矩阵。该模型表明在实际系统中，原始数据矩阵$\boldsymbol{X}$是一个低秩的矩阵，但是由于噪声或者测量误差$\boldsymbol{E}$的影响，使得能够直接观测到的矩阵$\boldsymbol{D}$的秩远大于低秩矩阵$\boldsymbol{X}$的秩。

换言之，矩阵的低秩估计就是用一个秩更低的

矩阵去近似原矩阵，其需要满足的条件是估计矩阵与原矩阵的误差达到最小，即：$\min \left\| \boldsymbol{D}-\boldsymbol{U}\boldsymbol{V}^{\mathrm{T}} \right\|_{\mathrm{F}}$。其中，$\|\cdot\|_{\mathrm{F}}$表示Frobenius范数。对于任一矩阵$\boldsymbol{Z}$，其Frobenius范数可以表示为：$\|\boldsymbol{Z}\|_{\mathrm{F}}=\sqrt{\sum_{i,j} Z_{i,j}^2}$，其中$Z_{i,j}$表示矩阵$\boldsymbol{Z}$第$i$行第$j$列的元素。

进而，将低秩矩阵$\boldsymbol{X}$可表示为$\boldsymbol{X}=\boldsymbol{U}_x\boldsymbol{V}_x^{\mathrm{T}}$。观测到的矩阵$\boldsymbol{D}$和估计结果可以表示为

$$\boldsymbol{D}=\boldsymbol{X}+\boldsymbol{E}=\boldsymbol{U}_x\boldsymbol{V}_x^{\mathrm{T}}+\boldsymbol{E}\approx\boldsymbol{U}\boldsymbol{V}^{\mathrm{T}} \tag{1}$$

估计的低秩矩阵为$\widehat{\boldsymbol{X}}=\boldsymbol{U}\boldsymbol{V}^{\mathrm{T}}$，根据矩阵的低秩估计，为了得到最优的估计，需要解决以下最优化的问题

$$\hat{\boldsymbol{X}}=\underset{\mathrm{rank}(\hat{\boldsymbol{X}})=\eta}{\arg\min}\left\|\boldsymbol{D}-\hat{\boldsymbol{X}}\right\|_{\mathrm{F}} \tag{2}$$

其中η为对估计矩阵$\widehat{\boldsymbol{X}}$的秩的约束。解决该优化问题最常用的方法就是奇异值分解(Singular Value Decomposition, SVD)，通过使用SVD对矩阵$\boldsymbol{D}$进行分解，然后根据秩η，对其奇异值进行收缩，即将部分奇异值置零，从而达到低秩估计的目的。

基于以上低秩估计原理，本文提出了基于LRAM(Low Rank Approximation of Matrices)的MC-DCSK传输系统，如下文所述。

3　基于LRAM的MC-DCSK系统模型

本节将首先介绍基于LRAM的MC-DCSK发射端及接收端结构，然后将详细描述基于快速Monte Carlo的LRAM方法。

3.1 收发信机结构

如图1所示为MC-DCSK系统发射机。在发射机中，首先二进制信息比特通过二进制相移键控(Binary Phase Shift Keying, BPSK)调制，生成数据流。然后对数据流进行串并转换，生成并行数据序列$[d_1,d_2,\cdots,d_k]$，其中k为并行数据的长度。混沌信号生成器生成了混沌序列$\boldsymbol{c}=[c_1,c_2,\cdots,c_\beta]$，然后将这$k$个并行数据分别使用混沌序列$\boldsymbol{c}$进行调制，可以得到$k$个调制信号：$\boldsymbol{t}_i=d_i\boldsymbol{c}$。其中$i\in\{1,2,\cdots,k\}$。为方便起见，令$i=0$时，$d_0=1$，可得$\boldsymbol{t}_0=d_0\boldsymbol{c}=\boldsymbol{c}$，即令$\boldsymbol{t}_0$表示参考混沌信号。随后发射端将参考信号和调制信号同时通过不同的子载波发射到无线信道中。

发射信号矩阵的示意图如图2所示。由图可知，发射信号所组成的矩阵$\boldsymbol{T}$，其秩为1。发射信号矩阵$\boldsymbol{T}$中的每一列是某一路子载波传输的信号。矩阵$\boldsymbol{T}$可以写成向量$\boldsymbol{c}$和$\boldsymbol{d}^{\mathrm{T}}$的乘积，$\boldsymbol{c}$为混沌序列向量，$\boldsymbol{d}$为BPSK信号向量。

发射信号经信道传输后，送入图3所示的基于LRAM的MC-DCSK接收机践行检测估计。当接收到发射机发送来的信号之后，各个子载波上的信号首先经过匹配滤波组成接收信号矩阵$\boldsymbol{R}$，而后对矩阵$\boldsymbol{R}$进行低秩估计，得到低秩矩阵$\widehat{\boldsymbol{B}}$，最后对其低秩矩阵$\widehat{\boldsymbol{B}}$进行MC-DCSK解调恢复信息。通过对接收信号矩阵进行低秩估计，并最小化估计信号与发送信号之间的距离，以有效降低噪声的影响，提升系统的可靠性。

