doi:10.3969/j.issn.1000-436x.2013.12.014

基于二级定位的编码信道信息隐藏算法

陈立全，卢苗，胡爱群，孙晓燕
(东南大学 信息安全研究中心，江苏 南京 210096)

摘 要：分析了以编码信道为载体的信息隐藏算法及容量，指出现有算法存在的问题，提出了一种结合容量上限判断的基于二级定位的信息隐藏算法。所提算法在秘密信息嵌入前首先计算系统隐藏容量上限，并判断是否超出；接着在嵌入位置选择过程中引入二级定位以及循环移位机制。仿真结果表明，相比已有算法，所提算法能较好地避免因隐藏容量过大而导致秘密通道暴露的风险；同时通过二级定位及循环移位机制提高嵌入位置的随机性，避免秘密信息相互覆盖，提升信息隐藏性能。

关键词：信息隐藏；编码信道；二级嵌入；循环移位
中图分类号：TN911.22 **文献标识码：**B **文章编号：**1000-436X(2013)12-0120-11

Improved information hiding algorithm based on twice positioning in coding channel

CHEN Li-quan, LU Miao, HU Ai-qun, SUN Xiao-yan
(Research Center of Information Security, Southeast Un versity, Nanjing 210096, China)

Abstract: Based on analysis of existing information hiding algorithms and capacities in coding channel, the defects of those existing algorithms were pointed out, and an improved information hiding algorithm with capacity upper limit analysis and based on twice positioning was proposed. the proposed algorithm, the information hiding capacity upper limit is firstly computed before embedding, and used for comparison with the size of hiding secret data. Then, twice positioning scheme and cyclic shift mechanism for choosing the embedding position were used in the proposed algorithm. Simulation results show that, compared with those existing algorithms, the proposed algorithm is able to avoid the risk of exposure of the secret channel caused by capacity exceeding of hiding data. It can not only improve the randomness of the embedding position, but also avoid the risk of overlap among different secret data. The hiding performances of the coding channel information hiding system are improved.

Key words: information hiding; coding channel; twice positioning; cyclic shift

1 引言

目前，信息隐藏研究较多集中在文本、图像、音频和视频等载体上进行[1]。而针对传输信道，特别是编码传输信道上的信息隐藏关键问题研究得还较少。此处的编码传输信道是指利用信道编码技术实现可靠传输的信道，用到的信道编码技术包括 RS 编码、BCH 编码、卷积编码以及 LDPC 编码等[2~8]。目前与信道编码相关的信息隐藏技术研究主要有 2 个方面：1) 将 RS、BCH 等纠错编码技术用到嵌入前的秘密信息处理或载体信息处理上，以提高隐藏和提取性能；2) 利用编码信道中冗余空间进行信息隐藏的技术。

已有研究表明，在普通信道上传输数据时，信

收稿日期：2013-06-09；修回日期：2013-10-22
基金项目：国家高技术研究发展计划(“863”计划)基金资助项目(2013AA014001)；国家自然科学基金资助项目(61372103)；2011 发改委信息安全专项基金资助项目
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2013AA014001); The National Natural Science Foundation of China (61372103); 2011 National Development and Reform Commission (NDRC) Information Security Special Project

道中的干扰会使接收信息出现一些随机性错误，而纠错编码技术可以改善这种错误的发生，并提供了一定的编码纠错空间。这一现象正好为信息隐藏在编码信道上的实现提供了基础。原则上只要保证秘密信息隐藏造成的置换错码以及信道干扰造成的误码总和小于信道编码的纠错能力，则可将秘密信息作为噪声隐藏到信道编码数据流中，这不仅不会使译码后秘密数据在视听觉上产生变化，更不会改变原始载体的统计特性[5]。

文献[2]分析了将 m 序列应用到信道编码信息隐藏系统中，其主要的方法就是用随机 m 序列对秘密信息本身以及嵌入位置选择上进行扰乱处理。文献[3]提出了一种基于纠错编码的信息隐藏算法，其对隐秘信息纠错编码之后，嵌入整数小波变换后的系数中，以提高隐藏性能。文献[5]扩展分析了 RS 编码、BCH 编码、卷积编码等在信息隐藏上的应用。而基于 LDPC 编码信道的信息隐藏方案也在文献[7]中被提出来。综合了上述文献，笔者还发现随着信道编码纠错能力的增强，秘密信息的不可检测性和安全性也随之提高，则该系统的隐藏容量随之会增加。

信息隐藏系统容量分析一直是信息安全学术研究的难题。Moulin P 曾提出信息隐藏容量的理论分析方法，但这方法不能适用所有的信息隐藏环境中[1]。文献[9]在 Moulin P 分析方法的基础上进行了改进，但是其仍未分析纠错编码信道上的信息隐藏容量问题。在 2008 年，Yan X 等对信道编码传输过程中的信息隐藏容量进行分析[4]，而后来 Chen L 等也拓展了在 Alamouti 空间编码信道中的信息隐藏容量分析[10]。

由于各信息隐藏系统均有容量上限，所以，在建立一个实用的信息隐藏系统之前，需要先进行信息容量的判定。文献[4]虽然提出需要在编码信道信息隐藏之前进行容量分析，但其未提出具体的结合实施方案。另外，在文献[3,5~7]中，容量分析的步骤未涉及，而且也未考虑嵌入秘密信息过大时的秘密信息相互覆盖的安全隐患。

因此，针对现有算法存在的缺陷，本文提出了一种基于二级定位的编码信道信息隐藏改进算法。改进算法在秘密信息嵌入前充分考虑系统隐藏容量的上限，并且在嵌入位置选择过程中引入二级定位以及循环移位机制，既可以避免信息隐藏出错，又可提高嵌入位置选择的随机性，并避免秘密信息相互覆盖的风险。

2　编码信道信息隐藏算法分析

2.1　以编码信道为载体的信息隐藏算法

现有的以编码信道为载体的信息隐藏算法思想大致可以归纳如下[3~6]。

1) 发送端

对秘密信息进行置乱、加密以及纠错编码等预处理，以提高其安全性及顽健性。

对信源载体进行信道编码，并根据编码规则将编码后的信源数据进行分组。采用的信道编码可以描述为 (n,k,t)，k 为编码器输入信息长度，n 为编码输出长度。根据信道编码参数，通常会将编码后的数据按每 n bit 分为一组。

