基于 Walsh-Hadamard 变换的卷积码盲识别

刘 健[①] 王晓君[②③] 周希元[①③]
[①](西安电子科技大学 ISN 国家重点实验室 西安 710071)
[②](河北科技大学信息科学与工程学院 石家庄 050018)
[③](中国电子科技集团公司第五十四研究所 石家庄 050081)

摘 要：该文针对信道编码的盲识别问题，提出了高误码率下$(n,1,m)$卷积码的盲识别方法。首先给出了盲识别的数学模型，进而扩展了 Walsh-Hadamard 变换的应用范围。证明了通过对截获码序列做 Walsh-Hadamard 变换可以解决卷积码的盲识别问题，该方法在智能通信、信息截获、密码分析等领域有重要的应用。仿真实验表明该算法可以对高误码率的卷积码进行有效的识别。

关键词：盲识别；卷积码；高误码率；Walsh-Hadamard 变换
中图分类号： TP391; TP309 **文献标识码**：A **文章编号**：1009-5896(2010)04-0884-05
DOI: 10.3724/SP.J.1146.2009.00359

Blind Recognition of Convolutional Coding Based on Walsh-Hadamard Transform

Liu Jian[①] Wang Xiao-jun[②③] Zhou Xi-yuan[①③]
[①](*National Key Laboratory of ISN*, *Xidian University*, *Xi'an* 710071, *China*)
[②](*College of Information Science and Engineering*, *Hebei University of Science and Technology*, *Shijiazhuang* 050018, *China*)
[③](*The No.*54 *Research Institute of CETC*, *Shijiazhuang* 050081, *China*)

Abstract: In order to solve the problem of the blind recognition of channel coding, a method of blind recognition of $(n,1,m)$ convolutional coding in the high bit error rate condition is proposed. Firstly, the mathematical model of the blind recognition is given, and then the application field of walsh-hadamard transform is enlarged. The authors show that putting the intercepted codes walsh-hadamard transform can be used to solve the problem of blind recognition of convolutional codes, which is usually applied to adaptive communication, information interception and cryptanalysis. The simulation experiments show the proposed methods can recognize the convolutional coding parameters effectively.

Key words: Blind recognition; Convolutional code; High bit error rate; Walsh-Hadamard ransform

1 引言

信道编码的盲识别在信息截获、信息对抗和智能通信等领域有重要应用，但公开发表文献并不多见。

目前，信道编码的盲识别技术研究主要涉及卷积码的盲识别，如：陆佩忠[1]等根据文献[2]提出的删除过程所等价的生成多项式变换模型，利用生成多项式矩阵和校验多项式矩阵之间的校验约束关系，提出了$n-1/n$码率删除卷积码的盲识别方法，但其并未对误码情况做出详细的分析。邹艳[3]等提出了基于快速合冲算法的$(2,1,m)$类卷积码盲识别算法，但其容错性能需要进一步研究。王丰华等[4]提出了基于欧几里德算法的$(2,1,m)$类卷积码盲识别算法，但由于卷积码是有记忆的，其算法要求所使用的数据必须是无记忆数据，且提出算法不能容错。

以上算法均未对误码问题进行深入的讨论，但是由于信息截获方所处的地理位置和接收方式的被动性，所得到的信号常常属于微弱信号，而具有信道编码设计的信息传输系统，靠编码增益克服信道干扰，因而常常降低发射功率，因此获取的数据必然存在误码。本文提出一种可以容错的卷积码盲识别算法，不仅将原有的识别种类进行了有效的扩展，而且可以在较高误码率的情况下取得良好效果，具有很好的实用价值。

2 问题描述

设C_p是一有误码的$(n,1,m)$卷积码序列，则卷积码的盲识别问题是：由C_p确定源码C的生成多项式。

2009-03-19 收到，2009-09-21 改回
国家自然科学基金(60773003)和陕西省自然科学基础研究计划项目(SJ08-ZT14)资助课题
通信作者：刘健 liujian_1101@163.com

