第 33 卷 第 6 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.6 Computer Engineering March 2007
·安全技术· 文章编号：1000—3428(2007)06—0118—02 文献标识码：A 中图分类号：TN918

基于 m 序列的信道编码信息隐藏算法

王伟祥，刘玉君，李文雄
（信息工程大学信息工程学院，郑州 450002）

摘 要：信道编码信息隐藏技术是一门新兴的信息隐藏技术。该文提出了一种基于 m 序列的信道编码信息隐藏算法。该算法采用 m 序列对秘密信息进行伪随机加扰，并利用 m 序列来选取秘密信息在码字载体中的嵌入位置。实验结果表明该隐藏算法具有较好的不可检测性和较高的安全性。

关键词：m 序列；信道编码；信息隐藏；嵌入算法

Information Hiding Algorithm in Channel Coding Based on m-Sequence

WANG Weixiang, LIU Yujun, LI Wenxiong
(Institute of Information Engineering, Information Engineering University, Zhengzhou 450002)

【Abstract】 Information hiding based on channel coding is a new field of information hiding technology. This paper presents an information hiding algorithm in channel coding based on m-sequence. It adds an m-sequence to the secret data, and selects the position of secret data in code carrier with m-sequence. The experiment results show that this algorithm has better imperceptibility and robustness.

【Key words】 m-Sequence; Channel coding; Information hiding; Embedded algorithm

信息隐藏技术具有很强的信息保密性和信息安全性。现阶段人们一般选择图像、文本、音频和视频等数字媒体数据作为载体[1,2]，而利用以上载体隐藏数据时，改变了原始数据某些比特的数值。本文研究的基于m序列的信道编码信息隐藏技术是一种新颖的信息隐藏技术，以原始信息数据的信道编码码字作为嵌入载体，利用m序列对秘密信息进行伪随机加扰并且确定其嵌入位置，提取译码后不会影响原始信息数据的结构和统计特性，因此具有较高的安全性和不可检测性。

1 信道编码信息隐藏技术

信道编码是一门提高数据传输可靠性的技术[3]。信道编码信息隐藏技术利用信道有噪声这种现象，在信道编码的纠错能力范围之内将秘密信息作为人为噪声嵌入其中[4]。使用信道编码码字作为嵌入载体有效地克服了数字媒体作为载体所带来的问题。

一方面在信道编码中嵌入秘密信息不会影响到原始信息数据的结构和统计特性，当然更不会使译码后的数据在视觉或听觉上产生变化，这是因为只要保证嵌入的秘密信息（人为噪声）与信道噪声的总体效应不超过信道编码的纠错范围，就能保证原始信息在信道译码后得到正确的复原。另一方面，信道编码技术在现代通信中应用越来越广泛，无论是卫星通信还是短波通信，都广泛地应用着信道编码技术，这就使得以信道编码为载体进行信息隐藏具有可行性。

2 m 序列基本原理

m序列是最大长度线性反馈移位寄存器序列的简称[3]，它具有近似随机序列的性质，又能按一定规律产生和复制，所以称其是伪随机序列。截获者若要获取信息就必须准确知道所用m序列的长度、种类和初始状态，但不同长度的m序列有无数种，同一长度的m序列当级数较大时也有许多种，因此m序列在信息安全上被广泛应用。

图 1 是一个 n 级移存器电路，各级寄存器抽头从左到右依次为 $c_1,\ldots,c_{n-1},c_n$，即乘法器 $c_i=0$ 或 $c_i=1$，但 $c_n=1$，否则就退化成 n-1 级移位寄存器。当给定 n 级线性移存器的生成多项式为本原多项式，寄存器的初始状态为非全零时，我们可以产生 1 到 2^n-1 之间的伪随机数序列，即 m 序列。