双方约定密钥 K，由 K 产生伪随机序列 $S=(s_1,s_2,s_3,\text{L}),\ \ s_i<n, i=1,2,\text{L}$，根据该序列确定秘密信息的嵌入位置。随机数 s_i 表示将秘密信息的第 i 位嵌入到载体信息的第 i 组中的第 s_i 位置，也即用秘密信息替换 s_i 位置的信源信息。按照这样的方法进行重复，直至秘密信息全部嵌入到信道编码中。

2) 接收端

利用相同密钥 K 产生伪随机序列 $S=(s_1,s_2,s_3,\text{L}),\ s_i<n, i=1,2,\text{L}$，并利用此序列和提取算法在信道译码前的接收数据中提取秘密信息，即随机数 s_i 表示提取载体数据中第 i 组的第 s_i 比特信息。

对提取出来的秘密信息进行纠错译码、解密以及反置乱等逆操作，得到隐藏信息。

对接收到的数据码流进行信道译码得到信源数据，实现正常通信。

2.2　现有算法分析

上述的这些以信道编码为载体的信息隐藏算法[3~6]存在 2 个方面的缺陷。

在信息隐藏前未考虑系统隐藏的容量。根据基于信道编码的信息隐藏原理可知，要保证隐藏系统的可行性，必须要求秘密信息修改和信道噪声的总体效应不能超过信道编码的纠错能力。给定隐藏载体和传输信道，若秘密信息超出了隐藏系统的承受范围，则信道译码后的信宿信息误码较大，影响正常通信，这反而会引起第三方的注意，从而暴露信息隐藏通道。文献[4]虽然曾说到需要在信息隐藏之前进行隐藏容量的判断，但是其主要分析了编码信道的容量，具体容量判断步骤与后续信息隐藏技术怎样结合及其效果没有做

分析和研究。

嵌入位置的选择不够合理。已有算法一般根据编码输出长度将编码数据流分组，然后按照秘密信息长度生成伪随机序列，将隐藏信息的每比特按照伪随机序列值嵌入到指定各码组的相应位置。这种方法存在以下不足之处：按照已有算法的思路，尽量要求隐藏信息长度小于编码分组数，这就大大限制了信道信息隐藏的能力，并降低了算法的灵活性；另外，一旦秘密信息长度大于分组数，则会出现嵌入位置不足的现象。此时，如果要继续执行嵌入算法，那么需要生成第二个伪随机序列，一方面增加了存储开销，另一方面也可能产生秘密信息相互覆盖的后果。具体的秘密信息相互覆盖过程如图 1 所示。

假设 M 为秘密信息长度，n 为信道编码输出长度，N 为编码数据流的分组数，$S=\{s_1, s_2, \text{L}\}$ 为伪随机序列。从图 1 (a)中可以看出，当 $M \le N$ 时，即秘密信息长度小于编码数据流的分组数，则伪随机序列的长度为秘密信息长度。秘密信息的嵌入过程是指根据伪随机序列值，将第 i 比特秘密信息嵌入到第 i 个分组的第 s_i 比特，其中，$i \le M$ ，$s_i \le n$。但是，当 $M > N$ 时，信息覆盖问题就出现了。如图 1(b)所示，若秘密信息长度大于编码数据流的分组数，则要将秘密信息进行分组，每组长度为 N ，分组数为 $L=\lceil M/N \rceil$。当第 L 组秘密信息进行嵌入时，由于 s_{L1} 与 s_{11}、s_{L2} 与 s_{12}、s_{LN} 与 s_{2N} 相同，表明第 L 组的第 1、2 及 N 位信息分别覆盖了第 1 组的第 1 比特、第 2 比特秘密信息以及第 2 组的第 N 比特秘密信息。图 1(b)只是假设一组秘密信息出现覆盖问题，而事实上，随着秘密信息的增加，伪随机序列个数增加，则排列中对应位置重合的概率变大，秘密信息覆盖的风险也随之变大。

3 基于二级定位的编码信道信息隐藏算法

为改进上述的 2 个问题，笔者提出的改进算法包括了信息容量分析部分和嵌入时的二级定位及循环移位机制部分。

3.1 信息隐藏容量分析

为防止秘密信息大小超过信息隐藏系统容量而破坏系统的不可检测性，改进算法引入信息隐藏容量分析模块。考虑到信道编码的纠错能力，在进行信息隐藏之前，必须保证隐藏信息替换量与信道干扰引起的总体误码在信道编码的纠错范围之内，只有这样，接收端才可以无失真地接收信源信息，