关于卷积码的详细描述参阅文献[5]。现介绍一些基本概念，用来描述和解决本文的主要问题。

设 F 是二元域，$F[D]$ 为多项式环，$F(D)$ 是有理函数域。称 $F(D)^n$ 的任意一个一维子空间 C 是码率为 $1/n$ 卷积码。如果 $\boldsymbol{G}(D)$ 是 $F(D)$ 上的 $1\times n$ 矩阵且行向量构成了 C 的一组基，则称 $\boldsymbol{G}(D)$ 是 C 的一个生成矩阵。如果 $\boldsymbol{G}(D)$ 是多项式生成矩阵，且 $\boldsymbol{G}(0)$ 是满秩的，则称 $\boldsymbol{G}(D)$ 是编码矩阵。

对于一个 $1/n$ 的卷积码，在任一时刻有 1 bit $M=(m)$ 的信息输入，则相应有 n bit 的编码序列输出 $C=(c_0,c_1,\cdots,c_{n-1})$，称 M 是该时刻的信息字，C 是该时刻的码字。其编码器结构如图 1 所示。

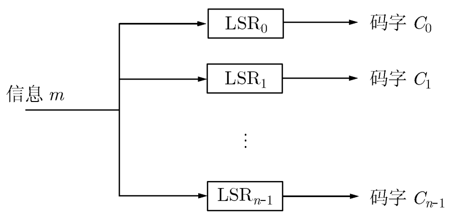

图 1　$(n,1,m)$ 卷积码编码结构图

3　卷积码的盲识别

为了方便理解，先讨论 $(2,1,m)$ 卷积码的盲识别方法，然后研究 $(n,1,m)$ 卷积码更为普遍的情况。

3.1 数学模型的建立

设 $m=(m_0,m_1,\cdots,m_{N-1})$ 是域 F 上的有限长度序列。根据卷积码的定义，其编码后的码序列 $C=(c_0,c_1,\cdots,c_{2N-1})$。将码的生成矩阵 $\boldsymbol{G}_\infty$ 写成 D 的函数形式：$\boldsymbol{G}(D)=[\boldsymbol{g}^{(1,1)}(D),\boldsymbol{g}^{(1,2)}(D)]$，则码字可以表示成：

$$\begin{aligned}\boldsymbol{C}(D)&=\boldsymbol{M}(D)\boldsymbol{G}(D)=\boldsymbol{M}(D)\left(\boldsymbol{g}^{(1,1)}(D),\boldsymbol{g}^{(1,2)}(D)\right)\\&=\left(\boldsymbol{M}(D)\boldsymbol{g}^{(1,1)}(D),\boldsymbol{M}(D)\boldsymbol{g}^{(1,2)}(D)\right)\end{aligned}\qquad(1)$$

根据卷积码生成矩阵与校验矩阵的关系：

$$\boldsymbol{G}(D)\cdot\boldsymbol{H}(D)^{\mathrm{T}}=0\qquad(2)$$

根据式(2)，将式(1)左右两边均乘以 $\boldsymbol{H}(D)^{\mathrm{T}}$ 得：

$$\boldsymbol{C}(D)\cdot\boldsymbol{H}(D)^{\mathrm{T}}=0\qquad(3)$$

因此，卷积码的盲识别问题可以等价为求解如下问题。

设 $\boldsymbol{c}_i(D)=c_{i0}+c_{i1}D+c_{i2}D^2+\cdots c_{iN}D^N, i=1,2$ 是域 F 上的 $(2,1,m)$ 卷积码码字序列的多项式表示，求集合 $\varPhi^{(2)}=\{(\boldsymbol{h}_1(D),\boldsymbol{h}_2(D),L)\in F[D]^2\times Z^+ \mid \exists d(D)\in F[D],\quad \boldsymbol{h}_1(D)+\boldsymbol{h}_2(D)\equiv \boldsymbol{d}(D) \bmod D^{N+1}, \deg \boldsymbol{d}(D)<m, \max(\deg \boldsymbol{h}_1(D),\deg \boldsymbol{h}_2(D)\le m)\}$ 中的元素对 $(\boldsymbol{h}_1(D),\boldsymbol{h}_2(D),m)$，使得 m 达到极小且 $(\boldsymbol{h}_1(0),\boldsymbol{h}_2(0))\ne(0,0)$。

