项目编号: 密级：XXXX 保存期限：X年

**XXXXXXXXX合作项目**

技术研究报告

（YYYY年度）

项目名称：

项目承担单位：

项目责任人：

项目委托单位：XXXXX

项目起止年限： 年 月至 年 月

填报日期： 年 月 日

说 明

一、本技术研究报告一般应由项目负责人填写。

二、所填各项内容，应按栏目所列要求详细、准确、清楚地填写，篇幅不够的栏目可自行加页。

三、请勿更改封面字体，正文用宋体四号字。

四、A4幅面纸，双面打印，左侧装订。

五、一式三份及电子版。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 撰写 | 撰写人 |  | 撰写日期 |  |
| 版本号 |  | 联系方式 |  |
| 审核 | 审核人 |  | 审核日期 |  |
| 联系方式 |  |
| 修订 | 修订人 |  | 修订日期 |  |
| 版本号 |  | 联系方式 |  |
| 修订 | 修订人 |  | 修订日期 |  |
| 版本号 |  | 联系方式 |  |

目 录

[1. 项目研究简况 5](#_Toc489714282)

[1.1项目背景 5](#_Toc489714283)

[1.2合同技术指标 5](#_Toc489714284)

[1.3国内外同类技术查新 5](#_Toc489714285)

[2. 项目目标和主要研究内容 6](#_Toc489714286)

[2.1项目研究目标 6](#_Toc489714287)

[2.2技术设计的依据和主导思想 6](#_Toc489714288)

[2.3解决的主要问题、技术难点 6](#_Toc489714289)

[3. 技术方案 7](#_Toc489714290)

[3.1技术原理和路线 7](#_Toc489714291)

[3.2具体实施方案 7](#_Toc489714292)

[3.2.1技术方案选择及调整情况 7](#_Toc489714293)

[3.2.2技术实现过程 7](#_Toc489714294)

[3.2.3关键技术与实现 8](#_Toc489714295)

[3.3与已有成果的比较 8](#_Toc489714296)

[4. 技术特点、创新性及达到的指标 9](#_Toc489714297)

[4.1技术特点 9](#_Toc489714298)

[4.2创新性 9](#_Toc489714299)

[4.3 总体性能及指标 9](#_Toc489714300)

[4.3.1 总体性能 9](#_Toc489714301)

[4.3.2 技术指标 9](#_Toc489714302)

[5. 总结 10](#_Toc489714303)

[5.1研制过程的经验与教训 10](#_Toc489714304)

[5.2技术成熟程度，推广应用的条件和前景 10](#_Toc489714305)

[5.3存在的问题及后续工作展望 10](#_Toc489714306)

[6. 附件(电子类)<包括但不限于此> 11](#_Toc489714307)

[6.1软件设计 11](#_Toc489714308)

[6.2硬件设计 11](#_Toc489714309)

[6.3参考文献等 11](#_Toc489714310)

[7、附件（化学类）<包括但不限于此> 12](#_Toc489714311)

[7.1试剂 12](#_Toc489714312)

[7.2工具 12](#_Toc489714313)

[7.3制作工艺等 12](#_Toc489714314)

[7.4参考文献等 12](#_Toc489714315)

[8、附件（生化类）<包括但不限于此> 13](#_Toc489714316)

[8.1产品配方及工艺 13](#_Toc489714317)

[8.2原料来源及成品的质检标准 13](#_Toc489714318)

[8.3参考文献等 13](#_Toc489714319)

[9、附件（其它类） 14](#_Toc489714320)

[10、其它说明 14](#_Toc489714321)

# 项目研究简况

1.1 项目背景

随着计算机网络技术和多媒体技术的广泛应用，信息隐藏技术得到了极大地推动。信息隐藏技术利用载体信息在时间或空间等方面的冗余特性，把秘密信息隐藏到载体信息中，从而得到隐秘载体。隐写术作为信息隐藏的重要分支，可以将秘密信息嵌入到图像、音频、视频等多媒体文件中，并且隐秘载体可以在公开信道上传输。隐写后，第三方无法确认隐秘载体中是否隐藏了信息，也很难提取或者去除所隐藏的信息，从而达到隐蔽通信，版权保护等目的。