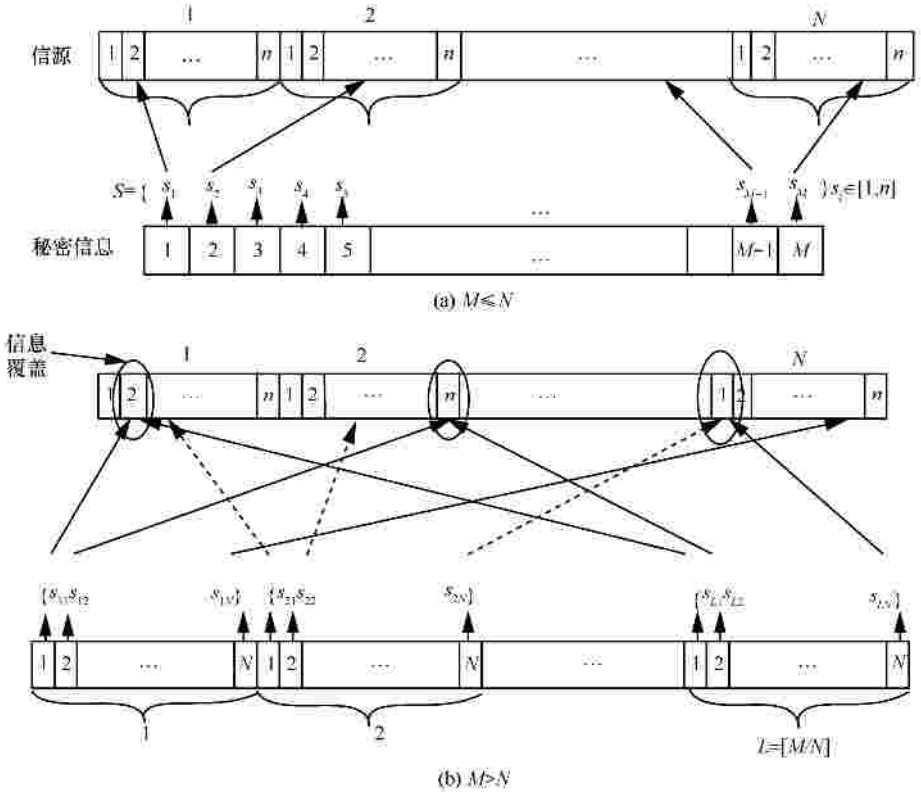

图 1 秘密信息覆盖过程

同时也能无误地提取隐秘信息。

以编码信道为载体的信息隐藏容量分析基础是[4,8]：秘密信息大小+伪装载体信道误码-秘密信息信道误码≤信道编码纠错能力。

下面以一个信道编码分组为例来说明编码信道的信息隐藏容量分析过程。

如图 2 所示，假设信道编码参数为 (n,k,t)，信道干扰造成的误比特率为 p_b。另外，(m_1,m_2,L,m_M) 表示秘密信息，k 表示编码输入长度，n 表示编码输出长度，t 为单个信道编码分组中的纠错数目。将秘密信息分别嵌入到信道编码分组的相应位置，且最坏的情况是，秘密信息与相应位置上的信源信息正好相反，也就是说，秘密信息对于编码数据流而言都是干扰，则由秘密信息造成的误比特数量为 M。嵌入秘密信息后的伪装数据流经过信道传输，因信道噪声等干扰会造成一定的误码。如图 2 所示，长度为 n 的待传输数据流中已经包含秘密信息序列，因此不可重复计算由秘密信息带来的误码，即经过信道传输后，由信道干扰造成的误比特数为 $(n-M)p_b$。综上所述，秘密信息与信道干扰的总体误码为 $M+(n-M)p_b$。

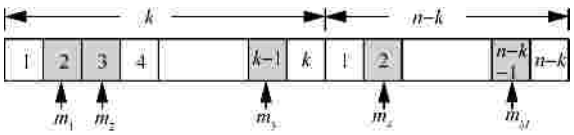

图 2　编码信道中信息隐藏容量分析示意

假设信息隐藏系统的参数设置如下：

C_0：信源数据码流长度；

C：信道编码后的信源数据长度；

$m_0=(m_{01},m_{02},\text{L},m_{0M_0})$：秘密信息码流；

$m=(m_1,m_2,\text{L},m_M)$：预处理后的秘密信息；

$E(C,m,K)$：秘密信息嵌入算法；

$D(C',K)$：秘密信息提取算法；

其中，M_0 为秘密信息长度，M 为预处理后的秘密信息长度；K 为双方事先约定的密钥，用于生成伪随机序列来确定秘密信息的嵌入位置；P_b 为信道误比特率。

若信道编码类型为分组码，设信道编码参数为 (n_1,k_1,t_1)，根据文献[4]，在理想的纠错情况下，基于分组信道编码的信息隐藏容量为

$$M+\left(CP_b-MP_b\right)\le\frac{C}{n_1}t_1 \tag{1}$$

$$M\le\frac{\frac{C}{n_1}t_1-CP_b}{1-P_b} \tag{2}$$

$$M_{\max}=\left\lfloor\frac{C_0}{k_1}\right\rfloor\frac{t_1-n_1P_b}{1-P_b} \tag{3}$$

若预处理方式未改变秘密信息的大小，则基于分组信道编码的信息隐藏容量为 $M_{\max}$；若秘密信息采用纠错编码方式进行预处理，且纠错编码参数为 (n_2,k_2,t_2)，则基于分组信道编码的信息隐藏容量为

$$M_{0\max}=\left\lfloor\frac{C_0}{k_1}\right\rfloor\frac{t_1-n_1P_b}{1-P_b}\frac{k_2}{n_2} \tag{4}$$

若信道编码类型为卷积码，设信道编码参数为 (n_1, k_1, t_1)，其中，L 表示编码约束长度，其值一般为 $L=(t_1+1)n_1$，表示当前码组与前 t_1 个码组有关，t_1 表示编码约束长度内的可纠错数，则基于卷积信道编码的信息隐藏容量为

$$M+\left(CP_b-MP_b\right)\le\frac{C}{L}t_1 \tag{5}$$

$$M\le\frac{\frac{C}{L}t_1-CP_b}{1-P_b} \tag{6}$$

$$M_{\max}=\left\lfloor\frac{C_0}{k_1}\right\rfloor n_1\frac{\frac{t_1}{L}-P_b}{1-P_b} \tag{7}$$

同理，若预处理方式未改变秘密信息的大小，则基于卷积信道编码的信息隐藏容量为 $M_{\max}$；若秘密信息采用纠错编码方式进行预处理，且纠错编码参数为 (n_2,k_2,t_2)，则基于卷积信道编码的信息隐藏容量为

$$M_{0\max}=\left\lfloor\frac{C_0}{k_1}\right\rfloor n_1\frac{\frac{t_1}{L}-P_b}{1-P_b}\frac{k_2}{n_2} \tag{8}$$

3.2　二级定位嵌入机制

为了提高嵌入位置选择的随机性，改进算法引入二级定位嵌入机制。二级定位嵌入机制的过程如图 3 所示。

图 3 中，假设信道编码输出长度为 n，分组数为 N，秘密信息长度为 M，且 $M\le N$，则二级定位算法可以表述为：首先按照秘密信息长度生成分组选择序列 S_1，其值为 $S_1=(s_{11},s_{12},\text{L},s_{1M})$，即 S_1 中的元素值为整数集合 $\{1,2,\text{L},N\}$ 中的任意 M 个。然

后根据密钥 K 及秘密信息长度 M 生成伪随机序列 S_2，其值为 $S_2=\{s_{21},s_{22},\cdots,s_{2n}\},1\le s_{2i}\le n$；最后，对于第 i 位秘密信息，根据 S_1 中的 s_{1i} 值来选择嵌入的分组位置，根据 S_2 中的 s_{2i} 值来确定该分组内的具体位置。相比文献[3~6]中已有算法的嵌入位置选择过程，即根据随机数 s_i 将第 i 比特秘密信息嵌入在第 i 组载体数据的第 s_i 比特，改进算法中每一位秘密信息的嵌入位置均由序列 S_1 和序列 S_2 共同确定，因此在一定程度上提高了嵌入位置选择的随机性。

