基于可逆元胞自动机的非正交分组加密码索引调制方案

马英杰[1]，王丹[2]，赵耿[1]，徐凤麟[1]，刘岳恒[2]
（1.北京电子科技学院电子与通信工程系，北京 100070；2.北京电子科技学院网络空间安全系，北京 100070）

摘　要：为满足6G网络的高速率通信和强安全通信需求，针对码索引调制（CIM）技术，提出了一种基于可逆元胞自动机的非正交分组加密码索引调制方案。构造了一种混杂可逆初等元胞自动机，通过多规则扩展、异或运算及序列逆序迭代增强序列随机性。信息流分为调制块和映射块，调制块分组后经过元胞自动机加密，其迭代规则和扩频码由映射块确定。仿真结果表明，所提方案的误码率性能与现有方案相比提升了约0.3~9 dB，密钥空间达到2^{209}，且加密后图像的直方图像素分布均匀，有效提高了通信系统的安全性和鲁棒性。

关键词：码索引调制；扩频传输；可逆初等元胞自动机；频谱效率
中图分类号：TN918.1
文献标志码：A
DOI：10.11959/j.issn.1000−436x.2025081

Nonorthogonal group encryption code index modulation scheme based on reversible cellular automata

MA Yingjie[1], WANG Dan[2], ZHAO Geng[1], XU Fenglin[1], LIU Yueheng[2]
1. Department of Electronic and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China
2. Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: To meet the high-rate communication and strong security communication requirements of 6G networks, a non-orthogonal grouping encryption code index modulation (NGECIM) scheme based on reversible cellular automata for code index modulation technology was proposed. A hybrid reversible elementary cellular automata (HRECA) was constructed, which enhanced the randomness of the sequence through multi-rule expansion, XOR operations, and sequence reverse iteration. The information flow was divided into modulation blocks and mapping blocks. After grouping, the modulation blocks were encrypted using cellular automata, with the iteration rules and spreading codes determined by the mapping blocks. Simulation results show that the proposed scheme improves the error rate performance by approximately 0.3~9 dB compared to existing schemes. The key space reaches 2^{209}, and the histogram pixel distribution of the encrypted image is uniform. This effectively improves the security and robustness of the communication system.

Keywords: CIM, spread spectrum transmission, reversible elementary cellular automata, spectral efficiency

0　引言

自5G商用以来，无线通信领域在发展模式、架构设计和安全性等方面迎来诸多挑战。随着6G中新兴使能技术的不断发展，通信系统的传输速率、能耗效率、安全性以及可靠性等多方面都需要提高。索引调制（IM, index modulation）是一种高效简单的调制技术，其使用通信系统中某些资源的索引来传送额外的信息。与传统的通信系统相比，

收稿日期：2025−01−05；修回日期：2025−04−21
通信作者：王丹，wangdan202305@163.com
基金项目：国家自然科学基金资助项目（No.62441208）；中央高校基本科研业务费资金资助项目（No.3282024060）
Foundation Items：The National Natural Science Foundation of China (No.62441208), The Fundamental Research Funds for the Central Universities (No.3282024060)

IM 技术在频谱效率、能量效率、抗干扰性能和硬件复杂度方面展现出了显著优势，在无线通信领域引起了广泛关注。IM 技术先后被应用于空域索引调制[1-3]和频域索引调制[4-6]，两者分别通过天线资源和子载波资源隐性传输部分信息比特。文献[7]将 IM 技术与直接扩频技术结合提出了码索引调制（CIM, code index modulation）技术，该技术将扩频码作为索引资源，选取部分信息比特映射为扩频码的索引值，根据索引表选择不同扩频码对另一部分信息比特扩频调制传输，接收端反向查找索引表恢复隐性传输的信息比特。虽然 CIM 技术具有更高的频谱效率且隐蔽性更好，但是需要消耗大量的扩频码索引资源，并且随着频谱效率的提升，所需的伪随机（PN, pseudo random）码数量呈指数级增加，这限制了其在实际应用中的性能。文献[8]将分组排序思想引入 CIM，通过索引值排序后为各组调制符号集中选取扩频码来降低伪随机码的耗费量，但是增加了接收端重新排序的计算复杂度。文献[9]提出了非正交-码索引调制（N-CIM, nonorthogonal-CIM）方案，通过选取相同的扩频码对调制符号的同相分量和正交分量进行扩频来降低系统的误码率，但耗费的扩频码数量随频谱效率的提升呈指数型增长。文献[10]结合文献[8-9]的思想提出了非正交分组-码索引调制（NG-CIM, nonorthogonal grouping-CIM）方案，在保证系统误码率性能的同时有效降低了伪随机码的消耗量，但是选择相同的扩频码在一定程度上降低了系统的隐蔽性和安全性，在视障信道中容易被窃听。为了提高通信系统的安全性，多种基于 CIM 的安全传输方案相继被提出。文献[11-12]提出了将扩频码域和波束域相结合的混合码域索引调制（CDIDM, code-domain index modulation with directional modulation）方案，通过角度隐蔽技术来提高系统的安全性和误码率性能。然而，随着扩频码数量的增加，误码率性能逐渐下降。文献[13-14]结合循环移位键控和码索引调制，同时提高了系统的频谱效率和安全性，但系统误码率性能较差。文献[15-16]将可逆初等元胞自动机（ECA, elementary cellular automata）引入码索引调制通信系统中进行加密，使用混沌规则的初等元胞自动机扩展扩频码，在降低系统误码率性能的同时保证了通信系统的安全性。但是该方案中初等元胞自动机产生的序列存在周期短和相关性高等问题。

为了在提高通信系统传输安全性的同时降低码索引调制方案的误码率，本文提出了一种基于可逆元胞自动机（CA）的非正交分组加密码索引调制（NGECIM, nonorthogonal grouping encryption CIM）方案，主要贡献如下。

1) 在可逆元胞自动机的基础上扩展，构造了一种混杂可逆初等元胞自动机（HRECA, hybrid reversible ECA）。将可逆初等元胞自动机的单一规则扩展为多规则进行迭代，并改变元胞自动机迭代的方式。每次根据可逆规则更新元胞状态值后，将左右两部分的元胞状态值进行异或运算，异或结果覆盖右侧的元胞状态值，最后将整个序列的逆序作为下一时刻的元胞状态值。与可逆初等元胞自动机相比，HRECA 生成的伪随机序列具有更高的复杂性、更低的自相关性和互相关性，将其应用于物理层数据加密可以提高通信系统的安全性和可靠性。

2) 提出了一种基于可逆元胞自动机的非正交分组加密码索引调制方案。发送端将信息比特分为调制块和映射块两部分，调制块在比特分组后通过 HRECA 对各组调制比特进行加密。各组调制比特作为 HRECA 的元胞状态初始值进行迭代，其中 HRECA 的迭代规则由映射比特在规则选择表中进行选择，同时映射比特对加密后的各组调制比特选取对应的扩频码组进行扩频处理，其中同一组调制符号的同相分量和正交分量使用相同的扩频码。在接收端合并同相和正交支路的信号，通过最大相关检测得到映射比特，反向查找选择表得到各组的扩频码，确定加密迭代规则，将接收端信号解扩后再使用 HRECA 反向迭代解密得到原始调制比特。加密后的调制比特具有更好的随机性，能有效地将某些高误差率的比特分散开，进行数字调制时可以减少错误的集中，从而能够在提高通信系统安全性的同时降低系统误码率。