基于发射端和接收端结构，经无线信道传输后，在接收端，接收信号矩阵可表示为

$$\boldsymbol{R}=\boldsymbol{B}+\boldsymbol{N} \tag{3}$$

式中，矩阵$\boldsymbol{N}$为噪声矩阵，矩阵$\boldsymbol{R}\in\mathbb{R}^{\boldsymbol{\beta}\times\boldsymbol{M}}$的每一列表示经过每一路子信道传输的承载用户信息的信号矩阵，$\boldsymbol{B}$表示承载用户信息的发射信号矩阵，由于其每列信号与参考混沌信号相关，因此具有低秩特性，即矩阵$\boldsymbol{R}$可以表示为低秩矩阵和噪声矩阵的

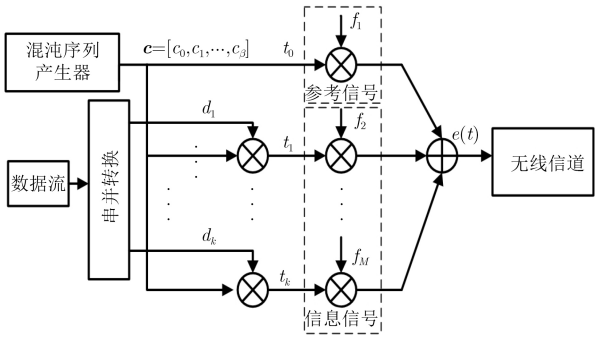


图 1 MC-DCSK系统发射机

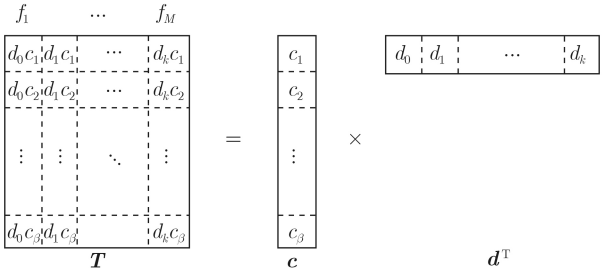


图 2 MC-DCSK系统发射信号矩阵示意图

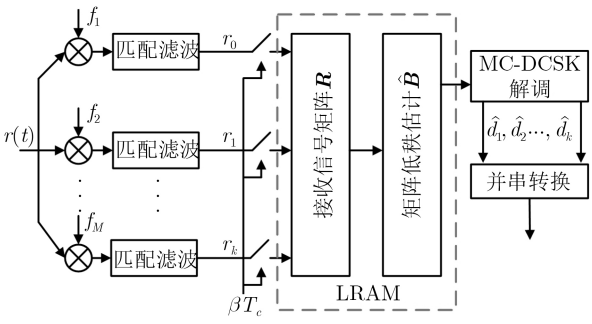


图 3 基于LRAM的MC-DCSK接收机框图

和。因此我们提出对接收矩阵$\boldsymbol{R}$采用低秩估计的方法来降低其噪声，从而提升系统可靠性。

3.2 基于快速Monte Carlo的LRAM检测估计方法

本节将使用基于快速Monte Carlo的LRAM算法来实现对接收信号矩阵的低秩估计。矩阵低秩估计常用的方法是SVD, SVD的过程在统计上对应于主成分分析(Principal Component Analysis, PCA)，其目标是最小化估计误差。在使用SVD分解后，根据秩的约束对奇异值进行收缩操作，即把部分奇异值置为0，然后把矩阵分解的结果相乘便可得到估计的低秩矩阵。然而，SVD算法的复杂度过高，当数据量比较大的时候，所需的时间较长。因此在本文中使用基于Monte Carlo的LRAM算法[12]来获得低秩矩阵，以降低低秩估计检测的复杂度。

基于快速Monte Carlo的LRAM算法核心是通过Monte Carlo的方法，在随机选择的机制下进行迭代运算，最终在指定的秩约束下达到收敛条件。对矩阵$\boldsymbol{A}$进行秩η估计的主要步骤包括两步：

第1步，从矩阵$\boldsymbol{A}$中选择η列使用改进的Gram-Schmidt算法(Modified Gram-Schmidt Algorithm, MGSA)获取正交阵$\boldsymbol{B}_0$。

第2步，进行迭代操作，在第t次迭代过程中，从矩阵$\boldsymbol{A}$中随机选择l列对$\boldsymbol{B}_{t-1}$进行更新获得正交阵$\boldsymbol{B}_t$。当满足$\|\boldsymbol{B}_{t-1}\|/\|\boldsymbol{B}_t\|>1-\varepsilon$时，其中$\varepsilon$为一个很小的正数，停止迭代。最后通过矩阵$\boldsymbol{B}_t$可获得奇异值和奇异向量。

由于使用Monte Carlo进行迭代，该方法无需像SVD一样计算出所有的奇异值，然后进行排序处理，因此可有效降低复杂度。更详细而言，对于一个$m\times n$的矩阵，如果使用SVD复杂度为$O\left(mn\cdot\min(m,n)\right)$，使用快速Monte Carlo的LRAM则复杂度变为$O\left(\eta mn\right)$，其中η为秩的约束。显然，$\eta\le\min(m,n)$，且当η越小时，其复杂度也会更低。在本文中η=1，可有效降低系统的复杂度。