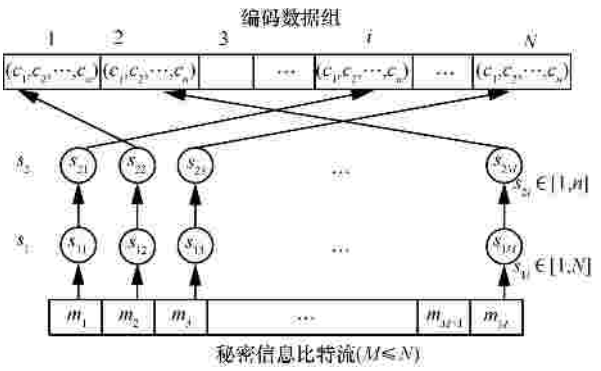

图 3 二级定位嵌入机制示意

但是，当 $M>N$ 时，信息覆盖问题就出现了。在算法中，为保证隐藏信息不出现覆盖现象，改进算法在嵌入位置的选择方面也做了改进。

首先，判断隐藏信息长度与信道编码分组数的大小：若隐藏信息长度不大于分组数，那就按照上述二级定位机制来选择嵌入位置。若隐藏信息长度大于分组数，则 $S_1=randperm(1,N)$，而且需要对秘密信息按照分组数长度进行分组，分组数为 $Packets=\lceil M/N\rceil$。第一组按照 $M\le N$ 时候的方法进行嵌入。嵌入完成后，将 S_2 数值加 1 取模 n 实现循环移位，以得到下一组秘密信息的位置选择序列。经过 $n-1$ 次移位可得 n 个不同的位置选择序列，最多可作为 n 组秘密信息的位置选择序列。具体流程如图 4 所示。移位次数由变量 $count$ 标识，以此类推，直到秘密信息全部嵌入或者 $count=n$ 时结束。一般来说，如果秘密信息长度满足系统隐藏容量的要求，那么在满足条件 $count=n$ 之前，秘密信息可以完全嵌入到载体中。

综上所述，较之现有算法，改进算法在秘密信息嵌入前充分考虑了系统隐藏容量上限问题，较好地避免了因隐藏容量过大而导致秘密通道暴露的风险。而且当秘密信息较大时，改进算法在嵌入位置选择过程中引入二级定位及循环移位机制，既提高了嵌入位置选择的随机性，又避免了秘密信息相互覆盖的风险。

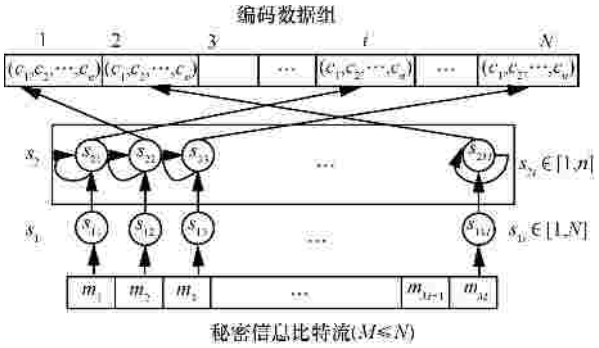

图 4 隐藏信息长度大于分组数时的嵌入位置选择

3.3 改进算法总体流程

引入信息隐藏容量分析模块以及二级定位嵌入机制后，本文提出的编码信道改进信息隐藏算法总体流程如图 5 所示。

大体步骤如下。

为避免秘密信息的大小超过隐藏系统容量而暴露信息隐藏通道，改进算法在秘密信息嵌入前设置容量分析模块。根据信道编码类型和预计的最差信道状况生成隐藏容量阈值，若待隐藏信息的长度不小于该数值，则隐藏过程不执行。

若隐藏信息长度符合要求，则按拟定的二级定位算法规则进行嵌入。

秘密信息的提取过程为嵌入过程的逆运算，即根据位置选择序列 S_1 和 S_2，从接收到的信息码流中提取秘密信息。

4 隐藏容量数值分析

由基于信道编码的信息隐藏原理可知，以信道编码为载体的信息隐藏容量与载体类型、信道编码方式以及信道条件有关。定义信息隐藏嵌入率为

$$Ratio=\frac{\text{嵌入秘密信息长度}}{\text{编码后的信源信息长度}} \tag{9}$$

当载体图像大小为 768 KB，秘密信息预处理方式为 (31,21,2)BCH 纠错编码，信道编码方式分别为(63,30,6)BCH 码、(15,7,4)RS 码、(2,1,9)卷积码以及(1024,3,6)LDPC 码时，做如下的分析。