1　系统模型

1.1　混杂可逆初等元胞自动机

元胞自动机理论最早由冯 • 诺依曼提出[17]，是一种在时间和空间上都离散的动力学系统，由一系列相同的单元格组成，这些单元格在一维或多维空间中规则排列从而构成元胞空间，每个元胞的下一个状态取决于它自身状态和周围邻居的当前状态[18]。初等元胞自动机是在一维空间中进行演化

的CA，元胞的状态仅限于0和1，并且元胞下一时刻的状态根据其自身状态及其左右相邻的2个元胞的状态确定。ECA的迭代公式可表示为

$$S_{t+1}(i)=f_R\left[S_t(i-1),S_t(i),S_t(i+1)\right] \tag{1}$$

其中，f_R表示局部转换函数，$S_t(i)$表示t时刻第i个元胞的状态值。Wolfram根据ECA的迭代方式将其迭代规则分为固定规则、周期规则、复杂规则和混沌规则[19]。可逆ECA是ECA中一种特殊的类型，其全局函数确保了每次状态转换都是一一映射的。在周期性ECA中，迭代规则一共有256种，其中有6种可逆的迭代规则{15,51,85,170,204,240}。表1是ECA No.85的迭代规则，其中，t表示当前时刻，$t+1$表示下一时刻。以110为例，当左侧元胞状态值为1，本身元胞状态值为1，右侧元胞状态值为0时，下一时刻该元胞状态值为1。在$t+1$时，8个状态组成的二进制数（01010101），即十进制的85[17]。

表1 ECA No.85的迭代规则

时刻	元胞状态值							
t	111	110	101	100	011	010	001	000
t+1	0	1	0	1	0	1	0	1

本文提出的混杂可逆初等元胞自动机，在每次迭代时同时选用2种及以上的ECA迭代规则进行迭代，在HRECA中每个元胞的状态会根据其自身状态和周围元胞的状态进行更新，这个更新过程可以使用不同的迭代规则来实现。 以双规则HRECA为例，其模型如图1所示。在图1中，HRECA包含了L个元胞，R1和R2分别表示2种不同的可逆迭代规则，采用周期型边界。在分界线左侧的元胞，遵循R1迭代规则进行演化，序号为1的元胞的下一状态值由序号为$\frac{L}{2}$和2的元胞以及该元胞的当前状态值决定，序号为$\frac{L}{2}$的元胞的下一状态值由序号为$\frac{L}{2}-1$和1的元胞以及该元胞的当前状态值决定。在分界线右侧的元胞，遵循R2迭代规则进行演化，序号为$\frac{L}{2}+1$的元胞的下一状态值由序号为L和$\frac{L}{2}+2$的元胞以及该元胞的当前状态值决定，序号为L的元胞的下一状态值由序号为$L-1$和$\frac{L}{2}+1$的元胞以及该元胞的当前状态值决定。每一次迭代后对两侧的元胞状态值进行异或运算，并将异或结果作为右侧的元胞状态值。最后将整个序列逆置，并将逆置后的序列作为下一次迭代的元胞状态初始值，HRECA的演化方式可表示为

$$c_i^{t'}=\phi\left(c_{i-1}^{t},c_i^{t},c_{i+1}^{t}\right) \tag{2}$$

$$\boldsymbol{C}_L^{t+1}=\delta\left(\boldsymbol{C}_1^{t'},\boldsymbol{C}_1^{t'}\oplus\boldsymbol{C}_{\frac{L}{2}+1}^{t'}\right) \tag{3}$$

其中，c_i^t表示第i个元胞在t时刻的状态值，ϕ表示元胞自动机的迭代函数，$\boldsymbol{C}_1^{t'}=\left(c_1^{t'},c_2^{t'},\cdots,c_{\frac{L}{2}}^{t'}\right)$，$\boldsymbol{C}_{\frac{L}{2}+1}^{t'}=\left(c_{\frac{L}{2}+1}^{t'},c_{\frac{L}{2}+2}^{t'},\cdots,c_L^{t'}\right)$，$\oplus$表示异或运算，$\delta$表示逆置运算，$\boldsymbol{C}_L^{t+1}$表示$L$个元胞在$t+1$时刻的状态值序列。

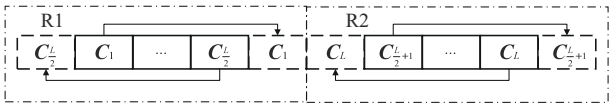


图1 双规则HRECA模型

假设ECA的元胞数量为100，迭代100次，图2展示了不同规则下ECA的迭代结果。从图2(a)和图2(b)可以看出，15号和51号规则下的元胞空间都随时间变化呈现出规则的迭代状态。从图2(c)可以看出，15号和51号在双规则HRECA下的元胞空间很快进入不规则的迭代状态，其动力学行为也保持在不规则迭代状态，并且随着迭代次数的增加，整个元胞空间会呈现出混沌状态，产生的序列中1和0的数量趋于平衡且具有较好的伪随机性。

1.2 发射机模型

本文提出的NGECIM方案的发射机模型如图3所示。在发射端，信息比特经串并转换后分为调制比特和映射比特两部分，首先将调制比特分为若干组，每组比特数相同，然后使用HRECA对各组调制比特进行加密，各组调制比特作为HRECA的元胞状态初始值进行迭代，其中HRECA的迭代规则和各组调制比特所需的扩频码组均由映射比特决定，加密完成后将各组调制比特映射为多组调制符号，并且每组调制符号的正交分量和同相分量使用相同的扩频码，最后经过载波调制合并发射信号。