音频作为使用最多的多媒体文件格式之一，应用十分广泛。音乐分享平台、网络电台、微信语音等都使用音频信号进行传播，因此采用数字音频作为载体，具有较好的伪装性。其中，MP3作为最流行的音频格式，具有隐写容量大，内容较为复杂等优点，是一种理想的隐写术嵌入载体。因此，基于MP3的音频隐写方法一直以来是国内外学者的重点研究对象。

为了实现隐蔽通信，在设计和实现隐写方法时需要综合考虑嵌入容量、不可检测性和不可感知性等因素，使得载体文件在进行信息嵌入后在感官质量、不可检测性和统计特性性上基本保持不变。现存的MP3隐写方法主要分为基于编码参数的隐写方法和基于编码数据的隐写方法。其中，基于编码参数的MP3隐写方法普遍隐写容量较低，且对音频的改动较大，容易被检测出。基于编码数据的MP3隐写方法与基于编码参数的隐写方法相比，隐写容量大幅提高，但是在隐写过程中依旧没有考虑嵌入操作对载体的感知性和统计特性的影响，也没有采用合理的方式避免在对载体影响较大的位置进行隐写，因此在抗隐写分析方面仍显不足。

为了提高隐写方法的安全负载，近些年来学术界提出了以自适应隐写术为代表的新型隐写术。自适应隐写术主要研究在保证一定的安全负载的情况下，根据音频内容选择嵌入位置，采用STC代数编码结合失真代价函数的方法，对载体进行自适应隐写。这种方法能够在载体中选择最佳的嵌入路径，减少对载体的修改次数，降低对载体的扰动，最小化嵌入操作对载体引起的失真。所以，自适应隐写算法一般具有较高的安全负载。目前，由于音频编码技术等因素的限定，尚不存在基于MP3的自适应隐写方法。

对此，本课题提出了两种基于MP3的自适应隐写方法，分别是基于等长熵码字替换的MP3自适应隐写方法和基于符号位修改的MP3自适应隐写方法。这两种隐写方法分别将MP3码流结构中的哈夫曼码字和系数符号位作为嵌入域，具有较大的隐写容量，根据心理声学模型设计相应的代价函数，结合STC编码方案实现自适应隐写。