图 6 和图 7 分别表示不同信道编码下的伪装载体误比特率、译码后的信源信息误比特率。

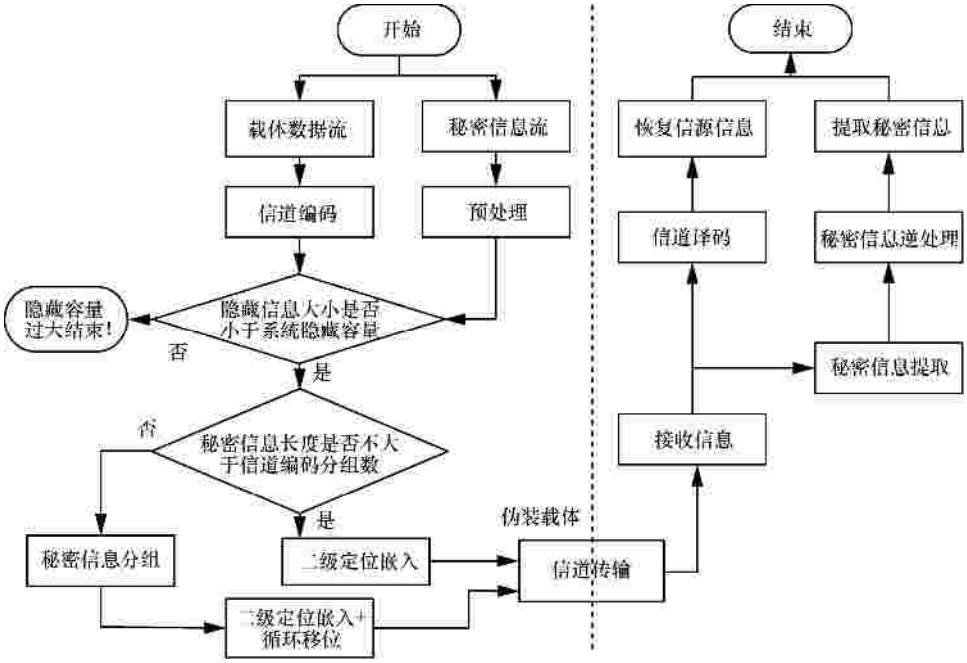

图 5　改进信息隐藏算法流程

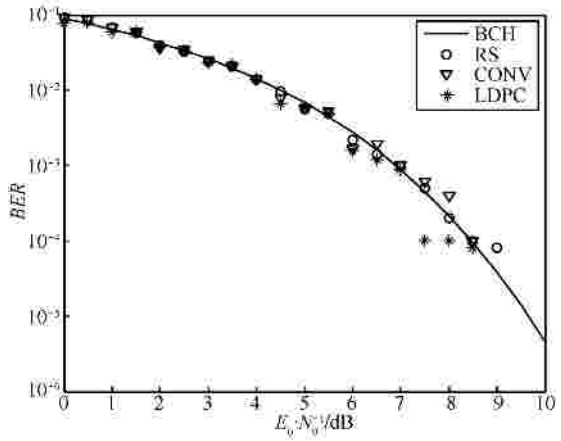

图 6　不同信道编码下的伪装载体误比特率

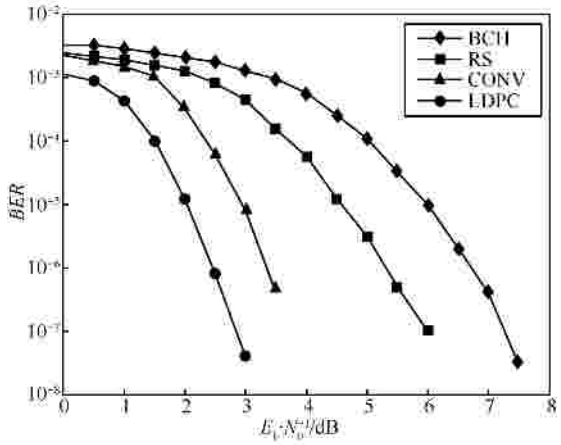

图 7　不同信道编码下的信源信息误比特率

图 6 中的曲线及描点分别表示以 BCH 编码、RS 编码、卷积编码以及 LDPC 编码为载体的信息隐藏系统嵌入秘密信息后，伪装载体与原始载体比较而得的误比特性能。它反映了秘密信息的嵌入及信道噪声的干扰对原始载体的影响程度。从图 6 中可以得出一个结论：就某一种信道编码而言，嵌入相同的秘密信息时，信噪比越高，即信道条件越好，则系统误比特率越低。对于信源信息来说，信道噪声与秘密信息都被当作随机干扰来处理，两者效应之和不能超过信道编码纠错能力。因此，只要信道条件不是极其恶劣，即信道产生的干扰不至于超出信道编码的纠错能力，此时，嵌入一定量的秘密信息也能保证伪装载体的误比特率在可接受的范围之内，不会破坏正常的通信。

图 7 中的曲线表示在不同信道条件下不同信道编码信源信息的误比特性能。从图中可知，当总的信道误比特效应相同时，信道编码的纠错能力越强，则译码后的信源信息误比特率越小。结合图 6 和图 7 进行分析，对于以 RS 和 BCH 编码为载体的信息隐藏系统来说，当伪装载体的误比特效应达到 10^{-3} 数量级时，经过信道译码后，信源数据的误比特率可以达到 10^{-6} 数量级，若再提高信道信噪比，那么基本上可以无误地还原信源信息。

表 1 及表 2 中的数据分别表示以 BCH 编码以及 LDPC 编码为载体的信息隐藏系统误比特性能。其中，两表中 p_e^1 表示伪装载体的误比特率，p_e^2 表示提取的秘密信息误比特率，p_e^3 表示信源信息的误比特率。

最后，笔者分析若信道误比特率确定，根据式(4)和式(8)可得基于信道编码的信息隐藏容量性能如图 8 所示。

从图 8 中可以看出，当载体信息确定时，随着信道干扰造成的误比特率的降低，基于信道编码的信息隐藏容量增加，且当信道误比特率相同时，信道编码的纠错能力越强，基于该信道编码的隐藏信息嵌入率就越大。但是对于具体的信道编码方式而言，当信道干扰造成的误比特率降低到一定程度时，隐藏容量值趋于稳定。这是因为，由式(4)和式(8)可知，当载体大小固定且 $p_b \to -\infty$ 时，若信道编码类型为分组编码，则信息隐藏容量满足 $M_{0\max} \to \left\lfloor \frac{C_0}{k_1} \right\rfloor t_1 \frac{k_2}{n_2}$；若信道编码类型为卷积码，则信息隐藏容量满足 $M_{0\max} \to \left\lfloor \frac{C_0}{k_1} \right\rfloor n_1 \frac{t_1}{L} \frac{k_2}{n_2}$，所以隐藏容量并不会随着信道误比特率的降低而一直增加。

从图 8 中还可知，当载体和信道编码方式确定时，虽然信息隐藏容量都会趋于一个稳定值，但是信道编码的纠错能力越强，则基于该信道编码的隐藏容量趋于稳定所要求的信道误比特率条件越宽松，也就是说，利用纠错能力较强的信道编码可以更好地在恶劣信道中实现信息隐藏。例如，要使秘密信息嵌入率

表 1 以 BCH 编码为载体的信息隐藏误比特性能

p_e	E_b/N_0							
	0	1	2	3	4	5	6	7
p_e^1	0.091 9	0.067 8	0.039 9	0.024 1	0.013 8	0.005 7	0.002 2	0.000 98
p_e^2	0.008 4	0.007 5	0.006 15	0.004 51	0.002 25	0.001 20	0.000 8	0.000 02
p_e^3	0.003 21	0.002 82	0.001 97	0.001 23	0.000 56	0.000 11	0.000 01	0.000 002

表 2 以 LDPC 编码为载体的信息隐藏误比特性能

p_e	E_b/N_0							
	0	1	2	3	4	5	6	7
p_e^1	0.078 1	0.060 0	0.036 8	0.022 8	0.013 9	0.006 1	0.001 5	0.000 86
p_e^2	0.008 3	0.007 4	0.006 2	0.004 82	0.002 41	0.000 91	0.000 28	0.000 03
p_e^3	0.001 08	0.000 31	0.000 08	0	0	0	0	0