4 基于LRAM的MC-DCSK接收机的性能分析

本节将首先证明所提出的LRAM检测性能可等效于基准MC-DCSK系统的性能，进而，本节将推导信息泄漏率表示式，以分析所提系统的理论安全性能。

4.1 LRAM等效于最大似然估计的证明

在接收信号矩阵$\boldsymbol{R}$中，第1列为接收到的参考信号，其他列为接收到的信息信号。其中，矩阵$\boldsymbol{B}$可表示为

$$\begin{aligned}\boldsymbol{B}&=\begin{pmatrix}\sum\limits_{l=1}^{L}\lambda_l c_{1-\tau_l}d_0 & \left(\sum\limits_{l=1}^{L}\lambda_l c_{1-\tau_l}\right)d_1 & \cdots & \left(\sum\limits_{l=1}^{L}\lambda_l c_{1-\tau_l}\right)d_k\\ \vdots & \vdots & \ddots & \vdots\\ \sum\limits_{l=1}^{L}\lambda_l c_{\beta-\tau_l}d_0 & \left(\sum\limits_{l=1}^{L}\lambda_l c_{\beta-\tau_l}\right)d_1 & \cdots & \left(\sum\limits_{l=1}^{L}\lambda_l c_{\beta-\tau_l}\right)d_k\end{pmatrix}\\&=\begin{pmatrix}\sum\limits_{l=1}^{L}\lambda_l c_{1-\tau_l}d_0 & \sum\limits_{l=1}^{L}\lambda_l c_{1-\tau_l}d_1 & \cdots & \sum\limits_{l=1}^{L}\lambda_l c_{\beta-\tau_l}\end{pmatrix}^{\mathrm{T}}\begin{pmatrix}d_0 & d_1 & \cdots & d_k\end{pmatrix}\end{aligned}\tag{4}$$

其中，$d_0=1$, λ_l和τ_l分别为第l条路径的信道系数和时延。从式(4)可看出：矩阵$\boldsymbol{B}$的秩为1。此外，噪声信号矩阵$\boldsymbol{N}$可表示为

$$\boldsymbol{N}=\begin{pmatrix}n_1^0 & n_1^1 & \cdots & n_1^k\\ \vdots & \vdots & \ddots & \vdots\\ n_\beta^0 & n_\beta^1 & \cdots & n_\beta^k\end{pmatrix}\tag{5}$$

矩阵$\boldsymbol{N}$中的每一个元素都是独立的零均值高斯噪声。

文献[13]中给出矩阵最优的rank-η估计可以由式(6)表示

$$\widehat{\boldsymbol{B}}=\mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=\eta}\left\|\boldsymbol{R}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}=\mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=\eta}\left\|\boldsymbol{B}+\boldsymbol{N}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}\tag{6}$$

因为式(4)中给出矩阵$\boldsymbol{B}$的秩为1，所以对于矩阵$\widehat{\boldsymbol{B}}$期望得到的秩也为1，即$\mathrm{rank}(\widehat{\boldsymbol{B}})=\eta=1$。令$\boldsymbol{b}_j$和$\widehat{\boldsymbol{b}}_j$分别表示矩阵$\boldsymbol{B}$和矩阵$\widehat{\boldsymbol{B}}$的第$j$列，$\boldsymbol{b}_1$表示$\boldsymbol{B}$的第1列，也是发送的参考信号。此外，$\widehat{\boldsymbol{b}}_1$表示$\widehat{\boldsymbol{B}}$的第1列，也是$\boldsymbol{b}_1$的估计值，即为参考信号的估计值。

接着，以下将证明通过解决$\mathop{\arg\min}\limits_{\mathrm{rank}(\widehat{\boldsymbol{B}})=1}\left\|\boldsymbol{R}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}$的问题，等价于对参考混沌信号的最优估计，即$\mathop{\arg\min}\limits_{\widehat{\boldsymbol{b}}_1}\left\|\boldsymbol{b}_1-\widehat{\boldsymbol{b}}_1\right\|^2$，也即证明

$$\mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=1}\left\|\boldsymbol{R}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}\Leftrightarrow\mathop{\arg\min}_{\widehat{\boldsymbol{b}}_1}\left\|\boldsymbol{b}_1-\widehat{\boldsymbol{b}}_1\right\|^2\tag{7}$$

首先，基于前面所述的$\mathrm{rank}(\widehat{\boldsymbol{B}})=\eta=1$，对式(6)进行运算可以得到

$$\begin{aligned}\mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=1}\left\|\boldsymbol{R}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}} &\Leftrightarrow \mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=1}\left\|\boldsymbol{R}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}^2\\ &\Leftrightarrow \mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=1}\left\|\boldsymbol{B}+\boldsymbol{N}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}^2\end{aligned} \tag{8}$$

令$B_{i,j}$, $\hat{B}_{i,j}$以及$N_{i,j}$分别表示$\boldsymbol{B}$, $\widehat{\boldsymbol{B}}$和$\boldsymbol{N}$的第i行和第j列的元素。根据Frobenius范数的表达式，式(8)可以展开为

$$\begin{aligned}&\mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=1}\left\|\boldsymbol{B}+\boldsymbol{N}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}\\ &\Leftrightarrow \mathop{\arg\min}_{B_{i,j}}\left(\sum_{i=1}^{\beta}\sum_{j=1}^{M}\left(B_{i,j}+N_{i,j}-\hat{B}_{i,j}\right)^2\right)\\ &\Leftrightarrow \mathop{\arg\min}_{B_{i,j}}\left(\sum_{i=1}^{\beta}\sum_{j=1}^{M}\left[\left(B_{i,j}-\hat{B}_{i,j}\right)^2+N_{i,j}^2\right.\right.\\ &\quad\left.\left.+2B_{i,j}N_{i,j}-2\hat{B}_{i,j}N_{i,j}\right]\right)\end{aligned} \tag{9}$$