设 $\boldsymbol{H}(D)=[\boldsymbol{h}^{(1,1)}(D),\boldsymbol{h}^{(1,2)}(D)]$，由式(2)得 $\boldsymbol{g}^{(1,1)}(D)\boldsymbol{h}^{(1,1)}(D)+\boldsymbol{g}^{(1,2)}(D)\boldsymbol{h}^{(1,2)}(D)=0$，所以 $\boldsymbol{g}^{(1,1)}(D)=\dfrac{\boldsymbol{g}^{(1,2)}(D)\boldsymbol{h}^{(1,2)}(D)}{\boldsymbol{h}^{(1,1)}(D)}$。

因为任一 $(n,1,m)$ 卷积码不产生第一类无限误差传播的条件为其编码矩阵 $\boldsymbol{G}(D)$ 有一个无反馈逆或有一个前反馈。无反馈逆的充分必要条件是：编码矩阵 $\boldsymbol{G}(D)$ 中的子多项式互素[6]。有一个前反馈的充分必要条件是

$$\mathrm{GCD}[\boldsymbol{g}^{(1,1)}(D),\boldsymbol{g}^{(1,2)}(D),\cdots\boldsymbol{g}^{(1,n)}(D)]=D^L\qquad(4)$$

式(4)中，$L\ge 0$，且存在有一个最小迟延为 L 的逆，其它任何迟延的逆都小于它[5]。

若待识别卷积码无反馈逆，则其生成矩阵 $\boldsymbol{g}^{(1,1)}(D)=\boldsymbol{h}^{(1,2)}(D)$，$\boldsymbol{g}^{(1,2)}(D)=\boldsymbol{h}^{(1,1)}(D)$。

若待识别卷积码有一个前反馈，则由式(4)得 $\mathrm{GCD}\left[\dfrac{\boldsymbol{g}^{(1,2)}(D)\boldsymbol{h}^{(1,2)}(D)}{\boldsymbol{h}^{(1,1)}(D)},\boldsymbol{g}^{(1,2)}(D)\right]=D^L$，其中 $L\ge 0$，且存在有一个最小迟延为 L 的逆，其它任何迟延的逆都小于它。因为 $\partial(\boldsymbol{g}^{(1,1)}(D))\le m$，$\partial(\boldsymbol{g}^{(1,2)}(D))\le m$，且 $\boldsymbol{h}_1(D)$ 和 $\boldsymbol{h}_2(D)$ 满足 $\max(\deg \boldsymbol{h}_1(D),\deg \boldsymbol{h}_2(D)\le m)$，则最小迟延为 $L=0$。综上所述得其生成矩阵 $\boldsymbol{g}^{(1,1)}(D)=\boldsymbol{h}^{(1,2)}(D)$，$\boldsymbol{g}^{(1,2)}(D)=\boldsymbol{h}^{(1,1)}(D)$。

当接收到的数据长度 $N>6k$ 时(其中 $k=m+1$ 为编码约束度)，卷积码的盲识别问题可以等价为求解如下的方程组：$\sum\limits_{j=0}^{n}\left(\sum\limits_{i=0}^{k-1}\boldsymbol{c}_{1,i+j}\boldsymbol{g}_{2,k-i-1}+\sum\limits_{i=0}^{k-1}\boldsymbol{c}_{2,i+j}\boldsymbol{g}_{1,k-i-1}\right)=0$，其中 $n\gg 2k$。

考虑实际接收数据为含错码序列，得 $\boldsymbol{r}_i(D)=\boldsymbol{c}_i(D)+\boldsymbol{e}_i(D)=(c_{i0}+c_{i1}D+c_{i2}D^2+\cdots c_{iN}D^N)+(e_{i0}+e_{i1}D+e_{i2}D^2+\cdots e_{iN}D^N)$，$i=1,2$。其中 $\boldsymbol{e}_i(D)=(e_{i0}+e_{i1}D+e_{i2}D^2+\cdots e_{iN}D^N)$，$i=1,2,$ 为误码多项式。