1.2 合同技术指标

本项目主要成果为音频自适应隐写系统，达到的技术指标包括：

1、数字音频格式。可支持MP3和WAV格式。

2、代价函数类型和数量。包含针对MP3域和针对时域的两类代价函数构造方法，数量不少于3种。

3、压缩码率。可以支持无损码率，96kbps、128kbps、160kbps、192kbps、320kbps等。

4、算法参数。可以支持负载率参数动态调整范围[0.1,0.5]，矩阵高度参数动态调整范围[7,12]。

5、隐写容量。在不同码率载体下，压缩域自适应隐写算法的平均隐写容量2kbps。

6、安全性指标。支持对软件算法的安全性做测试与验证，在1.8kbps嵌入率下攻击算法的检测准确率75%、在1.1kbps嵌入率下攻击算法的检测准确率65%。

7、嵌入速率。考虑到编码器的影响并利用指令加速、分段并行STC等优化技术后满足嵌入速率6.7kb/s(包括MP3压缩编码计算耗时)。

8、软件质量。软件界面设计合理，容易操作，稳定性强，除特定的算法开销，一般操作运行流畅。

9、文档质量。研究报告能够从原理上有力支撑以上系统的设计原则和采用的方法；自测报告数据详实，过程可重复；操作说明书可读性强，内容明确，阅读容易。

1.3 国内外同类技术查新

由于压缩域隐写方法与音频压缩编码标准有很大关联，主要依赖于编码参数和压缩流数据等因素。因此，按照印象隐写方式的因素，目前压缩域隐写可以分为基于编码参数的隐写方法和基于编码数据的隐写方法。常用于隐写的编码参数包括量化步长、码表索引、窗口类型、码率索引和比例因子长度索引等。基于编码数据的隐写包括码字映射和量化系数的修改等。其中MP3Stego算法是最经典的基于量化补偿的修改方法，他在MP3编码的内存循环中实现秘密信息的嵌入，通过调节量化误差的大小，将量化编码后的part2\_3块长度的奇偶性作为秘密消息的嵌入依据。Yan等人提出了一种基于量化步奇偶性的MP3隐写算法，通过修改量化不长的奇偶性来嵌入秘密信息。Yan提出了一种基于哈夫曼码表索引的MP3隐写算法，在编码过程中根据秘密信息选择编码使用的哈夫曼表，达到信息嵌入的目的。Yan提出了一种窗口类型转换达到嵌入信息的目的。码字映射隐写是利用哈夫曼编码阶段通过利用等长哈夫曼码字替换的方式进行信息隐藏的方法，本质上是一种特殊的量化系数修改方法。这类隐写算法具有很高的透明性和较大的嵌入容量。Liu和Guo提出了一种在QMDCT系数小值区进行哈夫曼码字替换的信息嵌入方法。Gao提出了一种哈夫曼码字替换的隐写算法，该算法直接在MP3大值区编码数据流上实现了信息的嵌入和提取。Yan在Gao哈夫曼码字替换的基础上进行改进，可以实现混合进制的隐写，增大了算法嵌入容量。

但是上述这些隐写方法受编码技术的、嵌入方案等因素的影响，并没有与自适应隐写相结合，在抗隐写分析方面性能较差，安全负载很低，因为不具备很好的实用性。本项目以目前最为流行的MP3编码技术为基础，结合STC编码策略，设计了合适的代价函数，实现了基于MP3的自适应隐写，能过合理平衡项目对嵌入容量和安全性等重要性质的需求。

# 项目目标和主要研究内容

2.1 项目研究目标

本项目的总体目标是，针对MP3和WAV格式的音频，研发嵌入容量大、透明性高、抗检测性强的自适应隐写方法，研发基于这种具有高安全负载的自适应音频隐写算法的新型隐写系统，可以安全嵌入多种格式的消息文件。项目的研究目标具体可以包括以下4个方面：

1、基于等长熵码字替换的MP3自适应隐写方法。当前基于码字替换的MP3隐写算法是通过对可相互替换的码字进行简单的奇偶分配实现信息嵌入，没有考虑码字替换对载体造成的扰动，导致嵌入效率和安全负载比较低。针对这种情况，以减少嵌入操作对载体的扰动，提高算法安全负载为目标。通过分析可相互替换码字与量化频域系数的分部关系，构造合理的码字搜索方案，根据心理声学模型设计相应的代价函数，计算失真并以码字奇偶分配后的二进制比特串为载体，结合STC编码方案实现自适应隐写。

2、基于符号位修改的MP3自适应隐写方法。当前基于符号位的MP3隐写算法，在信息嵌入过程中对符号位进行简单的奇偶分配，会对感知敏感区域的系数进行修改。由于符号位的改变会造成系数修改幅度放大到系数绝对值的二倍，增加了嵌入操作对音频载体的扰动。为了避免在音频敏感区域进行嵌入操作的问题，通过结合频域系数的改变幅度和心理声学模型来设计代价函数，在此基础上结合高效的隐写编码策略，提出具有高安全负载的自适应音频隐写算法。

3、双层自适应MP3隐写方案。传统的音频隐写方法采用顺序嵌入的方式，不可避免的会在静音片段等敏感部分进行修改嵌入，修改成静音片段还带来比较大的感知失真和统计失真，从而降低隐写算法的安全性。针对这种情况，通过帧间自适应可以根据消息长度及帧间代价大小来选择部分嵌入代价小的帧，结合代价函数和STC编码实现帧内自适应嵌入，选择修改代价最小的嵌入路径，使得嵌入操作对载体的扰动最小。通过帧内和帧间相结合的自适应方式实现双层MP3隐写，增大隐写算法的安全负载。