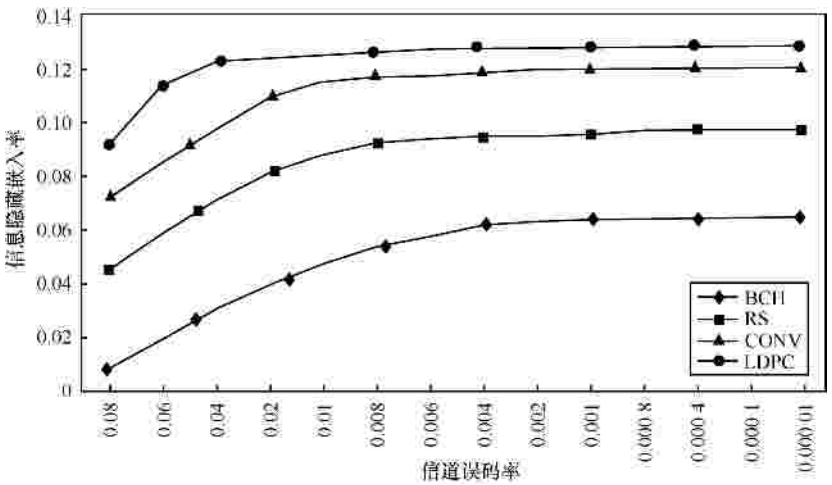

图 8 确定信道误比特率下的信息隐藏容量

达到6%，则以 BCH 编码为载体的信息隐藏系统要求信道干扰造成的误比特率低于6×10^{-3}，而基于 RS 编码的信息隐藏系统只需保证信道误比特率不大于6×10^{-2}，对于卷积码和 LDPC 编码而言，当信道造成的误码效应不超过8×10^{-2}数量级时，信息隐藏系统的嵌入率均可超过6%。另外，以 BCH 码为载体的信息隐藏容量趋于稳定的要求是：保证信道造成的误比特率控制在10^{-3}数量级，而基于 LDPC 编码的信息隐藏系统只要求信道误比特率的大小达到10^{-2}数量级。

由于信道编码的纠错能力有限，对于选定的隐藏载体，基于信道编码的信息隐藏容量是有上限的，若秘密信息大小超过该上限值，那么会使信源信息无法正确地恢复。所以，本文方法在秘密信息嵌入之前首先进行容量的判断，该方法具有重要意义和实用价值。

5　算法优势及复杂度分析

5.1　优势分析

笔者将提出的改进算法与文献[3~6]的算法进行比较，得到如表 3 所示的结果。

从表 3 可以看出，本文提出的二级定位算法通过将容量分析应用到具体算法中，并结合二级定位机制和循环移位方法，能有效地改善信息隐藏的效果。

5.2　开销与复杂度分析

5.2.1　存储开销分析

首先分析算法在存储上的开销。将二级定位算法与较完整的文献[5]中的信息隐藏算法进行比较（后简称：原有算法）。假设秘密信息不超过系统的最大隐藏容量，且假设待嵌入信息的长度与信道编码分组数的比值为 $R(R\geq1)$。该比值 R 表示平均每个信道编码分组所嵌入的信息为 R bit。若按一次嵌入操作只在每个分组中嵌入 1 bit 信息来计算，比值 R 表示需要进行 R 次嵌入操作才能将秘密信息完全隐藏，则 2 种算法在密钥分配和伪随机序列存储上的开销如表 4 所示。

表 4　　2 种算法的存储开销

算法	存储开销	
	密钥数	伪随机序列数
二级定位算法	1	2
原有算法	R	R

从表 4 中可以看出，原有算法的存储空间随着 R 的增大而增加。由表 4 可知，只有在 R=1 的情况下原有算法的性能略好于二级定位算法。R=1 表明秘密信息的大小不大于信道编码的分组数，也就是说，每个信道编码分组中至多嵌入 1 bit 秘密信息。这种情况对于秘密信息的大小限制是极为严格的。当 $R\geq2$ 时，改进的二级定位算法的存储空间明显小于原有算法。一般来说，信息隐藏系统要保证一定的隐藏容量，并且在不影响系统不可见性的前提下，最好尽可能多地隐藏信息。信息隐藏系统的发展趋势必定是实现大容量信息的安全隐藏。因此，对于大容量信息隐藏系统而言，较之原有算法，二级定位算法在存储开销上有着较大的优势。

5.2.2　计算复杂度分析

在计算复杂度方面，提出的二级定位改进算法相比原有算法[5]，主要增加了容量分析模块，而在二级定位及循环移位机制方面，增加的复杂度不多。

在容量分析模块中，由于笔者已经定义出各信道编码情况下的容量公式，所以当一个信道系统的参数如 (n_1,k_1,t_1) 及 (n_2,k_2,t_2) 等确定之后，按照公式 $M_{0\max}=\left[\frac{C_0}{k_1}\right]n_1\frac{\frac{t_1}{L}-P_b}{1-P_b}\frac{k_2}{n_2}$ 就可以计算出相应的容量。这个计算过程是一个线性计算，其复杂度为 $O(1)$。

另外在二级定位及循环移位机制中，二级定位仅仅比单次定位多了一次定位随机数生成过程，而且这个定位随机数是在编码长度 n 范围内生成，复杂度较低。另外，循环移位机制是做一次移位处理，

表 3　　二级定位算法的优势分析

算法	预防机制	定位方法	循环移位
文献[3]	无	小波域嵌入	无
文献[4]	提出了容量分析模型	无	无
文献[5]	建立了容量分析模型	单次定位	无
文献[6]	无	单次定位	无
二级定位算法	建立容量分析模型，并运用到具体算法中	二级定位，更灵活准确	带循环移位机制，防止秘密信息相关覆盖

而且这个移位处理仅当 $M > N$，也就是原有算法发生信息覆盖时进行，由此引入的复杂度相比整个信息隐藏系统性能提高而言，甚为微小。

6 MATLAB 仿真验证

接下来基于 MATLAB 软件对提出的算法进行仿真实验。假设载体信息为 768 KB 的 lenna.jpg 图像，秘密信息大小分别为 2 KB、19 KB 和 27 KB，其他的具体实验参数见表 5。