我们实际要解决的问题是，根据 $\boldsymbol{r}_i(D)$ 求解满足下列含错线性方程组中方程个数最多的一组解向量

$$\sum_{j=0}^{n}\left(\sum_{i=0}^{k-1}r_{1,i+j}g_{2,k\text{-}i\text{-}1}+\sum_{i=0}^{k-1}r_{2,i+j}g_{1,k-i-1}\right)=0\qquad(5)$$

3.2 基于 Walsh-Hadamard 变换求解方法

令 $\boldsymbol{x}=[g_{2,k-1},g_{1,k-1},\cdots,g_{2,0},g_{1,0}]^{\mathrm{T}}$

$$\boldsymbol{R}=\begin{bmatrix}r_{1,0}&r_{2,0}&\cdots&r_{1,k-1}&r_{2,k-1}\\r_{1,1}&r_{2,1}&\cdots&r_{1,k}&r_{2,k}\\\vdots&\vdots&\ddots&\vdots&\vdots\\r_{1,n}&r_{2,n}&\cdots&r_{1,k+n-1}&r_{2,k+n-1}\end{bmatrix}$$

则卷积码盲识别的数学模型进一步简化为求解方程

组 $\boldsymbol{R}\boldsymbol{x}=0$，其中 $\boldsymbol{R}$ 是 n 个 $2k$ 维行向量所组成的矩阵。$\boldsymbol{x}$ 是符合率最高的 $2k$ 维列向量。

以 3 维向量为例，首先构造一个 8×8 的方阵。

$$\boldsymbol{C}_{2^3}=\begin{bmatrix}00001111\\00110011\\01010101\end{bmatrix}^{\mathrm{T}}\times\begin{bmatrix}00001111\\00110011\\01010101\end{bmatrix}$$

$$=\begin{bmatrix}0&0&0&0&0&0&0&0\\0&1&0&1&0&1&0&1\\0&0&1&1&0&0&1&1\\0&1&1&0&0&1&1&0\\0&0&0&0&1&1&1&1\\0&1&0&1&1&0&1&0\\0&0&1&1&1&1&0&0\\0&1&1&0&1&0&0&1\end{bmatrix}$$

按照 $\boldsymbol{C}_{2^3}(i)=\begin{cases}1\ ,i=0\\-1,i=1\end{cases}$ 对矩阵 $\boldsymbol{C}_{2^3}$ 做变换，即为一个 3 阶 Hadamard 矩阵。可以发现二元域上 $\boldsymbol{x}\boldsymbol{R}=0$ 方程组的解与 $\boldsymbol{C}_{2^m}$ 矩阵有着密切的关系，$\boldsymbol{C}_{2^m}$ 中的每一组行(列)向量包括了这 3 维解向量中的任意两组积的所有形式。

以矩阵 $\boldsymbol{R}$ 中的行向量 $(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n)$ 为地址的单元进行累加，记作 $f(a_1,a_2,\cdots,a_n)$。然后对 $f(a_1,a_2,\cdots,a_n)$ 做 Walsh-Hadamard 变换。其变换后的向量中最大项的地址就为此含错方程的解，即与矩阵 $\boldsymbol{R}$ 中行向量正交最多的那组向量。蝶形运算可以实现快 Walsh-Hadamard 变换。具体内容可以参见文献[7]。

3.3 $(n,1,m)$ 卷积码的盲识别

由图 1 可知，$(n,1,m)$ 卷积码的实质为将输入码序列经过 n 个 LSR 得到 n 个输出。故可以将 $(n,1,m)$ 卷积码等价为若干个 $(2,1,m)$ 卷积码的叠加。