由于混沌信号与噪声信号是不相关的，当扩频因子β较大的时候，相关系数将接近于0，故可得

$$\boldsymbol{b}_j\cdot\boldsymbol{n}_j=\sum_{i=1}^{\beta}B_{i,j}N_{i,j}\approx 0,\quad \widehat{\boldsymbol{b}}_j\cdot\boldsymbol{n}_j=\sum_{i=1}^{\beta}\hat{B}_{i,j}N_{i,j}\approx 0 \tag{10}$$

其中$\boldsymbol{b}_j$和$\widehat{\boldsymbol{b}}_j$分别表示矩阵$\boldsymbol{B}$和矩阵$\widehat{\boldsymbol{B}}$的第$j$列。根据该式我们可以继续推导得到

$$\begin{aligned}&\mathop{\arg\min}_{B_{i,j}}\left(\sum_{i=1}^{\beta}\sum_{j=1}^{M}\left[\left(B_{i,j}-\hat{B}_{i,j}\right)^2+N_{i,j}^2\right.\right.\\ &\quad\left.\left.+2B_{i,j}N_{i,j}-2\hat{B}_{i,j}N_{i,j}\right]\right)\\ &\Leftrightarrow \mathop{\arg\min}_{B_{i,j}}\left(\sum_{i=1}^{\beta}\sum_{j=1}^{M}\left[\left(B_{i,j}-\hat{B}_{i,j}\right)^2+N_{i,j}^2\right]\right)\end{aligned} \tag{11}$$

接着，结合式(9)和式(11)，可得

$$\begin{aligned}&\mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=1}\left\|\boldsymbol{B}+\boldsymbol{N}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}\\ &\Leftrightarrow \mathop{\arg\min}_{B_{i,j}}\left(\sum_{i=1}^{\beta}\sum_{j=1}^{M}\left(B_{i,j}+N_{i,j}-\hat{B}_{i,j}\right)^2\right)\\ &\Leftrightarrow \mathop{\arg\min}_{B_{i,j}}\left(\sum_{i=1}^{\beta}\sum_{j=1}^{M}\left[\left(B_{i,j}-\hat{B}_{i,j}\right)^2+N_{i,j}^2\right]\right)\\ &\Leftrightarrow \mathop{\arg\min}_{B_{i,j}}\left(\sum_{i=1}^{\beta}\sum_{j=1}^{M}\left[B_{i,j}^2+\hat{B}_{i,j}^2+N_{i,j}^2-2B_{i,j}\hat{B}_{i,j}\right]\right)\end{aligned} \tag{12}$$

对混沌信号进行能量归一化，故有

$$\sum_{i=1}^{\beta}B_{i,j}^2=\sum_{i=1}^{\beta}\hat{B}_{i,j}^2=1,\quad \sum_{i=1}^{\beta}N_{i,j}^2=\sigma^2 \tag{13}$$

其中σ^2为噪声方差。将式(13)代入式(12)，最优化问题可以进一步表示为

$$\begin{aligned}&\mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=1}\left\|\boldsymbol{B}+\boldsymbol{N}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}\\ &\Leftrightarrow \mathop{\arg\min}_{B_{i,j}}\left(2M+\sigma^2M-\sum_{i=1}^{\beta}\sum_{j=1}^{M}2B_{i,j}\hat{B}_{i,j}\right)\\ &\Leftrightarrow \mathop{\arg\min}_{\hat{\boldsymbol{b}}_j}\left(2M+\sigma^2M-\sum_{j=1}^{M}2\left(\hat{\boldsymbol{b}}_j\cdot\hat{\boldsymbol{b}}_j\right)\right)\\ &\Leftrightarrow \mathop{\arg\max}_{\hat{\boldsymbol{b}}_j}\left(\sum_{j=1}^{M}\left(\hat{\boldsymbol{b}}_j\cdot\hat{\boldsymbol{b}}_j\right)\right)\end{aligned} \tag{14}$$

根据式(14)可知，$\mathop{\arg\min}_{\mathrm{rank}(\widehat{\boldsymbol{B}})=1}\left\|\boldsymbol{R}-\widehat{\boldsymbol{B}}\right\|_{\mathrm{F}}$的最优解计算问题可转化成计算$\mathop{\arg\max}_{\hat{\boldsymbol{b}}_j}\left(\sum_{j=1}^{M}\left(\boldsymbol{b}_j\cdot\widehat{\boldsymbol{b}}_j\right)\right)$最优解的问题，即需要求得$M$个向量使得这两个矩阵对应的向量的相关值最大。由于$\boldsymbol{B}$的秩为1，其估计矩阵$\widehat{\boldsymbol{B}}$的秩也设置为1，所以相关值最大化的问题可以由$M$对向量间的相关值最大化问题，简化成参考向量$\boldsymbol{b}_1$和$\widehat{\boldsymbol{b}}_1$的相关值最大化问题。其证明详述如下。