6.1 容量上限实验

此项仿真选用的载体图像大小为 768 KB，信道编码方式分别为(63, 30, 6)BCH 码，秘密信息大小为 27 KB，采用(31, 21, 2)BCH 纠错编码。图 9 表示在 AWGN 信道中，信道信噪比为 10dB 时，隐藏容量超过信道编码纠错能力上限时的信源信息及秘密信息的恢复图。

根据式(4)及图 8 中的 BCH 曲线可知，当采用(63,30,6)BCH 信道编码、(31,21,2)BCH 码纠错编码时，随着信道条件的改善，信息隐藏容量逐渐增大，当信道为理想状态时，信息隐藏嵌入率约为 0.064 5。若秘密信息大小为 27 KB，则经计算可得，此时的嵌入率为 0.098 8，大大超过了系统的隐藏容量上限。

从图 9 中可以看出，当嵌入量过大时，载体图像被噪声严重污染，导致接收端无法正确地还原载体信息。若出现此类情况，则监听者会认为该信道可能被人为利用，一方面，可以对本次截获的信息流进行信息隐藏分析，提取秘密信息；另一方面，隐藏通道的暴露会导致后续更多的秘密信息被监听。由此可以看出，信息隐藏容量分析模块的引入有利于提高信息隐藏系统的安全性。

图 9 信息隐藏效果示意图

6.2 与原有算法的比较

根据 MATLAB 仿真结果考虑本文提出的二级定位改进算法（简称：改进算法）和文献[5]中的原有算法在信源误比特率和秘密信息误比特率方面的性能。

由表 5 的数据可知，当秘密信息大小为 19 KB 时，秘密信息与编码数据流的比值约为 0.025。根据图 8 的数值分析结果可知，当信道干扰造成的误比特率达到 10^{-2} 数量级时，系统可承受的秘密信息大小与编码数据长度的比例大于 0.025。也就是说，信道误比特率达到 10^{-2} 数量级时，嵌入的 2 KB 大小和 19 KB 大小的秘密信息均不会超过隐藏容量上限。

表 5 本文算法对比实验时的 MATLAB 仿真参数

仿真参数	具体参数值	
载体信息	768 KB lenna.jpg	
信道编码方式	(63,30,6)BCH	
信道编码分组数	$N=\left\lceil\frac{768\times1\,024\times8}{30}\right\rceil=209\,715$	
编码后的信源信息长度	$C=63\times N=63\times\left\lceil\frac{768\times1\,024\times8}{30}\right\rceil=13\,212\,045$	
秘密信息	Xh_2.jpg(2 KB)	Xh_19.jpg(19 KB)
纠错编码方式	(15, 7, 4) RS	(15, 7, 4) RS
编码后的秘密信息长度	$M_1=\left\lceil\frac{2\times1\,024\times8}{7}\right\rceil\times15=35\,100$	$M_2=\left\lceil\frac{19\times1\,024\times8}{7}\right\rceil\times15=333\,525$
嵌入比率	$Ratio_1$=0.002 7	$Ratio_2$=0.025 0

但是，若按照现有的嵌入算法进行信息隐藏，由于纠错编码后的秘密信息数据长度已经超过信道编码的分组数，所以当在每个信道编码分组中嵌入 1 bit 信息后，剩余的秘密信息需要从第一个分组开始进行新一轮的嵌入过程。又因为位置选择序列具有随机性，第二次的嵌入位置有可能和第一次重复，从而造成信息覆盖。将 2 KB 和 19 KB 大小的秘密信息图像分别采用原有嵌入算法和改进二级定位嵌入算法隐藏到信道编码数据流中，得到的误比特性能如图 10 所示。

从图 10 中可以看出：在没有超过隐藏容量上限时，当秘密信息大小为 2 KB 时，传统算法与改进算法性能相当；当秘密信息大小为 19 KB 时，采用改进算法进行信息隐藏后，提取的秘密信息的误比特性能明显好于原有算法。这是因为，当秘密信息较大时，采用改进算法可以避免嵌入的秘密信息相互覆盖的问题，从而提高秘密信息的准确性。但是，从图 10(c)中可以看出，当信道条件不是很理想时，采用改进算法得到的信源信息误码性能要比原有算法略差，这是因为，当秘密信息较大时，采用原有算法进行信息隐藏时出现秘密信息覆盖的情况，这就相当于减小了秘密信息产生的噪声效应，所以信源信息的译码效果要稍好一些。

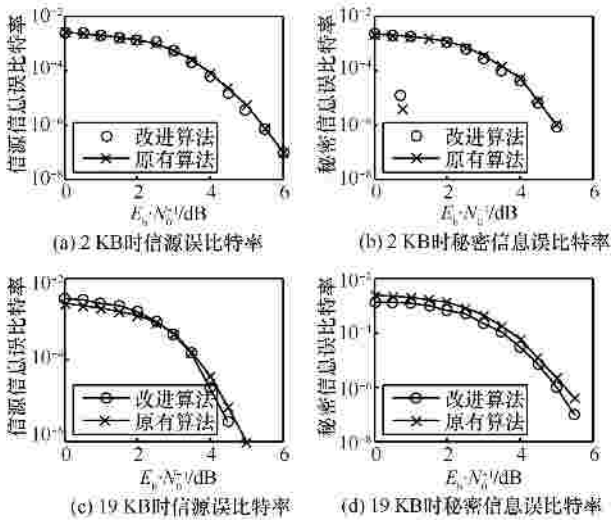

图 10　改进算法与现有算法的性能比较

从实际情况考虑，基于信道编码的信息隐藏系统旨在实现信息隐藏，只要保证信源信息在一定的信道信噪比条件下能够基本恢复，而不引起监听者的怀疑即可。而且，信息隐藏的性能指标之一是隐藏容量，由图 10 可知，改进算法可以在隐藏容量较大时获得较好的信源信息误比特性能，实用性较强。

另外，信息隐藏系统通常使用归一化系数来描述原始秘密信息与提取秘密信息之间的相似程度，其定义如下

$$NC = \frac{\sum_{i=0}^{N-1} I(i)I'(i)}{\sqrt{\sum_{i=0}^{N-1} I^2(i)}\sqrt{\sum_{i=0}^{N-1} I'^2(i)}} \tag{10}$$