以码率为 $1/n$ 的码率为例，可以将截获数据分成 n 路，按顺序选取其中两路按照 $(2,1,m)$ 卷积码的识别方法进行识别，通过 $n-1$ 次运算即可以得出 $n-1$ 组参数。运行第 $t-1$ 次运算，可以得出 $\boldsymbol{g}^{(1,t-1)}(D)$ 和 $\boldsymbol{g}^{(1,t)}(D)$。运行第 t 次运算，可以得出 $\boldsymbol{g}^{(1,t)}(D)'$ 和 $\boldsymbol{g}^{(1,t+1)}(D)'$。如果 $\boldsymbol{g}^{(1,t)}(D)=\boldsymbol{g}^{(1,t)}(D)'$，则将运算进行直到第 $n-1$ 运算结束为止。如果 $\boldsymbol{g}^{(1,t)}(D)=\boldsymbol{X}\ \boldsymbol{g}^{(1,t)}(D)'$，其中 $\boldsymbol{X}$ 为 D 的函数，则将后面运算结果均乘以 $\boldsymbol{X}$ 即可。反之将前面的运算结果均乘以 $\boldsymbol{X}$。最终需保证 $\mathrm{GCD}[\boldsymbol{g}^{(1,1)}(D),\boldsymbol{g}^{(1,2)}(D),\cdots,\boldsymbol{g}^{(1,n)}(D)]=D^L$，到此识别完毕。

若 n 的数值未知，可以遍历进行上述运算，当第 n 次运算后得 $\boldsymbol{g}^{(1,n+1)}(D)=\boldsymbol{g}^{(1,1)}(D)$，识别结束。

3.4 求解向量置信度分析

当采用基于 Walsh-Hadamard 变换求解方法时，由于接收卷积码序列有误码，有必要从概率角度讨论解向量的置信度问题。

求校验矩阵时，设某解向量代入方程组成立方程个数为 m_1，不成立方程个数为 m_2，则 $m_1+m_2=m$，$m_1-m_2=f(a_1,a_2,\cdots,a_n)$。则符合率 FHL $=1/2+f(a_1,a_2\cdots,a_n)/2m$，其中 m 为方程个数。

假设 $\boldsymbol{c}=(c_1,c_2,\cdots,c_n)$ 是 n 元含错方程组的解向量，方程成立的概率为 p。当 $\boldsymbol{c}$ 满足第 i 个方程时，令 $\xi_i=1$，当 $\boldsymbol{c}$ 不满足第 i 个方程时，令 $\xi_i=-1$。则 $E\left(\sum_{i=1}^{m}\xi_i\right)=m(p-q)$，$D\left(\sum_{i=1}^{m}\xi_i\right)=4mpq$。其中 m 为方程个数。当 m 足够大时，由中心极限定理有：$\sum\xi_i-m(p-q)/\sqrt{4mpq}\propto N(0,1)$。

令 $z=m_1-m_2$，计算统计量：

$$T=z-m(p-q)/\sqrt{4mpq}\tag{11}$$

如果显著性水平为 α，则

$$\alpha/2=1-F(t)\tag{12}$$

其中 $F(t)$ 是 t 的概率分布函数。由式(12)可以给出一个标准 t。在解方程过程中应保证 $T\ge t$。

取 $p=q=0.5$，则 $T=z/\sqrt{m}$。可以根据此式来判别解向量的置信度。当 $t\ge 3$ 时，错误概率为 0.00135，在数学上一般将 $t\ge 3$ 称为不可能事件。此时将门限值 t 设为 3。

3.5 求解实例分析

下面以 $(2,1,m)$ 卷积码盲识别的计算实例说明上述结果的正确性。

例 1 在误码率为 5×10^{-2} 情况下截获到一段码序列如下所示(由于篇幅原因只给出了数据的一部分)：

01110000110111100110100001000110010111001111

0100001101110011101100000

按照文中方法对以上数据做 12 阶的 Walsh-Hadamard 变换，其结果如图 2 所示。其中共有 7 组解向量的 T 高于 10。此时可以判定此 7 组解向量均为所构造方程组的解。解向量不唯一是由于构造方程时将编码约束度估计过大所造成的。此时仅需将任意一组解向量化简到满足式(4)的要求即可。最终可以识别出此卷积码的编码矩阵为：$\boldsymbol{G}(D)=[1+D+D^2+D^3,1+D+D^3]$。