根据式(3)可知，$\boldsymbol{R}$的第j列为$\boldsymbol{b}_j+\boldsymbol{n}_j$，所以$\widehat{\boldsymbol{B}}$的第$j$列可以表示为

$$\widehat{\boldsymbol{b}}_j=\frac{(\boldsymbol{b}_j+\boldsymbol{n}_j)\cdot\widehat{\boldsymbol{b}}_1}{(\boldsymbol{b}_1+\boldsymbol{n}_1)\cdot\widehat{\boldsymbol{b}}_1}\widehat{\boldsymbol{b}}_1 \tag{15}$$

将式(15)代入式(14)中可以得到

$$\begin{aligned}&\mathop{\arg\max}_{\hat{\boldsymbol{b}}_j}\left(\sum_{j=1}^{M}\left(\boldsymbol{b}_j\cdot\hat{\boldsymbol{b}}_j\right)\right)\\ &\Leftrightarrow \mathop{\arg\max}_{\hat{\boldsymbol{b}}_j}\left(\sum_{j=1}^{M}\left(\boldsymbol{b}_j\cdot\frac{(\boldsymbol{b}_j+\boldsymbol{n}_j)\cdot\hat{\boldsymbol{b}}_1}{(\boldsymbol{b}_1+\boldsymbol{n}_1)\cdot\hat{\boldsymbol{b}}_1}\hat{\boldsymbol{b}}_1\right)\right)\\ &\Leftrightarrow \mathop{\arg\max}_{\hat{\boldsymbol{b}}_j}\left(\sum_{j=1}^{M}\left(\frac{\left(\boldsymbol{b}_1\cdot\hat{\boldsymbol{b}}_j\right)^2}{(\boldsymbol{b}_1+\boldsymbol{n}_1)\cdot\hat{\boldsymbol{b}}_1}\right)\right)\\ &\Leftrightarrow \mathop{\arg\max}_{\hat{\boldsymbol{b}}_1}\left(\sum_{j=1}^{M}\left(\frac{\left(\boldsymbol{b}_1\cdot d_{j-1}\hat{\boldsymbol{b}}_1\right)^2}{(\boldsymbol{b}_1+\boldsymbol{n}_1)\cdot\hat{\boldsymbol{b}}_1}\right)\right)\end{aligned} \tag{16}$$

其中$\boldsymbol{b}_j=d_{j-1}\boldsymbol{b}_1$。由于噪声信号$\boldsymbol{n}_1$和$\boldsymbol{n}_j$与$\widehat{\boldsymbol{b}}_1$和$\boldsymbol{b}_j$相关性低，可以进一步得到

$$\begin{aligned}&\arg\max_{\hat{\boldsymbol{b}}_1}\left(\sum_{j=1}^{M}\left(\frac{\left(\boldsymbol{b}_1\cdot d_{j-1}\hat{\boldsymbol{b}}_1\right)^2}{(\boldsymbol{b}_1+\boldsymbol{n}_1)\cdot\hat{\boldsymbol{b}}_1}\right)\right)\\&\Leftrightarrow\arg\max_{\hat{\boldsymbol{b}}_1}\left(\sum_{j=1}^{M}\left(\frac{\left(\boldsymbol{b}_1\cdot\hat{\boldsymbol{b}}_1\right)^2}{\boldsymbol{b}_1\cdot\hat{\boldsymbol{b}}_1+\boldsymbol{n}_1\cdot\hat{\boldsymbol{b}}_1}\right)\right)\\&\Leftrightarrow\arg\max_{\hat{\boldsymbol{b}}_1}\left(\boldsymbol{b}_1\cdot\hat{\boldsymbol{b}}_1\right)\end{aligned}\tag{17}$$

由于$||\widehat{\boldsymbol{b}}_1||=||\boldsymbol{b}_1||=1$，式(17)中给出的最大化问题可以进一步转换为

$$\begin{aligned}&\arg\max_{\hat{\boldsymbol{b}}_1}\left(\boldsymbol{b}_1\cdot\hat{\boldsymbol{b}}_1\right)\\&\Leftrightarrow\arg\min_{\hat{\boldsymbol{b}}_1}\left(\|\boldsymbol{b}_1\|^2+\left\|\hat{\boldsymbol{b}}_1\right\|^2-2\boldsymbol{b}_1\cdot\hat{\boldsymbol{b}}_1\right)\\&\Leftrightarrow\arg\min_{\hat{\boldsymbol{b}}_1}\left\|\boldsymbol{b}_1-\hat{\boldsymbol{b}}_1\right\|^2\end{aligned}\tag{18}$$

最后，根据式(18)可得：最优化问题可以转换为对参考信号的最优估计$\arg\min_{\widehat{\boldsymbol{b}}_1}||\boldsymbol{b}_1-\widehat{\boldsymbol{b}}_1||^2$，即

$$\arg\min_{\text{rank}(\hat{\boldsymbol{B}})=1}\left\|\boldsymbol{R}-\hat{\boldsymbol{B}}\right\|_{\text{F}}\Leftrightarrow\arg\min_{\hat{\boldsymbol{b}}_1}\left\|\boldsymbol{b}_1-\hat{\boldsymbol{b}}_1\right\|^2\tag{19}$$