4、基于以上对系统进行隐写设计，研发能够集成以上隐写方法的软件系统。

2.2 技术设计的依据和主导思想

现存的MP3隐写算法主要存在隐写容量低和安全负载低的问题。基于量化步长修改的隐写算法和基于码表索引修改的隐写算法都是基于编码参数实现的MP3隐写，这一类隐写算法容量普遍较低，此外，基于量化编码参数修改的隐写算法将秘密信息嵌入到量化或编码使用的参数中，会导致整帧或者颗粒的编码结果发生改变，对音频的统计特征影响较大，使隐写算法的抗检测能力较弱。基于码字替换的隐写算法和基于量化系数修改的隐写算法在编码数据中嵌入信息，由于编码数据数量较多，这类隐写算法容量普遍高于基于量化编码参数修改的隐写算法。但是，嵌入操作过程中没有考虑数据修改对音频造成的感知失真和统计扰动，导致算法在抗隐写分析方面较弱，安全负载较低。

为了解决MP3隐写算法安全负载较低的问题，需要在嵌入过程中选取修改代价小的嵌入点进行操作。自适应隐写算法能够有效解决这一问题。自适应隐写方法可以保证在一定负载的情况下减少对载体的修改次数，降低对载体的扰动。在适应隐写算法中，嵌入位置的选择、嵌入效率的高低、嵌入容量的大小很大程度上由载体的内容特性决定。结合STC编码可以选择最优的修改路径，使得嵌入总失真最小。自适应隐写需要合理的代价函数来计算每个嵌入点修改对载体带来的失真。音频隐写的代价函数主要从两个方面进行分析：1）心理声学模型，主要分析人耳对音频的感知特性；2）统计特性，隐写分析算法普遍是基于音频统计特性来实现的，以统计特性为基础构造代价函数，能够有效提高隐写算法抗检测能力。

因此，为了设计满足高安全负载且抗检测能力强的MP3的自适应隐写算法，需要基于MP3的编码标准，结合高效的STC编码策略，设计合适的代价函数，使得隐写操作对载体造成的扰动最小。

## 2.2.1 MP3编码

MP3是一种有损压缩的数字音频编码方式，通过心理声学模型，去掉一些人耳无法感知的音频细节，即保证了音频质量又大幅降低了音频数据量。

如图2-1所示，MP3编码时首先将输入的PCM(Pluse Code Modulation）信号进行分帧操作，一个编码帧(frame)包含1152采样点.然后将每帧中的采样点通过子带滤波器组划分成32个相等带宽的子频带信号，接着对每个子频带进行修正离散余弦变换(Modified Discrete



图2-1 MP3编码结构框架图

Cosine Transform,MDCT)，将每个子频带信号又划分成18个频带(长窗)或6个频带(短窗)。利用这种方式消除了子带滤波造成的带间重叠,将音频信号从时域变换到频域.这样共产生576个或192个频带。同时，对输入的PCM信号进行快速傅里叶变换(Fast Fourier Transformation,FFT)后，通过心理声学模型分析音频内容并计算掩蔽效应的阈值，确定每个子频带里的信号能量与掩蔽阈值的比率—信号掩噪比(Signal-to-Mask Ratio,SMR)，并确定在MDCT操作中使用的窗口类型.量化编码部分利用信掩比SMR来决定分配给每一个子带信号的量化位数，使量化噪声低于掩蔽阈值。量化过程中引入迭代算法去控制码率和音损程度，使在满足目标码率情况下，可感知的音损尽可能小。