4 仿真实验与结果分析

由于 $(n,1,m)$ 卷积码的识别基础是对 $(2,1,m)$ 卷积码进行识别，故仅对 $(2,1,m)$ 卷积码进行了仿真实

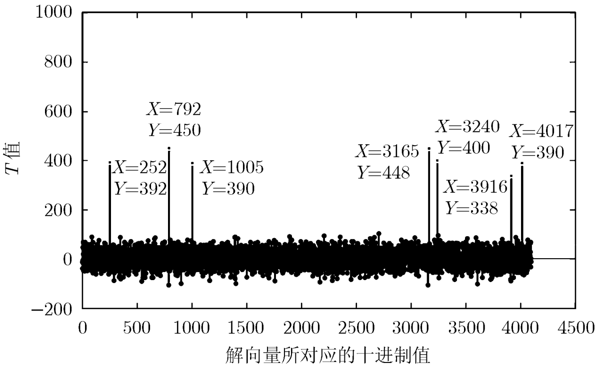

图 2 卷积码盲识别实例图

验。针对不同误码率和不同的编码约束度，根据 3.4 节给出的判决门限，通过蒙特卡罗仿真实验统计了识别概率。

4.1 数据来源

针对不同编码存贮值，随机选取其它编码参数，在不同误码率下，用 Matlab 各生成 1000 组仿真数据。码长与误码率的选择参见表 1。

表 1 仿真数据参数选择表

编码存贮(m)	误码率(P_e)
$m=2$	2×10^{-1}, 1.9×10^{-1}, 1.8×10^{-1}, 1.7×10^{-1}, 1.6×10^{-1}, 1.5×10^{-1}, 1.4×10^{-1}, 1.3×10^{-1}
$m=3$	1.5×10^{-1}, 1.4×10^{-1}, 1.3×10^{-1}, 1.2×10^{-1}, 1.1×10^{-1}, 1.0×10^{-1}, 0.9×10^{-1}, 0.5×10^{-1}
$m=4$	1.4×10^{-1}, 1.3×10^{-1}, 1.2×10^{-1}, 1.1×10^{-1}, 1.0×10^{-1}, 0.9×10^{-1}, 0.5×10^{-1}
$m=5$	1.1×10^{-1}, 1.0×10^{-1}, 0.9×10^{-1}, 0.8×10^{-1}, 0.7×10^{-1}, 0.6×10^{-1}, 0.5×10^{-1}
$m=6$	1.0×10^{-1}, 0.9×10^{-1}, 0.8×10^{-1}, 0.7×10^{-1}, 0.6×10^{-1}, 0.5×10^{-1}
$m=7$	1.0×10^{-1}, 0.9×10^{-1}, 0.8×10^{-1}, 0.7×10^{-1}, 0.6×10^{-1}, 0.5×10^{-1}
$m=8$	1.0×10^{-1}, 0.9×10^{-1}, 0.8×10^{-1}, 0.7×10^{-1}, 0.6×10^{-1}, 0.5×10^{-1}
$m=9$	1.0×10^{-1}, 0.9×10^{-1}, 0.8×10^{-1}, 0.7×10^{-1}, 0.6×10^{-1}, 0.5×10^{-1}, 0.4×10^{-1}
$m=10$	1.0×10^{-1}, 0.9×10^{-1}, 0.8×10^{-1}, 0.7×10^{-1}, 0.6×10^{-1}, 0.5×10^{-1}, 0.4×10^{-1}
$m=11$	1.0×10^{-1}, 0.9×10^{-1}, 0.8×10^{-1}, 0.7×10^{-1}, 0.6×10^{-1}, 0.5×10^{-1}, 0.4×10^{-1}
$m=12$	1.0×10^{-1}, 0.9×10^{-1}, 0.8×10^{-1}, 0.7×10^{-1}, 0.6×10^{-1}, 0.5×10^{-1}, 0.4×10^{-1}
$m=13$	1.0×10^{-1}, 0.9×10^{-1}, 0.8×10^{-1}, 0.7×10^{-1}, 0.6×10^{-1}, 0.5×10^{-1}, 0.4×10^{-1}, 0.3×10^{-1}