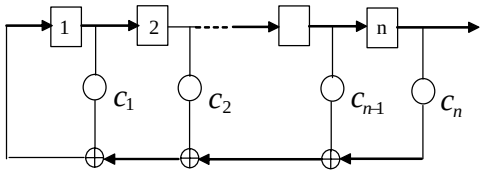

图 1 n 级线性移存器

m 序列具有类似白噪声的性质，但它又是周期的、有规律的，可以人为产生和复制。因为其具有类似白噪声的性质，相关函数具有尖锐特性，所以易于从其它信号或干扰中分离出来，具有良好的抗干扰特性。

3 隐藏算法及实现方案

基于 m 序列的信道编码信息隐藏算法如下：

(1)发送方

1)首先利用密钥K_1产生m序列：

$S_1=(s_1,s_2,s_3\ldots)$，$s_i \le 2^n-1$，$i=1,2,\ldots$，

将秘密信息同这个 m 序列进行模二加（伪随机加扰），然后进行纠错编码。选用的纠错码类型要根据可靠性需求和信道容量来定，选用纠错能力较强的纠错码时，秘密信息的

基金项目：军队部批项目
作者简介：王伟祥(1980－)，男，硕士生，主研方向：信道编码，信号与信息处理，信息隐藏技术；刘玉君，教授；李文雄，硕士生
收稿日期：2006-03-30 **E-mail：**wangweixiang2008@163.com

可靠性相对较高，但隐藏量相对较小；反之选用纠错能力较弱的纠错码时，秘密信息的可靠性相对较低，但隐藏量相对较大。本文采用的是纠单个错的（15,11）汉明码。将经过纠错编码后的秘密信息码字序列记为

$$m = (m_1, m_2, \ldots, m_M)$$

2)根据信道特性和秘密信息的数据量来确定信源数据的信道编码类型。此处的编码方式应选用纠错能力较强的码子，本文采用的是（127,71）可纠正 9 个错误的 BCH 码。将经过纠错编码后的信源数据序列每 2^n-1比特分为一组，记为

$$c = (c_1, c_2, \ldots, c_N)$$

其中c_i为长度为 2^n-1的一组数据。

3)利用密钥K_2产生另一m序列：$S_2 = (s_1, s_2, s_3 \ldots)$，$s_i \le 2^n - 1$，$i = 1, 2, \ldots$，利用此m序列选取秘密信息的嵌入位置，随机数$s_i$表示在码字载体的第$i$组数据的第$s_i$比特嵌入秘密信息。嵌入方式采用替换法，即用秘密信息数据的第i比特替换第i组码字载体数据的第s_i比特。最后将携带秘密信息的码字载体送入信道进行传输。

(2)接收方

1)利用密钥K_2生成m序列：$S_2 = (s_1, s_2, s_3 \ldots)$，$s_i \le 2^n - 1$，$i = 1, 2, \ldots$，按照m序列和提取算法在未经过信道译码的接收数据中提取数据，得到的数据为含有信道噪声的秘密信息码字序列：$m' = (m'_1, m'_2, \ldots, m'_M)$。

2)对含有信道噪声的秘密信息码字序列：$m' = (m'_1, m'_2, \ldots, m'_M)$进行纠错译码。若信道噪声在纠错码的纠错范围内，就可以无错地恢复秘密信息码字序列：$m = (m_1, m_2, \ldots, m_M)$。

3)利用密钥K_1产生m序列：$S_1 = (s_1, s_2, s_3 \ldots)$，$s_i \le 2^n - 1$，$i = 1, 2, \ldots$，将秘密信息码字序列译码后的数据与此m序列模二加（伪随机去扰），即可得到秘密信息。

基于 m 序列的信道编码信息隐藏算法具有较高的安全性。因为对于截获方一般是直接对接收数据进行信道译码，判断译码后得数据是否可疑。而当信道噪声与嵌入信息量的和未超过纠错码的纠错能力时，则可以无错地恢复出信源数据。译码得到的数据同发送方的信源数据完全一致，所以不会怀疑接收的数据中含有秘密信息。信道编码信息隐藏实现方案如图 2 所示。