由式(19)可见，借由矩阵低秩估计检测，可得参考混沌信号的最大似然估计，并进而等效于对承载信息的混沌调制信号进行了最大似然估计，因此，有效增强了MC-DCSK信号的传输可靠性。

4.2 信息泄露率理论安全性能分析

为了量化衡量系统的安全性和保密性，以下本文将推导存在恶意窃听用户时系统信息泄露率的计算式。假设“0”，“1”比特在信道传输中出现的概率相等，窃听者恢复出的信息$\boldsymbol{Y}_e^{'}$与原始的发送信息$\boldsymbol{X}$之间的互信息$I\left(\boldsymbol{Y}_e^{'};\boldsymbol{X}\right)$可以通过式(20)得到

$$\begin{aligned}I\left(\boldsymbol{Y}_e^{'};\boldsymbol{X}\right)&=H\left(\boldsymbol{Y}_e^{'}\right)-H\left(\boldsymbol{Y}_e^{'}|\boldsymbol{X}\right)\\&=1+P_e\lg P_e+(1-P_e)\lg(1-P_e)\end{aligned}\tag{20}$$

式中：$H(\cdot)$表示信息熵，P_e表示窃听者的误码率。然后，可以通过式(20)给出的互信息$I\left(\boldsymbol{Y}_e^{'};\boldsymbol{X}\right)$计算系统对窃听者的信息泄露$L$，可表示为：$L=I\left(\boldsymbol{Y}_e^{'};\boldsymbol{X}\right)$。综上可得：所提方案并未改变MC-DCSK发射端结构，因此窃听者的误码率P_e保持不变，因此MC-DCSK-LRAM系统安全性能与基准MC-DCSK系统一致。

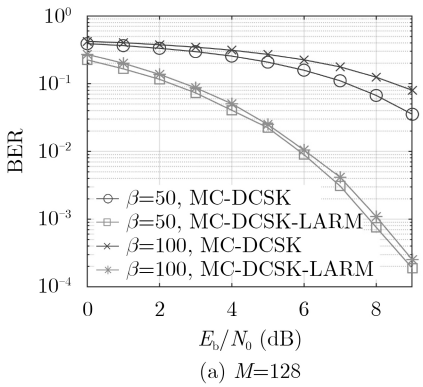
5 仿真结果与分析

本节首先给出了MC-DCSK-LRAM，传统MC-DCSK系统在AWGN信道和多径衰落信道下的BER仿真性能，然后比较了MC-DCSK-LRAM，SA-MCDCSK[5]和MC-DCSK-IR[6]在AWGN信道和多径衰落信道下的BER性能，其中LRAM采用基于快速Monte Carlo的LRAM的方式实现。在仿真中，M表示子载波的数量，β为扩频因子。在仿真中参数设置为$\beta=50,100$, $M=64,128$，其他仿真参数在下文中给出。

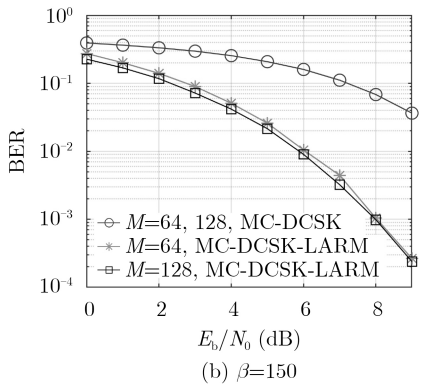
图4比较了MC-DCSK和MC-DCSK-LRAM在AWGN信道下的性能。图4(a)给出了$M=128$, $\beta=50,100$的BER仿真结果。从图4中可以观察到，MC-DCSK-LRAM系统的BER比MC-DCSK系统显著更低，且当β更小时BER显著降低。图4(b)给出了$M=64,128$, $\beta=150$时的仿真结果，由该图可知当M更大时可取得更低的BER。同时，图4表明：通过使用LRAM，可以有效地提升AWGN信道下MC-DCSK系统的BER性能。

进而，本文探究了所提方案在多径Rayleigh衰落信道下的性能。根据文献[3]中给出的多径Rayleigh衰落信道模型，多径信道的参数为$E[\lambda_1^2]=4/7$，$E[\lambda_2^2]=2/7$，$E[\lambda_3^2]=1/7$，$\tau_1=0$，$\tau_2=3$, $\tau_3=6$。其中$E[\lambda_1^2],E[\lambda_2^2],E[\lambda_3^2]$分别表示3条传输路径的能量，$\tau_1,\tau_2,\tau_3$分别表示3条传输路径的延时。