4.2 结果分析

图 3 为卷积码的识别概率与误码率的曲线图(由于常用 $(2,1,m)$ 卷积码的编码存贮值一般小于 7，故只对编码存贮值小于 7 的卷积码进行了蒙特卡罗仿真实验)。当误码率 $P_e=1.8\times10^{-1}$ 时，$m=2$ 的卷积码的识别概率超过了 80%。当误码率 $P_e=0.8\times10^{-1}$ 时，$m=6$ 的卷积码的识别概率也超过了 85%。随着 m 的增加，生成矩阵向量 $\boldsymbol{x}$ 中的未知数的个数会线性增加，由于容错矩阵分解法的实质是求解出满足方程个数最多的解向量，所以，随着误码率和编码存贮的增加，识别概率将降低。

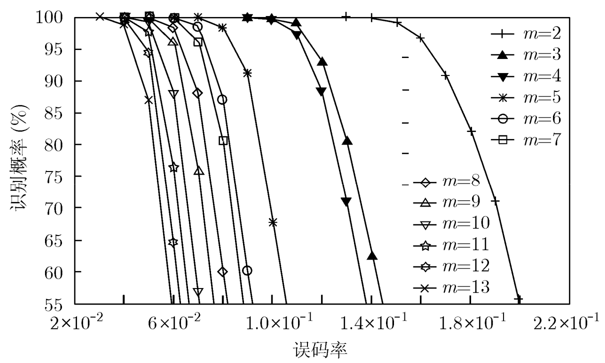

图 3 卷积码识别概率曲线图

5 结束语

本文建立了 $(n,1,m)$ 卷积码盲识别的数学模型，在高误码率的情况下，通过 WHT 最终解决了卷积码的盲识别问题。实验表明该算法能够有效的解决卷积码盲识别问题，本识别算法已经成功的应用在信息截获领域。

参 考 文 献

[1] Lu Pei-zhong, Shen Li, Zou Yan, and Luo Xiang-yang. Blind recognition of punctured convolutional codes[J]. *Science in China Ser. F Information Sciences*, 2005, 48(4): 484–498.

[2] Begin G and Haccoun D. High-rate punctured convolutional codes: Structure properties and construction techniques [J]. *IEEE Transactions on Communicaitons*, 1989, 37(11): 1381–1385.

[3] 邹艳，陆佩忠. 关键方程的新推广[J]. 计算机学报，2006, 29(5): 712–718.

Zou Yan and Lu Pei-zhong. A new generalization of key equation[J]. *Chinese Journal of Computers*, 2006, 29(5): 712–718.

[4] Wang Feng-hua, Huang Zhi-tao, and Zhou Yi-yu. A method for blind recognition of convolution code based euclidean algorithm[C].// IEEE International Conference on Wireless Communications. Shanghai: IEEE Press, 2007: 1414–1417.

[5] 王新梅，肖国镇. 纠错码—原理与方法[M]. 西安：西安电子科技大学出版社, 1991: 378-415.
Wang Xin-mei and Xiao Guo-zhen. Theory and Method of Error-Correcting Codes[M]. Xi'an: Xidian University Press, 1991: 378-415.

[6] 刘玉君. 信道编码(修订版)[M]. 郑州：河南科学技术出版社，2001: 190-256.
Liu Yu-jun. Channel Coding[M]. Zhengzhou: Henan Science Press, 2001: 190-256.

[7] 邹艳，陆佩忠，朱雪岭. 软判决快速相关攻击新算法与应用[J]. 计算机研究与发展，2007，44(4)：581-588.
Zou Yan, Lu Pei-zhong and Zhu Xue-line. A novel algorithm of soft fast correlation attack and applications [J]. *Journal of Computer Research and Developrent*, 2007, 44(4): 581-588.

刘 健： 男，1983 年生，博士生，研究方向为通信侦察与通信对抗.
王晓君： 男，1973 年生，副教授，研究方向为电子对抗技术.
周希元： 男，1944 年生，研究员，博士生导师，研究方向为信息对抗与电子战.