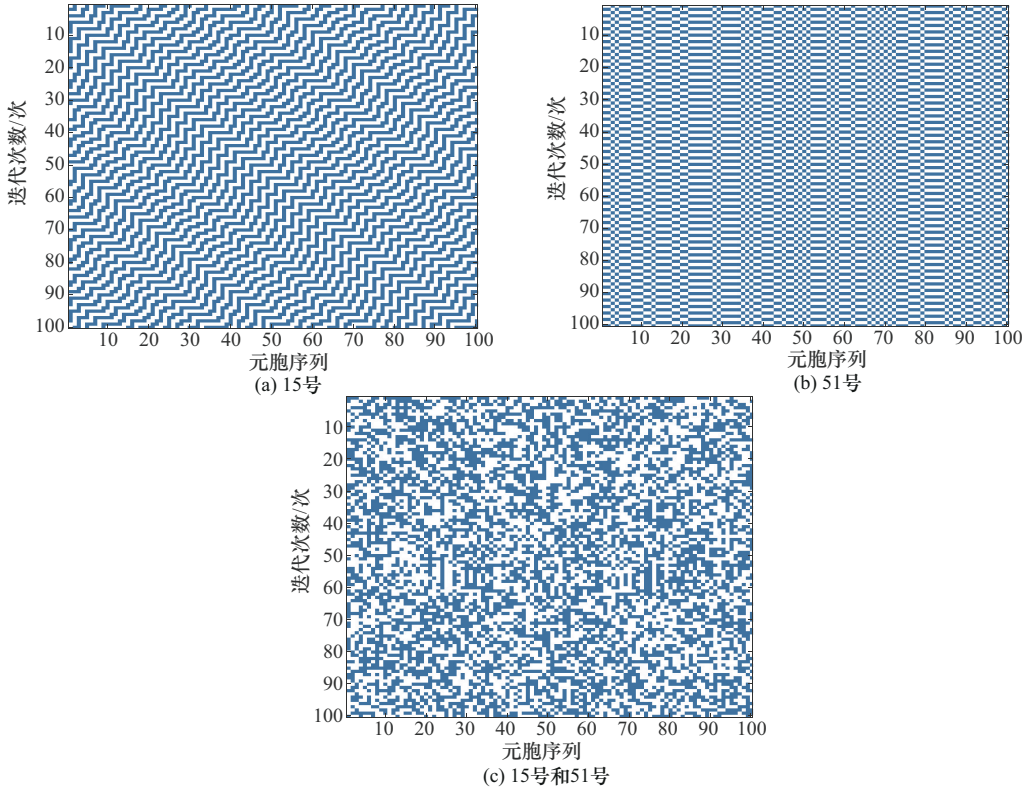


图2　不同规则下ECA的迭代结果

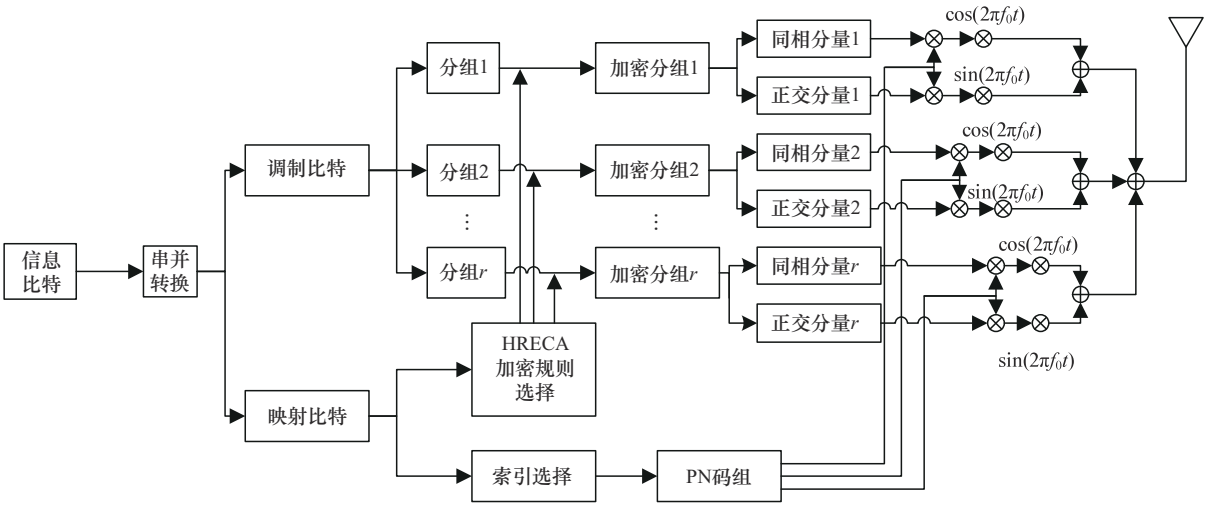


图3　NGECIM发射机模型

假设分组数为r，使用正交振幅调制（QAM, quadrature amplitude modulation），调制阶数为M，第t个传输时隙的信息比特$\boldsymbol{b}_t$可表示为

$$\boldsymbol{b}_t = [b_{1,t}, b_{2,t}, \cdots, b_{r,t}, b_{n,t}] \tag{4}$$

其中，$b_{r,t}$表示第t个时隙的第r组调制比特，$b_{n,t}$表示第t个时隙的映射比特。加密后的调制比特表示为$\boldsymbol{b}_t^e = [b_{1,t}^{e_1}, b_{2,t}^{e_2}, \cdots, b_{r,t}^{e_r}]$，其中，$\boldsymbol{b}_t^e = \partial(\boldsymbol{b}_t, e)$，$\partial$表示加密函数，$e$表示迭代规则，迭代规则集合为$\{e_1, \cdots, e_{r'}\}$。调制比特数$Z_m = r\mathrm{lb}\,M$，映射比特数为$Z_n$，扩频码集为$\{\boldsymbol{h}_1, \cdots, \boldsymbol{h}_n\}$，其中第$i$个扩频码序列表示为$\boldsymbol{h}_i = [h_{i,1}, \cdots, h_{i,L}]$，$L$表示扩频码长。NGECIM所需扩频码的数量$n$满足式(5)。

$$\binom{n}{r} \geqslant 2^{Z\_n} \tag{5}$$

其中，$\binom{n}{r}$表示从n个扩频码中选择r个组合数，即n取得最小值以保证扩频码资源的消耗量最低。在第t个时隙，第r个加密后的调制比特分组经过数字调制后可表示为

$$x(t) = a_{t,r} + \mathrm{j}b_{t,r} \tag{6}$$

其中，$a_{t,r}$表示调制符号的实部，$b_{t,r}$表示调制符号的虚部。在一个传输时隙中的总比特数可表示为

$$Z = Z\_m + Z\_n \tag{7}$$

各组调制符号经载波合并后发送的信号表示为

$$y(t)=\sum_{i=1}^{G}\sum_{r=1}^{R}\sum_{k=1}^{L}\{a_{i,r}h_{i,k}P(t-(iL+k)T_c)\cos(2\pi f_0 t)+ b_{i,r}h_{i,k}P(t-(iL+k)T_c)\sin(2\pi f_0 t)\} \tag{8}$$

其中，G表示传输时隙的个数，R表示调制比特分组的个数，L表示扩频码的长度，$a_{i,r}$表示第i个时隙的第r组调制符号的实部，$b_{i,r}$表示第i个时隙的第r组调制符号的虚部，$h_{i,k}$表示第i个时隙扩频码的第k个码片，$P(t)$表示矩阵脉冲成型函数，T_c表示码片的长度，f_0表示载波频率。

1.3 加密规则选择方式

在每一个传输时隙中，映射比特决定了各组调制比特加密的迭代规则。当分组数为2、映射比特数为2、HRECA为双规则迭代时，加密规则选择如表2所示。当映射比特为01时，第一组调制比特的迭代规则为(e_1,e_2)，第二组调制比特的迭代规则为(e_1,e_4)。

表2 HRECA加密规则选择

映射比特	迭代规则
00	(e_1,e_2)、(e_1,e_3)
01	(e_1,e_2)、(e_1,e_4)
10	(e_1,e_2)、(e_1,e_5)
11	(e_1,e_2)、(e_1,e_6)