经过三层迭代量化循环后，MDCT系数被处为容易存储和编码的离散值。每个颗粒中包含576个QMDCT系数。按照系数对应的频率值从低到高的顺序，QMDCT可以分为三个区域，大值区、小值区和零区，如图2-2所示。大值区中的QMDCT系数差异比较大，主要对应音频信号中的低频部分；小值区的QMDCT系数只包含0、-1和1，主要对应音频信号的中频部分；零区中的QMDCT系数全部为0，主要对应音频信号的高频部分。为取得更好的压缩编码效果，大值区部分又划分为三个互补重叠的子区域。

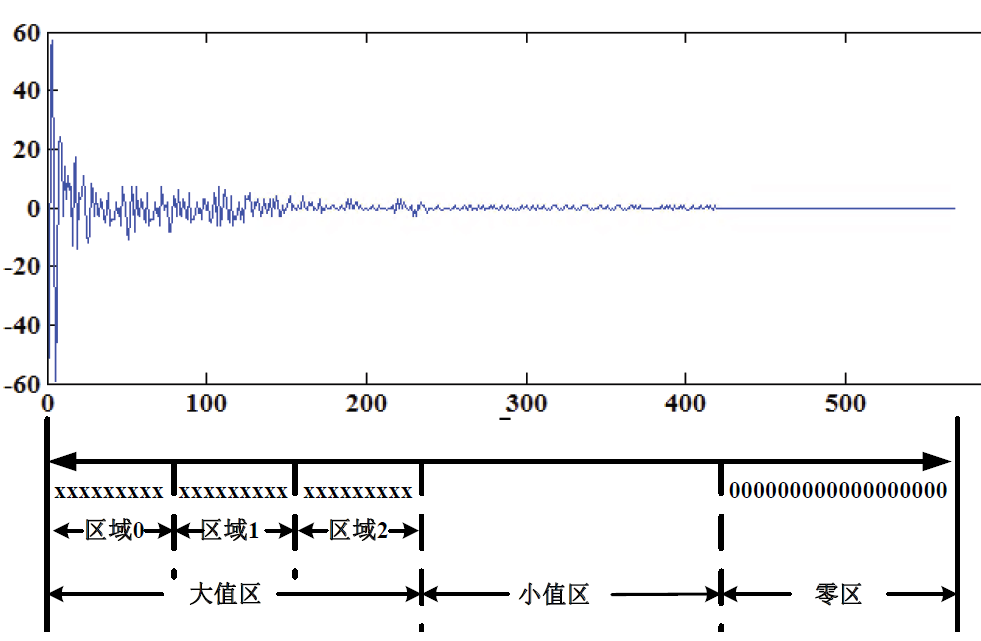


图2-2 颗粒内QMDCT系数区域划分

其中哈夫曼编码适用于无损压缩的熵编码算法，在MP3编码器中使用哈夫曼编码进行熵编码。哈夫曼编码使用变长码字依据源符号可能出现的概率对源符号进行编码，通常以短码子编码大概率出现的源符号，以长码字编码小概率出现的源符号。编码器中使用34个哈夫曼编码表编码QMDCT系数对，其中0~31号码表用于大值区中系数编码，32和33号码表用于小值区中系数的编码。大值区中，每两个QMDCT系数是一个编码单元，编码成一个哈夫曼码字，结构如2-3所示。其中Huffcode为系数编码之后的哈夫曼码字，哈夫曼码字中能编码最大系数值为15，当QMDCT系数大于15时进行截断，QMDCT系数值按照15进行编码，超过15的部分以二进制的形式表示，称之为linbits位。此外，只有16~31号码表中的码字具有linbits位。每一个非零的系数都有一个符号位(sign)来表示其正负。其中0表示正数，1表示负数。如果QMDCT系数为零，则不存在对应的符号位。与大值区不同，小值区中QMDCT系数每四个为一个编码单元，编码成一个码字，结构如图2-4所示。小值区中的QMDCT系数绝对值最大为1，不存在超过15的情况，因此小值区编码时不存在linbits位。与大值区类似的是，只有非零的QMDCT系数存在符号位。