图5给出了在多径信道下不同参数β和M下的

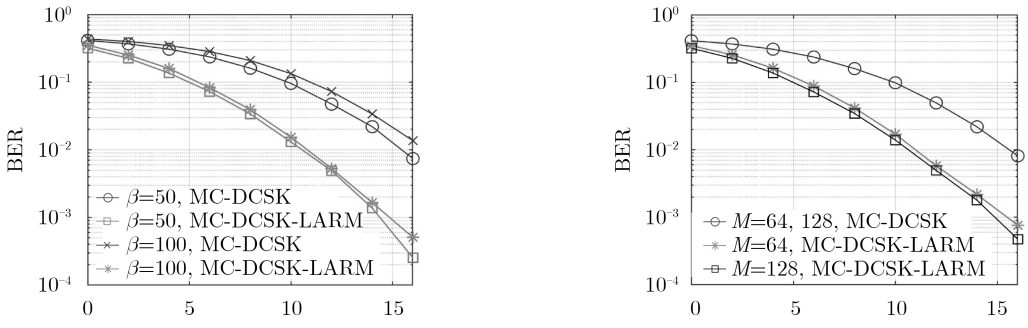


(a) M=128



(b) β=150

图 4 AWGN信道下BER性能与比较



(a) M=128　　(b) β=150

图 5 多径信道下BER性能与比较

BER仿真。从中可以观察得到：当参数为$M=128$, $\beta=50,100$以及$M=64,128$, $\beta=50$时, MC-DCSK-LRAM系统的BER均优于MC-DCSK系统。此外，与AWGN信道下的BER性能相似，β更小以及M更大时，MC-DCSK-LRAM系统可以获得相对更好的性能。

除此以外，图6分析了在多径衰落信道下时延对BER性能的影响。系统参数为$E_b/N_0=15$ dB, $\beta=50$, $M=64$。多径信道参数为$\mathrm{E}[\lambda_1^2]=4/7$, $\mathrm{E}[\lambda_2^2]=2/7$, $\mathrm{E}[\lambda_3^2]=1/7$, $\tau_1=0$, $\tau_2\in[1,40]$, $\tau_3=\tau_2+1$。如图6所示，随着时延τ_2的增加，MC-DCSK和MC-DCSK-LRAM系统的BER都会增加，但是当时延并不大的时候，MC-DCSK-LRAM系统依旧可以获得比MC-DCSK系统更好的BER性能。随着τ_2的增加，MC-DCSK-LRAM的性能逐渐恶化，逐渐接近于MC-DCSK的性能。

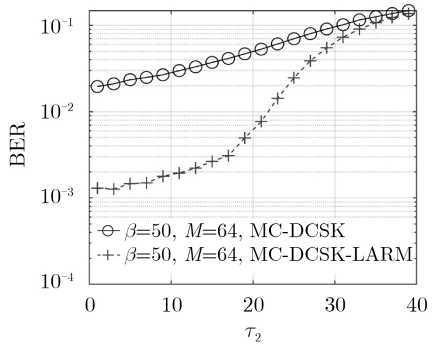
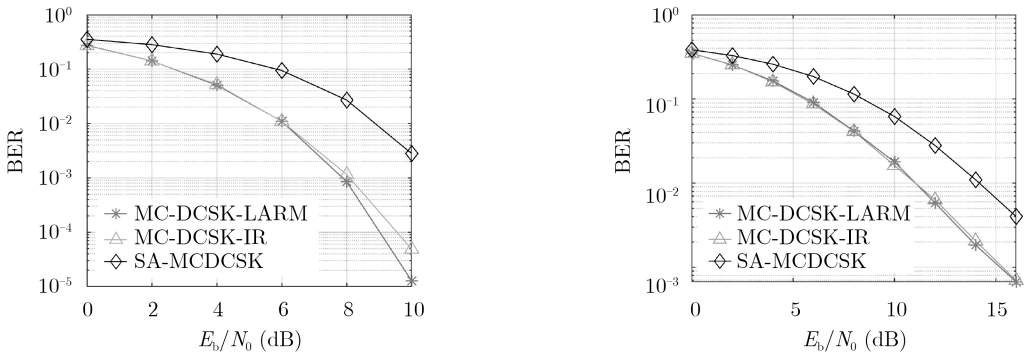


图 6 多径信道下MC-DCSK-LRAM接收机BER性能与时延关系

更进一步，本文将MC-DCSK-LRAM系统与其他可靠性方案如MC-DCSK-IR以及SA-MCDCSK方案在AWGN信道和多径衰落信道下的BER性能进行了比较。比较结果如图7所示，其中$\beta=50$, $M=64$。

图7(a)比较了在AWGN信道下的BER性能。可以很明显地看出MC-DCSK-LRAM比另外两种方案性能更好，特别是在高信噪比情况下MC-DCSK-LRAM的BER性能略优于MC-DCSK-IR。这是因为虽然MC-DCSK-IR系统通过迭代解调理论上能够得到最优解，但是在实际系统中迭代性能受制于有限的β和M值，在高信噪比处迭代解调的精度略低于MC-DCSK-LRAM的等效最大似然检测。

图7(b)则给出了在多径衰落信道下的BER性能。其中多径信道条件为$\mathrm{E}[\lambda_1^2]=4/7$, $\mathrm{E}[\lambda_2^2]=2/7$, $\mathrm{E}[\lambda_3^2]=1/7$, $\tau_1=0$, $\tau_2=3$, $\tau_3=6$。如图所示，由于多径传播效应，MC-DCSK-IR以及MC-DCSK-LRAM系统的BER性能接近。此外，从图中可观察到，两者性能均优于SA-MCDCSK系统。