1.4 扩频码映射方式

同样地，映射比特还需要映射为扩频码索引，并根据索引选择为各组加密后的调制符号选择相应的扩频码。当分组数为3、每一组的调制比特数为2、映射比特数为3时，所需扩频码的数量满足式(9)。

$$\binom{n}{3} \geqslant 2^3 \tag{9}$$

因此n的值取5，即扩频码的数量为5。扩频码索引选择如表3所示。当映射比特为011时，选择扩频码索引h_1、h_3和h_4，分别为3组调制符号扩频。

表3 扩频码索引选择

映射比特	扩频码索引
000	h_1、h_2、h_3
001	h_1、h_2、h_4
010	h_1、h_2、h_5
011	h_1、h_3、h_4
100	h_1、h_3、h_5
101	h_1、h_4、h_5
110	h_2、h_3、h_4
111	h_2、h_3、h_5

1.5 接收机模型

NGECIM接收机模型如图4所示。接收端接收到的信号可表示为

$$r(t) = s(t)y(t) + g(t) \tag{10}$$

其中，$r(t)$表示接收端信号，$s(t)$表示信道系数，$g(t)$表示均值为0、方差为$\frac{N_0}{2}$的高斯白噪声函数。在理想情况下，接收到的信号经载波恢复后可以表示为

$$r(t) = \sum_{i=1}^{G}\sum_{r=1}^{R}\sum_{k=1}^{L}\{s_i(t)(a_{i,r}+\mathrm{j}b_{i,r})h_{i,k}P(t-(iL+k)T_c)+g(t)\} \tag{11}$$

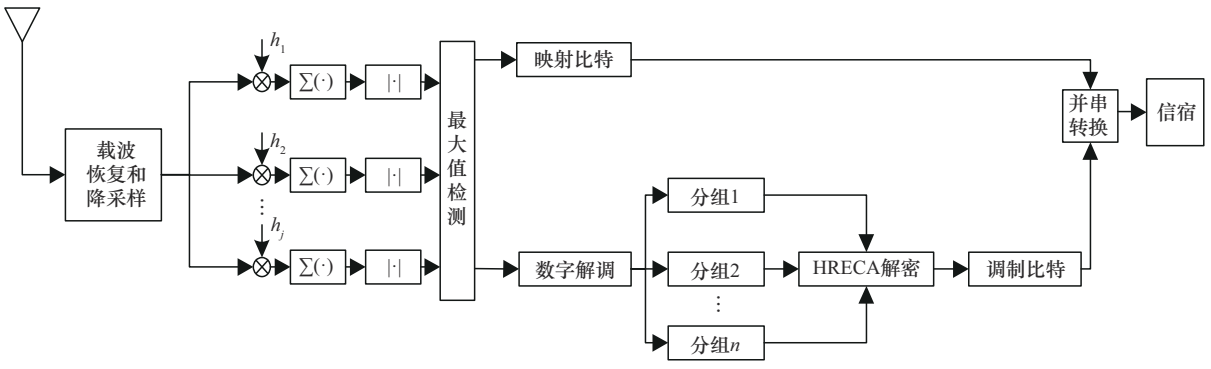


图4 NGECIM接收机模型

接收端信号经过载波恢复后，首先进行最大相关检测，将$r(t)$与n个相关器做相关运算并求和，由于每一组调制符号的同相和正交支路选择的扩频码相同，因此可以将两支路合并检测以增大检测的正确性。第i个传输时隙的第n_j个相关器的输出可表示为

$$r_{i,n_j}=\sum_{r=1}^{R}\sum_{k=1}^{L}\left\{\left|s_i\right|^2(a_{i,r}+\mathrm{j}b_{i,r})h_{n,i,k}h_{n_j,i,k}+s_ih_{n_j,i,k}f_{n_j,i}\right\} \tag{12}$$

进一步化简为

$$r_{i,n_j}=\begin{cases}\pm\left|s_i\right|^2(a_i+b_i)E_s+v_{i,n_j},n=n_j\\ v_{i,n_j},n\neq n_j\end{cases} \tag{13}$$

其中，$E_s=\sum_{k=1}^{L}h_{i,n_j,k}^2$表示一个周期内扩频码的能量，$v_{i,n_j}=\sum_{k=1}^{L}s_ih_{i,n_j,k}f_{i,n_j}$表示相关器的输出噪声。取运算结果$r_{i,n_j}$的绝对值进行对比，前$r$个最大值即$r$组调制符号的同相分量和正交分量，其表达式为

$$n_j'=\arg\max_n\left\{\left|r_{i,n_j}\right|\right\} \tag{14}$$

其中，n_j'表示经检测后确定的扩频码索引值。根据其对应的输出值r_{i,n_j}进行解调处理，同时根据n_j'查询扩频码索引选择表获得相应的映射比特信息，然后根据映射比特信息查找HRECA加密规则选择表，确定发送端各组调制比特加密时选择的迭代规则，并通过HRECA解密得到各组的原始调制比特，经过分组合并及并串转换后恢复信息比特。

1.6　复杂度分析

在不同的扩频通信方案中，可以通过比较每个传输时隙内的扩频和解扩运算次数，评估各个方案的复杂度和性能。本节分析NGECIM方案的复杂度，并与已有方案NG-CIM[10]、非正交码移键控和码索引调制（N-CSK-CIM）[13]、结合循环移位键控和码索引调制的混合差分混沌键控（CSK-CIM-DCSK）[14]和扩展码索引调制（E-CIM）[15]进行对比。假设上述方案的频谱效率一致，映射比特长度为n_c，NG-CIM方案和NGECIM方案的分组数均为r，CSK-CIM-DCSK方案采用DCSK调制传递一位比特，CSK-CIM-DCSK和N-CSK-CIM中CSK传输比特数为n_{csk}，且扩频码个数n满足式(15)。

$$\binom{n}{r}\geqslant 2^{n_c} \tag{15}$$

在发送端，N-CSK-CIM和E-CIM方案需要执行2次扩频运算，CSK-CIM-DCSK方案需要执行1次扩频运算。由于分组数为r，NG-CIM和NGECIM方案需要执行$2r$次的扩频运算。在上述5种方案中，调制符号的同相分量和正交分量都使用了相同的扩频码，因此在接收端，以上各方案都将同相和正交支路合并后再执行解扩运算，需要与发射端使用的扩频码进行相关运算。其中，NG-CIM和NGECIM方案需要执行n次解扩运算；E-CIM方案仅需要对同相支路进行相关运算和1次正交分量解扩，因此需要执行$2^{n_c}+1$次解扩运算；N-CSK-CIM和CSK-CIM-DCSK方案需要考虑到n_{csk}，因此需要执行$2^{n_c+n_{\mathrm{csk}}}$次解扩运算。表4展示了5种方案在相同频谱效率下的复杂度对比。当r=2、频谱效率为8 bit/(s·Hz)时，复杂度分别为CSK-CIM-DCSK（129次）、N-CSK-CIM（66次）、E-CIM（19次）、NG-CIM（11次）和NGECIM（11次）。当频谱效率为10 bit/(s·Hz)时，复杂度分别为CSK-CIM-DCSK（513次）、N-CSK-CIM（258次）、E-CIM（67次）、NG-CIM（16次）和NGECIM（16次）。进一步提升频谱效率至12 bit/(s·Hz)时，复杂度分别为CSK-CIM-DCSK（2 049次）、N-CSK-CIM（1 026次）、E-CIM（259次）、NG-CIM（28次）和NGECIM（28次）。由此可见，随着频谱效率的提高，N-CSK-CIM、CSK-CIM-DCSK和E-CIM方案的复杂度显著高于NG-CIM和NGECIM方案。