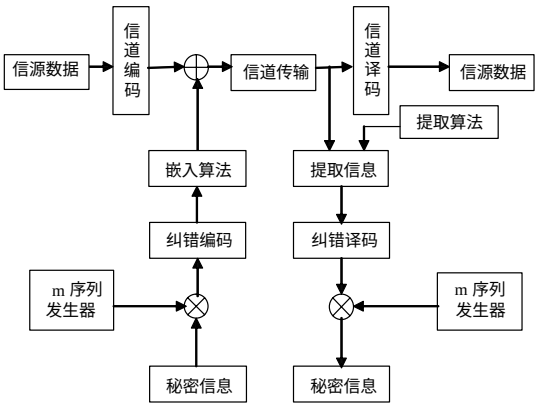

图 2 信道编码信息隐藏实现方案

在嵌入算法中两次用到 m 序列：一次是将秘密信息与 m 序列进行模二加；另一次是用 m 序列来选取秘密信息码字序列在码字载体的嵌入位置。秘密信息与 m 序列进行模二加，这样就将秘密信息变成了不可理解的密文，攻击者即使提取后也不能理解其内容。在接收端则必须加上同样的 m 序列才能恢复出秘密信息。这是因为将 m 序列模二加了两次，就等于未加入。攻击者要获得秘密信息是非常困难的，因为不同长度的 m 序列有无穷多个，同一长度的 m 序列也有很多个。此外，同一 m 序列的初值不同，也不能用于提取秘密信息，这里的初值就是提取秘密信息所需的密钥。

4 实验结果

实验在二进制对称信道条件下进行，调制方式为 BPSK。载体信源选用大小为 257KB 的 bmp 图像，秘密数据选用大小为 0.5KB~10KB 的文本文档。

实验结果表明，信息嵌入率取为 1%的情况下，当信道误码率低于 10^{-3}时，译码后的载体信源和秘密信息都可以正确恢复；当信道误码率达到 5.0×10^{-3}时，译码后的载体信源出现少量比特错误，但秘密信息可以完全正确恢复；当信道误码率达到 10^{-2}时，秘密信息和载体信源都将出现错误。当改变嵌入量时，错误率将随着嵌入量的增加而增加。见图 3、图 4。实验数据如表 1 所示。

图 3 嵌入量合适信源数据恢复情况

图 4 嵌入量过大信源数据恢复情况

表 1 基于 m 序列的信道编码信息隐藏实验结果

A \ B	10^{-2}	5×10^{-3}	10^{-3}	5×10^{-4}	10^{-4}
嵌入信息后的 Pe	**0.011 357**	**0.006 316**	**0.002 286**	**0.001 763**	**0.001 328**
提取秘密信息的 Pe	**0.000 604**	**0**	**0**	**0**	**0**
恢复载体信源的 Pe	**0.001 546**	**0.000 365**	**0**	**0**	**0**

由实验可知：

(1)接收的码字载体的错误来源于两方面：一是秘密信息嵌入造成的码字载体改变；二是信道噪声造成的码字载体的改变。当秘密信息嵌入和信道噪声造成的总体误码效应不超过码字的纠错能力时，截获者可以无错地恢复出信源数据。信源数据的结构和统计特性没有发生改变，这样就不致引起截获者的怀疑，因此该算法具有较高的安全性；

(2)在没有获得密钥的情况下，从检测错误位置入手来提取 m 序列，进而获得秘密信息是不可行的。因为信道噪声同样造成了码字载体的改变。由于噪声干扰的存在，使得接收的纠错码中存在随机错误，而随机错误的出现及类型具有一定的复杂性和随机性，对信道错误不易得到较完备的统计模型，因此对统计检测具有一定的抗攻击性；

(3)采用 m 序列对秘密信息进行伪随机加扰使得秘密信息在统计特性上接近随机噪声，一定程度上提高了秘密信息的安全性。

(4)为进一步提高隐藏算法的安全性和不可检测性，首先应保证秘密信息嵌入和信道噪声所造成的总体误码效应不超过载体码字的纠错能力；其次隐藏量要小，即秘密信息嵌入造成的误码效应小于或远小于信道噪声造成的误码效应。

(下转第 122 页)