(a) AWGN信道　　(b) 多径信道

图 7 MC-DCSK-LRAM系统与MC-DCSK-IR系统、SA-MCDCSK系统的性能比较

6 结束语

本文针对MC-DCSK系统中参考混沌信号的传输差错将导致接收端的可靠性下降的问题，基于共享参考混沌信号的多路混沌调制信号具有相关性因而信号矩阵具有低秩性的特点，提出矩阵低秩估计检测的方法，对接收信号进行近似估计，进而得到参考混沌信号的最大似然估计，提高了参考混沌信号的检测精度。更进一步，本文将其用于解调混沌调制信号，并证明了应用矩阵低秩估计方法，可等效实现接收信息的最大似然估计，从而提升了MC-DCSK系统的传输可靠性。在此基础上，本文对AWGN信道和多径衰落信道上的MC-DCSK系统BER性能进行了仿真，并与传统的MC-DCSK系统以及改进的MC-DCSK系统的BER性能进行了比较和分析。结果表明，基于矩阵低秩估计的MC-DCSK-LRAM系统在不改变发射端结构、无需传输多路参考混沌信号的条件下，取得了更优的传输可靠性。因此，本文的研究成果易于推广应用到现有的混沌通信系统中，具有较强的实用性。未来可进一步开展的研究工作包括进一步探究多用户混沌通信系统中矩阵低秩估计检测方法的应用及其性能评估。

参 考 文 献

[1] 李付鹏, 刘敬彪, 王光义, 等. 基于混沌集的图像加密算法[J]. 电子与信息学报, 2020, 42(4): 981–987. doi: 10.11999/JEIT190344.
LI Fupeng, LIU Jingbiao, WANG Guangyi, *et al*. An image encryption algorithm based on chaos set[J]. *Journal of Electronics & Information Technology*, 2020, 42(4): 981–987. doi: 10.11999/JEIT190344.

[2] HU Wei, WANG Lin, CAI Guofa, *et al*. Non-coherent capacity of *M*-ary DCSK modulation system over multipath Rayleigh fading channels[J]. *IEEE Access*, 2016, 5: 956–966. doi: 10.1109/ACCESS.2016.2623798.

[3] KADDOUM G, RICHARDSON F D, and GAGNON F. Design and analysis of a multi-carrier differential chaos shift keying communication system[J]. *IEEE Transactions on Communications*, 2013, 61(8): 3281–3291. doi: 10.1109/TCOMM.2013.071013.130225.

[4] ZHOU Hongmin, ZHANG Ying, and YU Ying. Noise reduction multi-carrier differential chaos shift keying system[J]. *Journal of Circuits, Systems and Computers*, 2018, 27(14): 1850233. doi: 10.1142/S021812661850233X.

[5] YANG Hua, JIANG Guoping, TANG W K S, *et al*. Multi-carrier differential chaos shift keying system with subcarriers allocation for noise reduction[J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2018, 65(11): 1733–1737. doi: 10.1109/TCSII.2017.2752754.

[6] CHEN Bingjun, ZHANG Lin, and WU Zhiqiang. General iterative receiver design for enhanced reliability in multi-carrier differential chaos shift keying systems[J]. *IEEE Transactions on Communications*, 2019, 67(11): 7824–7839. doi: 10.1109/TCOMM.2019.2939799.

[7] CHEN Pingping, WANG Lin, and LAU F C M. One analog STBC-DCSK transmission scheme not requiring channel state information[J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2013, 60(4): 1027–1037. doi: 10.1109/TCSI.2012.2209304.

[8] 张刚, 孟维, 张天骐. 多用户分段移位差分混沌键控通信方案[J]. 电子与信息学报, 2017, 39(5): 1219–1225. doi: 10.11999/JEIT160795.
ZHANG Gang, MENG Wei, and ZHANG Tianqi. Multiuser communication scheme based on segment shift differential chaos shift keying[J]. *Journal of Electronics & Information Technology*, 2017, 39(5): 1219–1225. doi: 10.11999/JEIT160795.

[9] KONSTANTINIDES K, NATARAJAN B, and YOVANOF G S. Noise estimation and filtering using block-based singular value decomposition[J]. *IEEE Transactions on Image Processing*, 1997, 6(3): 479–483. doi: 10.1109/83.557359.

[10] ZHOU Xiaowei, YANG Can, ZHAO Hongyu, *et al*. Low-rank modeling and its applications in image analysis[J]. *ACM Computing Surveys*, 2014, 47(2): 36. doi: 10.1145/2674559.

[11] LIU Guangcan, LIN Zhouchen, and YU Yong. Robust subspace segmentation by low-rank representation[C]. The 27th International Conference on International Conference on Machine Learning, Madison, USA, 2010: 663–670.

[12] FRIEDLAND S, NIKNEJAD A, KAVEH M, *et al*. Fast Monte-Carlo low rank approximations for matrices[C]. 2006 IEEE/SMC International Conference on System of Systems Engineering, Los Angeles, USA, 2006: 218–223. doi: 10.1109/SYSOSE.2006.1652299.

[13] YE Jieping. Generalized low rank approximations of matrices[J]. *Machine Learning*, 2005, 61(1/3): 167–191. doi: 10.1007/s10994-005-3561-6.

张 琳：女，1976年生，副教授，研究方向为无线通信、混沌调制、智能信息传输等.

陈炳均：男，1995年生，硕士生，研究方向为高可靠性数字混沌通信系统等.

吴志强：男，1973年生，教授，研究方向为无线通信、调制识别与混叠信号检测、大数据与智能信息传输等.

责任编辑：余 蓉