表4　复杂度对比

方案	扩频次数/次	解扩次数/次
N-CSK-CIM	2	$2^{n_c+n_{\mathrm{csk}}}$
CSK-CIM-DCSK	1	$2^{n_c+n_{\mathrm{csk}}}$
E-CIM	2	$2^{n_c}+1$
NG-CIM	$2r$	n
NGECIM	$2r$	n

2　仿真分析

2.1　误码率分析

本节对NGECIM方案的误码率性能进行仿真验证，扩频码选取64位的Walsh序列，在加性白高斯噪声环境下与NG-CIM[10]、N-CSK-CIM[13]和CSK-CIM-DCSK[14]方案进行对比。

映射比特数设置为2，NGECIM和NG-CIM方案分组数设置为2，采用4QAM，图5展示了频谱效

率为 6 bit/(s·Hz)时上述 4 种方案的误码率曲线。可以看出，当信噪比（SNR, signal-to-noise ratio）为 0 dB 时，NGECIM 方案的误码率低于 N-CSK-CIM 和 CSK-CIM-DCSK 方案，略高于 NG-CIM 方案。随着信噪比的增加，NGECIM 方案的误码率趋近于 NG-CIM 方案，当误码率降至 10^{-4} 时，NGECIM 与 NG-CIM 方案的信噪比均为 4.9 dB，NGECIM 与 N-CSK-CIM 方案相比性能提升约 0.7 dB，与 CSK-CIM-DCSK 方案相比性能提升约 8 dB。

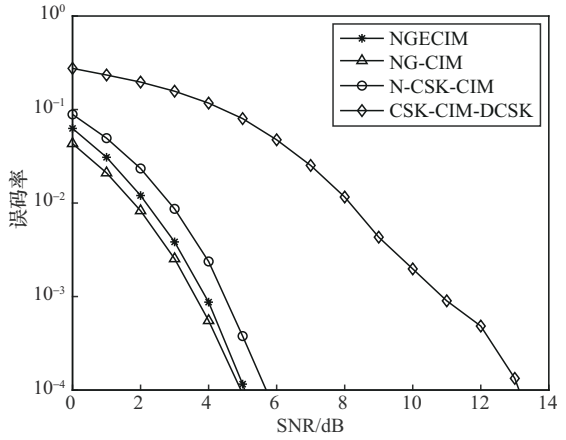


图 5 频谱效率为 6 bit/(s·Hz)时 4 种方案的误码率曲线

当映射比特数增至 3 时，其他条件保持不变，图 6 展示了频谱效率为 7 bit/(s·Hz)时上述 4 种方案的误码率曲线。可以看出，4 种方案的误码率性能与频谱效率为 6 bit/(s·Hz)时差别不大，但是在误码率还未降至 10^{-4} 时，NGECIM 方案的误码率曲线已经与 NG-CIM 方案的误码率曲线重合。当误码率为 10^{-4} 时，NGECIM 与 N-CSK-CIM 方案相比性能提升约 0.3 dB，与 CSK-CIM-DCSK 方案相比性能提升约 9 dB。

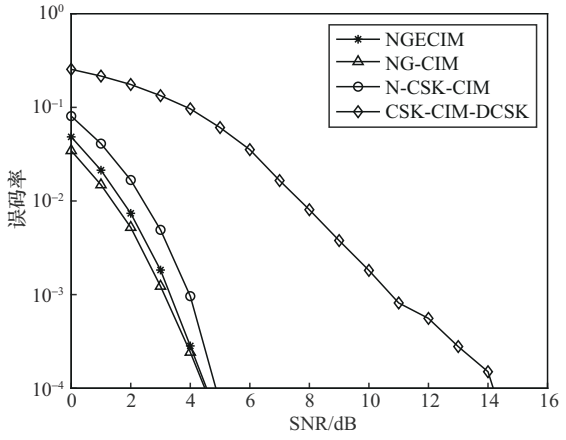


图 6 频谱效率为 7 bit/(s·Hz)时 4 种方案的误码率曲线

当调制阶数增加至 16QAM，映射比特数为 2，其他条件保持不变，图 7 展示了频谱效率为 10 bit/(s·Hz)时上述 4 种方案的误码率曲线。可以看出，当信噪比为 0 dB 时，NGECIM、N-CSK-CIM 与 NG-CIM 方案的误码率十分相近，CSK-CIM-DCSK 方案的误码率仍然显著高于其他 3 种方案。当误码率降至 10^{-2} 时，NGECIM 与 NG-CIM 方案的信噪比相同，之后 NGECIM 方案的性能逐渐优于 NG-CIM 方案。当误码率降至 10^{-4} 时，NGECIM 与 NG-CIM 方案相比性能提升约 0.5 dB，与 N-CSK-CIM 方案相比性能提升约 0.9 dB，与 CSK-CIM-DCSK 方案相比性能提升约 7 dB。

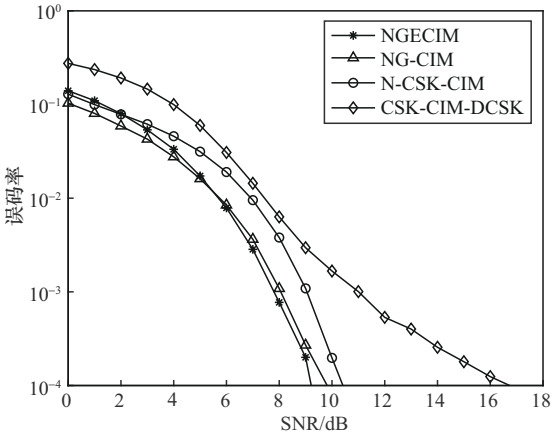


图 7 频谱效率为 10 bit/(s·Hz)时 4 种方案的误码率曲线

当扩频码个数均为 4 时，使用 64QAM、256QAM 和 1 024QAM 这 3 种不同的调制阶数，NG-CIM 和 NGECIM 方案的误码率曲线如图 8 所示。可以看出，当误码率降至 10^{-5}、调制阶数为 64 时，NGECIM 比 NG-CIM 方案性能提高约 1.3 dB；调制阶数为 256 时，NGECIM 比 NG-CIM 方案性能提高约 1.6 dB；调制阶数为 1 024 时，NGECIM 比 NG-CIM 方案性能提高约 2 dB。NGECIM 方案的误码率性能表现更优的原因是本文方案对原始调制比特进行加密，然后再进行扩频调制，避免了数据流中存在明显的周期性。加密后的调制比特的随机性更好，避免了高阶 QAM 星座点过于密集导致的误码率增加。通过分散高误差率的比特，减少错误的集中发生，从而提升了系统整体的误码率性能。