最后，将哈夫曼码字与其他边信息按照MPEG-1标准规定的帧格式组成位比特流，进而生成MP3文件。

2.2.2 STC编码

STC编码是自适应隐写的核心处理环节，能够显著提高隐写的隐蔽性。最优嵌入一般寻求一个整体的优化效果，而STC编码的目标正是形成一个这样的总体优化效果。矩阵编码仅仅在分组上优化，湿纸编码在计算上难以形成这样的效果，相比较，由于STC编码采用了带状矩阵构造校验矩阵，使得能够通过逐步求解动态增减记录状态的方法，完成全局的优化。

在现实算法中实现最小失真嵌入，一个直观的想法就是利用线性提取方程的多解性质，在解空间选择总体失真最小的嵌入方法。典型的，设为二元域上的校验矩阵，原始载体为，相应的隐密载体为，表示载体的LSB序列，表示嵌入的消息，满足提取方程的解集可以描述为

|  |  |
| --- | --- |
|  | (2-1) |

则最小失真嵌入直观上是实现以下嵌入与提取：

|  |  |
| --- | --- |
|  | (2-2) |
|  | (2-3) |

其中，Emb和Ext分别表示嵌入和提取算法。但是，如果基于湿纸编码和矩阵编码，只能在一个载体分组下采取在所有有效嵌入中逐个比较失真的方法，在分组长度加大后计算上是困难的，另外，由于分组最小失真的总和不一定整体最小的。因此，需要一个能在计算上方便的总体失真最小化方案，需要避免对全部情况进行逐个尝试后在评估失真和的枚举方法，希望能够提前排除不够优化的情况。STC的主要特点是采用带状校验矩阵，提取方程的求解可以逐子快进行，这样有利于提取方程的构造。STC校验矩阵有小矩阵

|  |  |
| --- | --- |
|  | (2-4) |

按照对角线方向不断重复，每次重复的方法是，将小矩阵摆放在上一个小矩阵的右侧并向下移动一行，最后形成带状矩阵

|  |  |
| --- | --- |
|  | (2-5) |

如果将*H*视为校验矩阵，*m*为校验子，为了表叔方便以下用*x*和*y*分别表示载体和隐秘载体可修改的位平面，其中元素与*H*中元素属于统一有限域，例如最常用的GF(2)。STC编码可以看做是通过逐步修改x或者逐步构造y使得并满足失真和最小。在逐步构造提取方程是，STC每次通过新加入w个y中元素确定一个消息比特，依次构造以下等式并记录其有效解修改叠加量。

|  |  |
| --- | --- |
|  | (2-6) |

其中，为可能叠加的修改分量，，其中加法是有限域上的操作，以上每行构造的对隐秘载体y的运算关系，实际是约束嵌入方式必须能够支持正确的提取相应的消息元素，这样的修改叠加量是有效的，STC在记录它们的同时，也记录其逐渐累计的失真和，及时删除不可能达到的最小失真的目标的情况记录。

STC具有以下性质：

(1)、若为负载率，则;

(2)、由于*H*每列最多有*h*个非零元素，仅影响*h*个消息比特；

(3)、。

校验矩阵*H*的尺度可以表现为

其中，m即为矩阵的行数，也是子矩阵的重复次数。按照上述规则，对角线最后的局部区域子矩阵没有得到完全复制，但是这并不影响编解码。

2.3 解决的主要问题、技术难点

2.3.1 解决的主要问题

**（1）将自适应隐写引入到音频隐写当中**

目前音频隐写领域发展缓慢，受编码技术和嵌入方案等因素的影响，没有与信息隐藏的最新成果自适应隐写相结合，导致现存的音频隐写在抗隐写分析方面性能较差，安全性负载较低，限制了音频隐写的应用和发展。为了解决音频隐写安全负债率低的问题，基于当前比较流行的音频编码标准，结合当前信息隐藏领域的最新成果，提出了比较合理的音频自适应隐写方案，提高音频隐写的安全负载。