其中，N 表示隐藏信息长度，I 表示原始秘密信息，I' 表示提取后的秘密信息。NC 越大，表示提取秘密信息的正确性越高，说明系统的顽健性越好。

当秘密信息大小为 19 KB 时，在各信道信噪比条件下，使用改进算法和原有算法得到的秘密信息归一化系数如图 11 所示。

从图 11 中可知，采用改进算法获得的秘密信息 NC 值明显大于原有算法，尤其当信道条件较不理想时，这种优势更加明显。但是，NC 值的提高不是无限的，当信道条件较好，秘密信息可以完全无误地提取时，NC 值趋于稳定。

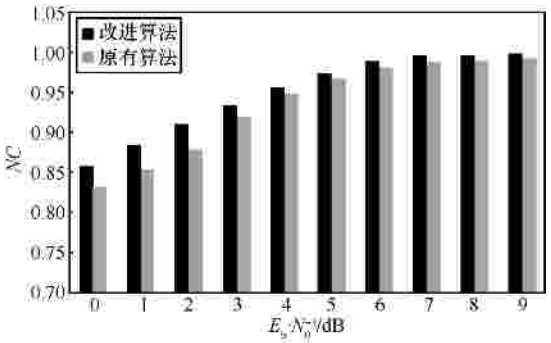

图 11　2 种算法得到的秘密信息归一化系数

另外，伪装载体的峰值信噪比 PSNR 测试结果如图 12 所示。

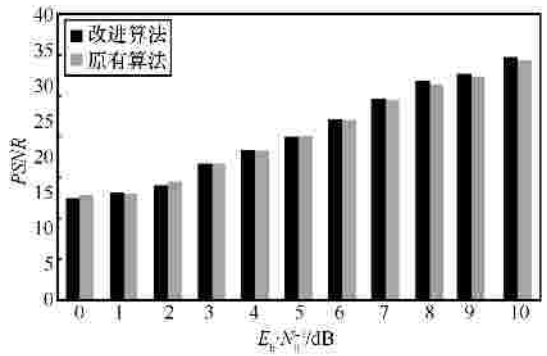

图 12　2 种算法得到的伪装载体峰值信噪比 PSNR

从图 12 中可以看出，伪装载体的峰值信噪比会随着信道信噪比的增加而增加。而采用改进算法后，相比原有算法，两者伪装载体图像的峰值信噪比大小并没有很大的差距。这是因为编码信源的干扰源有 2 类，即信道本身存在的干扰和秘密信息，而这 2 个条件对于嵌入算法来说是基本固定的。但是，从图 11 可以看出，不同算法的选择对秘密信息归一化系数有着很大的影响。

7 结束语

本文通过对现有的编码信道信息隐藏算法的分析，提出了一种基于二级定位的编码信道信息隐藏改进算法。算法在秘密信息嵌入前分析并考虑系统隐藏容量上限问题，在嵌入位置选择过程中引入二级定位及循环移位机制。经数值分析及 MATLAB 仿真分析可知，较之原有算法，改进算法在秘密信息较大的情况下能够避免发生秘密信息覆盖的风险，提高秘密信息的误比特性能。随着大容量信息隐藏需求以及信道编码技术的日益发展，基于二级定位的编码信道信息隐藏技术必将获得广泛的发展与应用。

参考文献：

[1] MOULIN P, O'SULLIVAN J A. Information-theoretic analysis of information hiding[J]. IEEE Transactions on Information Theory, 2003, 49(3):563-592.

[2] 王伟祥, 刘玉君, 李文雄. 基于 *m* 序列的信道编码信息隐藏算法[J]. 计算机工程, 2007, 33(6):118-119, 122.
WANG W X, LIU Y J, LI W X. Information hiding algorithm in channel coding based on *m*-sequence[J]. Computer Engineering, 2007, 33(6):118-119, 122.

[3] 王桂艳, 马社详. 基于纠错编码的信息隐藏算法[J]. 天津理工大学学报, 2008, 24(3):40-42.
WANG G Y, MA S X. Information hiding based on integer DWT and error correct coding[J]. Journal of Tianjin University of Technology, 2008, 24(3):40-42.

[4] 阎雪虎. 基于纠错码的信息隐藏容量模型[J]. 计算机工程, 2010, 36(3):172-173, 176.
YAN X H. Information hiding capacity model based on error-correcting codes[J]. Computer Engineering, 2010, 36(3):172-173, 176.

[5] 王晓飞. 基于信道编码的信息隐藏技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2009.
WANG X F. Research on Channel Coding Based Information Hiding Techniques[D]. Harbin: Harbin Institude of Technology, 2009.

[6] 王天宇, 刘玉君, 唐冬明等. 基于 RS 码的有扰信道信息隐藏技术的研究[J]. 信息工程大学学报, 2004, 5(3):85-88.
WANG T Y, LIU Y J, TANG D M, *et al*. Study of information hiding based on RS code in noise channel technology[J]. Journal of Information Engineering University, 2004, 5(3):85-88.

[7] 王伟祥, 刘玉君, 李文雄. 利用 LDPC 码实现信道编码信息隐藏技术[J]. 信息工程大学学报, 2006, 7(1):49-50,53.
WANG W X, LIU Y J, LI W X. Implementation of information hiding technology in channel coding using low-density parity-check code[J]. Journal of Information Engineering University, 2006, 7(1):49-50,53.

[8] YAN X H, GUAN S, NIU X M. Research on the capacity of error-correcting codes-based information hiding[A]. International Conference on Intelligent Information Hiding and Multimed Signal Processing[C]. Harbin, China, 2008.1158-116.

[9] HARMSEN J J, PEARLMAN W A. Capacity of steganographic channels[J]. IEEE Transactions on Information Theory, 2009, 55(4): 267-273.

[10] CHEN L Q, LU M, CHEN J B. Researches and simulations of information hiding in alamouti transmission system[A]. The Seventh International Conference on Computational Intelligence and Security[C]. Sanya, China, 2011.593-597.

作者简介：

陈立全（1976-），男，广西玉林人，东南大学副教授、硕士生导师，主要研究方向为信息安全、信息隐藏。

卢苗（1987-），女，浙江湖州人，东南大学硕士生，主要研究方向为编码信道信息隐藏。

胡爱群（1964-），男，江苏如皋人，东南大学教授、博士生导师，主要研究方向为无线网络信息安全。

孙晓燕（1989-），女，江苏南通人，东南大学硕士生，主要研究方向为信息隐藏。