在调制阶数固定为 64 的情况下，图 9 展示了 NG-CIM 和 NGECIM 方案在不同 PN 码数量（4PN、

7PN、12PN）下的误码率曲线，2 种方案的分组数均为2。可以看出，在 PN 码个数为4、信噪比低于 7 dB 时，NGECIM 方案的误码率性能略差于 NG-CIM，但是当信噪比增加到 7 dB 以后，NGECIM 方案的误码率性能开始优于 NG-CIM，当误码率降至 10^{-5} 时，NGECIM 方案的误码率性能比 NG-CIM 提高约 1.3 dB。在 PN 码个数为 7、信噪比低于 11 dB 时，NGECIM 方案的误码率性能略差于 NG-CIM，当信噪比增加到 11 dB 以后，NGECIM 和 NG-CIM 方案的误码率曲线几乎重合。在 PN 码个数为 12 时，NGECIM 方案的误码率性能整体略差于 NG-CIM。这是因为扩频码数量的增加导致隐性传输的比特增多，隐性传输的容错能力较低导致误码率增加。

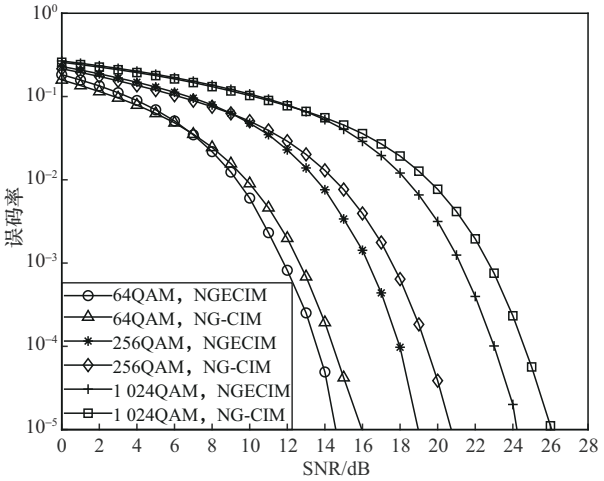


图8　不同调制阶数下 2 种方案的误码率曲线

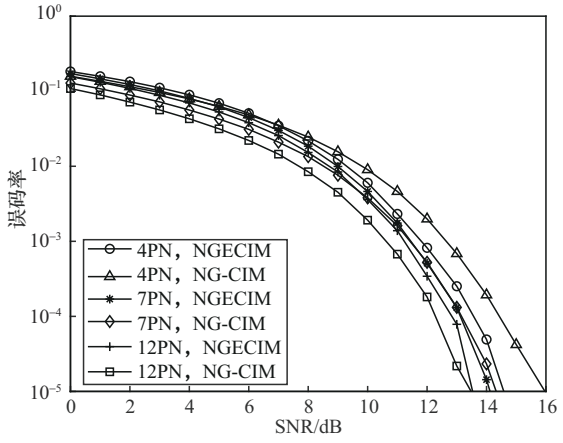


图9　不同扩频码数下 2 种方案的误码率曲线

2.2　安全性能分析

本节将对本文方案进行安全性能的评估，分析其密钥空间的规模、抵御统计攻击的能力以及系统的鲁棒性。

2.2.1　密钥空间分析

加密算法的安全性很大程度上取决于密钥的复杂度。本文所提 NGECIM 方案通过 HRECA 对各组调制比特加密。HRECA 的初始随机序列与调制比特异或后的结果作为 HRECA 的元胞状态初始值再迭代 100 次，其迭代规则由映射比特在规则选择表中选择。以双规则 HRECA 为例，共有 12 种迭代规则组合可以选择，分别是 {(204, 15)、(204, 85)、(204, 170)、(204, 240)、(170, 15)、(170, 51)、(170, 240)、(240, 51)、(240, 85)、(15, 51)、(15, 85)、(85, 51)}。元胞数量为 200，选择扩频码为 64 位的 Walsh 序列，因此系统密钥空间大小为 $2^{200} \times 12 \times 64 \approx 2^{209}$，明显超过 2^{128}，足以抵御暴力攻击。

2.2.2　统计攻击分析

统计攻击可以通过分析加密数据的统计特性推断出明文或密钥，在图像加密中，攻击者可能会通过分析密文图像的统计特征来获取有关明文图像的信息。直方图分析是统计攻击的一种常见形式，直方图反映了图像中像素值的出现频率，理想情况下，一个随机密文图像中的每个像素值出现频率应均等。本节选用 CVG-UGR 图像数据库中的 Cameraman、Barbara、Goldhill、Peppers 这 4 张灰度图像作为测试对象，图像尺寸为 512×512。图 10 模拟仿真了在信噪比为 14 dB 的条件下，发射端、窃听端及接收端的 Cameraman 图像及分布直方图。可以看出，发送端和接收端的图像直方图中像素分布不均且规律明显，而窃听端的图像直方图中像素分布均匀，无法从中提取任何有助于破解算法的统计信息，无法对系统实施有效的统计攻击。

相关性分析在图像加密中具有重要作用，它通过衡量相邻像素间的相关性来评估加密方案的性能。在理想情况下，密文图像的相邻像素相关性应接近零，这表明加密算法能有效隐藏原始图像的结构特征，从而抵御基于统计分析的攻击。本节将 4 张图像分别抽取 5 000 个像素点计算其相关系数大小，如表 5 所示。可以看出，加密前的 4 张图像在水平、垂直和对角方向上的相关系数接近 1，表明像素间存在高度相关性；加密后的 4 张图像在相同方向上的相关系数都接近 0，说明像素间的相关性显著降低。因此，本文方案能够有效抵抗统计攻击分析。

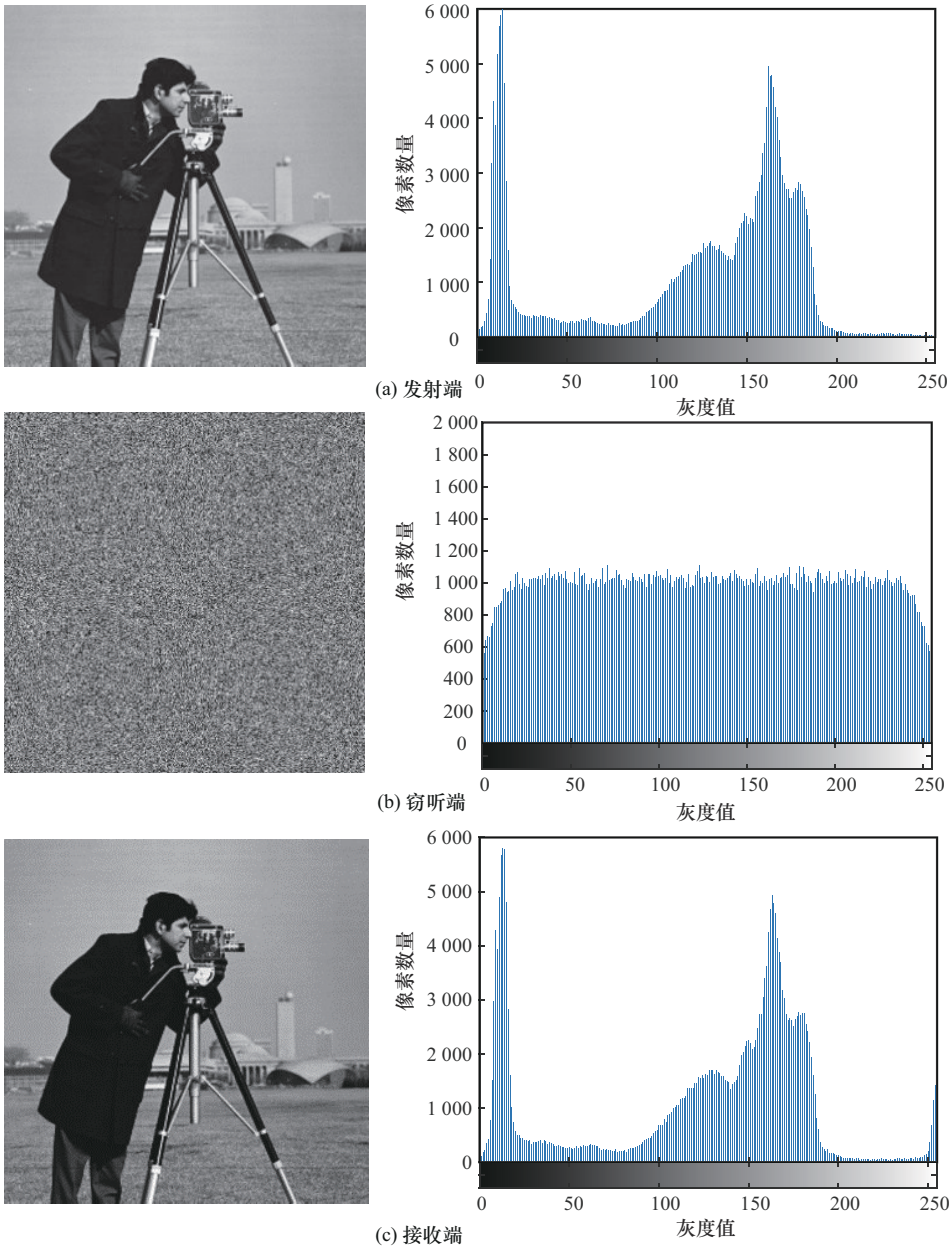


图 10　Cameraman 图像及分布直方图

表 5　　测试图像相关系数

图像	加密情况	水平	垂直	对角
Cameraman	加密前	0.975 9	0.979 3	0.969 0
	加密后	−0.009 3	−0.004 0	−0.045 2
Barbara	加密前	0.835 1	0.956 1	0.850 0
	加密后	−0.006 8	−0.009 5	−0.001 2
Goldhill	加密前	0.942 6	0.969 8	−0.963 2
	加密后	−0.008 3	−0.005 3	0.093 0
Peppers	加密前	0.977 2	0.978 0	0.959 9
	加密后	−0.005 3	−0.007 6	0.024 3

2.2.3　鲁棒性分析

鲁棒性是衡量图像加密方案在面对信道噪声干扰时保持图像质量的能力，通过对比不同信噪比条件下的图像恢复结果，可以评估加密方案在实际传输中的稳定性和可靠性。为了直观展示加密方案的鲁棒性，在不同信噪比条件下传输 Cameraman 图像，并对比 NGECIM 和 N-CSK-CIM[13]这 2 种方案的恢复图像质量，结果如图 11 所示。从图 11 中可以看出，在不同信噪比条件下，本文方案在接收端恢复的图像噪点更少，图像质量更接近原始图像。

(a1) SNR=6 dB　(a2) SNR=10 dB　(a3) SNR=14 dB

(a) N-CSK-CIM方案接收的图像

(b1) SNR=6 dB　(b2) SNR=10 dB　(b3) SNR=14 dB

(b) NGECIM方案接收的图像

图11　不同加密方案鲁棒性对比

峰值信噪比（PSNR, peak signal-to-noise ratio）和均方误差（MSE, mean squared error）是经典的图像质量评估指标。PSNR值越高，MSE值越低表示接收图像与原图相似度越高。以Cameraman、Barbara、Goldhill、Peppers这4张灰度图像为例，表6和表7分别展示了2种索引调制方案在不同信噪比下图像的PSNR和MSE值。可以看出，在相同信噪比情况下，NGECIM方案的PSNR值均比N-CSK-CIM方案高，NGECIM方案的MSE值均比N-CSK-CIM方案低。因此，本文方案的鲁棒性表现更优。

3　结束语

近年来，随着6G的研究不断提速，为满足更高的数据速率、频谱效率、高可靠性和高安全性等需求，码索引调制技术因其良好的抗干扰性和强信息隐蔽性得到广泛应用。本文为提升码索引调制系

表6　　**接收端图像PSNR值对比**

图像	方案	PSNR		
		SNR=6 dB	SNR=10 dB	SNR=14 dB
Cameraman	N-CSK-CIM	15.841 2	23.528 3	24.871 1
	NGECIM	18.017 3	24.699 7	24.871 5
Barbara	N-CSK-CIM	17.913 8	26.289 8	34.935 1
	NGECIM	19.374 2	29.486 5	36.269 9
Goldhill	N-CSK-CIM	17.987 1	26.480 4	34.680 2
	NGECIM	19.536 7	29.490 1	35.688 4
Peppers	N-CSK-CIM	18.477 4	25.860 0	34.687 6
	NGECIM	19.058 3	28.962 0	36.442 0

表7　　**接收端图像MSE值对比**

图像	方案	MSE		
		SNR=6 dB	SNR=10 dB	SNR=14 dB
Cameraman	N-CSK-CIM	1 694.165 3	288.568 3	211.821 3
	NGECIM	1 026.481 7	220.348 6	211.801 6
Barbara	N-CSK-CIM	1 051.234 5	152.790 3	20.872 1
	NGECIM	751.041 5	73.185 8	15.349 4
Goldhill	N-CSK-CIM	1 033.637 5	146.230 9	22.133 9
	NGECIM	723.453 0	73.126 2	17.548 5
Peppers	N-CSK-CIM	923.295 6	168.687 6	22.096 4
	NGECIM	807.704 8	82.581 6	14.752 9

统的误码率性能的同时提高通信系统的安全性能，首先提出了一个混杂可逆初等元胞自动机，将可逆初等元胞自动机的单一规则扩展为多规则进行迭代，同时改变其迭代方式使元胞自动机生成的伪随机序列具有更好的复杂性和随机性。然后提出了一种基于可逆元胞自动机的非正交分组加密码索引调制方案，在发射端将信息比特分为调制比特和映射比特两部分，调制比特分为数量相同的若干组，使用 HRECA 对各组调制比特进行加密。其中 HRECA 的迭代规则由映射比特决定，加密完成后将各组调制比特映射为多组调制符号，同时映射比特需要根据索引选择表为各组调制符号选择相应的扩频码进行扩频传输。使用 HRECA 对原始调制比特进行置乱加密，使置乱后的信号变得更加随机，通过分散高误差率的比特以降低系统的误码率。仿真结果表明，NGECIM 方案的误码率性能与 N-CSK-CIM 方案相比提升约 0.3~0.9 dB，与 CSK-CIM-DCSK 方案相比提升约 7~9 dB。随着频谱效率的提升，增加调制比特数相较于增加映射比特数能带来更好的误码率性能表现，NGECIM 方案相较于 NG-CIM 在误码率性能上约有 1.3~2 dB 的提升。此外，安全性分析验证了本文方案具有良好的安全性，密钥空间达到 2^{209} 足以抵抗暴力攻击；加密图像的直方图像素分布均匀，可以抵抗统计攻击；接收端恢复的图像噪点少，PSNR 和 MSE 值均证明本文方案具有较好的鲁棒性。未来，索引调制技术有望应用于 6G 空天地海协同信息网络中，特别是在高移动性通信场景中，以实现多尺度、跨媒介信息的高速、实时和可靠传输。

参考文献：

[1] ALBINSAID H, SINGH K, BISWAS S, et al. Block deep neural network-based signal detector for generalized spatial modulation[J]. IEEE Communications Letters, 2020, 24(12): 2775-2779.

[2] LAI I W, SHIH J W, LEE C W, et al. Spatial permutation modulation for multiple-input multiple-output (MIMO) systems[J]. IEEE Access, 2019, 7: 68206-68218.

[3] BITRA H, PONNUSAMY P. Performance analysis of adaptive generalized spatial modulation[C]//Proceedings of the 2020 International Conference on Artificial Intelligence and Signal Processing (AISP). Piscataway: IEEE Press, 2020: 1-6.

[4] DANG S P, MA G Q, SHIHADA B, et al. A novel error performance analysis methodology for OFDM-IM[J]. IEEE Wireless Communications Letters, 2019, 8(3): 897-900.

[5] LUONG T V, KO Y, VIEN N A, et al. Deep learning-based detector for OFDM-IM[J]. IEEE Wireless Communications Letters, 2019, 8(4): 1159-1162.

[6] BESSEGHIER M, GHOUALI S, DJEBBAR A B. Optimized greedy detection for OFDM-IM systems[J]. IEEE Communications Letters, 2023, 27(8): 2034-2037.

[7] KADDOUM G, AHMED M F A, NIJSURE Y. Code index modulation: a high data rate and energy efficient communication system[J]. IEEE Communications Letters, 2015, 19(2): 175-178.

[8] 邢峰英, 郑鹤, 刘永花, 等. 直接序列扩频分组映射码索引调制[J]. 电讯技术, 2017, 57(6): 703-709.
XING F Y, ZHENG H, LIU Y H, et al. Direct sequence spread spectrum block mapping code index modulation[J]. Telecommunication Engineering, 2017, 57(6): 703-709.

[9] 葛利嘉, 江治林, 冯胜, 等. 非正交-码索引调制方法[J]. 电子与信息学报, 2018, 40(10): 2331-2336.
GE L J, JIANG Z L, FENG S, et al. Non-orthogonal-code index modulation[J]. Journal of Electronics & Information Technology, 2018, 40(10): 2331-2336.

[10] 赵耿, 刘阿龙, 马英杰. 直接序列扩频非正交分组码索引调制技术研究[J]. 计算机仿真, 2023, 40(7): 249-253, 266.
ZHAO G, LIU A L, MA Y J. Research on direct sequence spread spectrum nonorthogonal groupingcode index modulation technology[J]. Computer Simulation, 2023, 40(7): 249-253, 266.

[11] YAO X, YANG P, LIU Z L, et al. A novel hybrid code-domain index modulation scheme[J]. IEEE Communications Letters, 2021, 25(10): 3403-3407.

[12] YAO X, YANG P, FU J L, et al. A hybrid multi-domain index modulation for covert communication[J]. IEEE Wireless Communications Letters, 2022, 11(1): 8-12.

[13] 刘学勇, 巴晓辉, 陈杰, 等. 非正交码移键控和码索引调制算法[J]. 系统工程与电子技术, 2021, 43(1): 232-236.
LIU X Y, BA X H, CHEN J, et al. Algorithm for non-orthogonal code shift keying and code index modulation[J]. Systems Engineering and Electronics, 2021, 43(1): 232-236.

[14] LIN Z X, XU W K, SUN H X, et al. A hybrid DCSK scheme combining cyclic shift keying and code index modulation[J]. IEEE Communications Letters, 2023, 27(9): 2303-2307.

[15] 赵耿, 黄思婕, 马英杰, 等. 基于可逆元胞自动机加密的扩展码索引调制方案[J]. 计算机科学, 2024, 51(6): 416-422.
ZHAO G, HUANG S J, MA Y J, et al. Extended code index modulation scheme based on reversible elementary cellular automata encryption[J]. Computer Science, 2024, 51(6): 416-422.

[16] MA Y J, HUANG S J, ZHAO G, et al. A switching chaotic coupled map lattices system based on elementary cellular automata and its applications[J]. International Journal of Bifurcation and Chaos, 2024, 34 (12): 1-22.

[17] 郭晓威, 郭亚军. 一种基于Rule30+细胞自动机的流密码设计方法[J]. 密码学报, 2020, 7(4): 439-452.
GUO X W, GUO Y J. An efficient stream cipher design based on Rule30+ cellular automaton[J]. Journal of Cryptologic Research, 2020, 7(4): 439-452.

[18] DONG Y H, ZHAO G. A spatiotemporal chaotic system based on pseudo-random coupled map lattices and elementary cellular automata[J]. Chaos, Solitons & Fractals, 2021, 151: 111217.

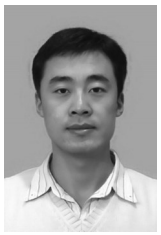
[19] 董有恒, 赵耿, 马英杰. 基于分区初等元胞自动机的二维伪随机耦合映像格系统及其动态特性[J]. 通信学报, 2022, 43(1): 71-82.
DONG Y H, ZHAO G, MA Y J. Two-dimensional pseudo-random coupled map lattices system based on partitioned elementary cellular automata and its dynamic properties[J]. Journal on Communications, 2022, 43(1): 71-82.

[作者简介]

马英杰（1979– ），女，吉林通化人，博士，北京电子科技学院副教授，主要研究方向为混沌保密通信等。

王丹（1999– ），女，河北保定人，北京电子科技学院硕士生，主要研究方向为混沌保密通信等。

赵耿（1964– ），男，四川苍溪人，博士，北京电子科技学院教授，主要研究方向为混沌密码与保密通信等。



徐凤麟（1977– ），男，山东高密人，北京电子科技学院讲师，主要研究方向为保密通信等。

刘岳恒（2001– ），男，吉林省吉林市人，北京电子科技学院硕士生，主要研究方向为混沌保密通信等。