**（2）解决了顺序嵌入造成载体音频失真较大，安全性较差的问题**

传统的音频隐写算法通常采用顺序嵌入的方式，从前向后嵌入秘密信息，顺序嵌入市无法避免的会在音频敏感或者静音帧进行嵌入，给载体音频带来较大的扰动。此外，采用顺序嵌入时，攻击者甚至可以通过分析算法预估出嵌入使用的帧和秘密信息的长度，降低了算法安全性。为了解决这一问题，项目组提出帧选择方案，通过对载体音频进行预处理，选择适合嵌入的帧进行帧内自适应隐写。

2.3.2 技术难点

项目实施过程中，问题在于长消息文件嵌入到多个载体文件、隐写设计和基于lame编码器开发等方面，具体而言，技术难点主要在以下几点：

（1）长消息文件嵌入到多文件的实现：在实际应用中，当需要嵌入较长的消息文件时，单个载体音频可能无法完全嵌入，导致信息提取时消息不完整。因此，需要设计消息协议头，包括消息文件的长度，隐写算法嵌入和提取的相关参数等。在嵌入时先嵌入协议头，在提取过程中参照协议头按顺序提取秘密信息。

（2）隐写设计：在MP3编码过程中，任意修改频域系数会改变帧长度导致编码失败。针对“帧偏移效应”问题，项目组需要设计嵌入方案，保证隐写前后的码流长度不变。除此以外，如何避免在载体音频的敏感帧和静音帧进行嵌入，造成明显的感知失真也是技术难点之一。

（3）基于lame编码器开发：由于音频隐写高度依赖音频编解码系统，项目的相关研发需要建立在对音频编解码系统的深入了解和分析的基础上。编码器是目前最好的MP3编码引擎，具有高质量的编码和全面的MP3技术。因此，项目组需要阅读上万行lame的核心代码，掌握MP3编解码的关键函数和数据结构，结合编码器设计构造失真代价函数。

# 技术方案

3.1技术原理和路线

本项目针对MP3压缩格式音频设计了两种相应的自适应隐写算法，分别是基于等长熵码字替换自适应隐写算法（AHCM）和基于符号位修改的自适应隐写算法（ACS）。这两种隐写算法能够解决MP3隐写的“帧偏移问题”，并且提出适用于音频载体的代价函数构造方法，提高音频隐写算法的安全性和感知透明性。项目组还设计了基于帧选择方案，在信息嵌入之前进行预编码，选择出适合嵌入的音频帧，避免在载体音频的敏感帧和静音帧进行嵌入造成感知失真。除此以外，项目组利用消息协议头实现了长消息文件在多个音频载体中的嵌入。基于相关技术研究成果，研制一套音频自适应隐写软件。最后利用已有的隐写分析算法进行安全性验证。

（1）基于等长熵码字替换自适应隐写算法设计：

为了解决频域系数修改造成的帧偏移现象，提出了基于等长哈夫曼码字替换的MP3自适应隐写算法。该算法对每一帧内相互替换之后不会改变帧长度的码字进行奇偶匹配，以奇偶匹配后的比特向量作为载体进行信息嵌入。算法以码字替换的引起的系数变化幅度作为嵌入操作对载体的扰动值，通过心理声学模型中的绝对静音阈值计算扰动敏感度，结合扰动值和敏感度计算嵌入代价，并且利用STC编码方式自适应地选择最佳嵌入路径，从而有效的提高隐写算法的安全负载。

（2）基于符号位修改的MP3自适应隐写研究

为了避免嵌入操作导致帧长度发生变化，提出了基于符号位修改的MP3自适应隐写算法。对符号位的修改不会导致码字长度发生改变，因此，算法的通过修改频域系数的符号位来嵌入信息，并且通过设置阈值的方式选择可以嵌入秘密信息的系数范围。每一帧可用的频域系数符号位组成比特向量作为载体，将频域系数的修改幅度和心理声学模型相结合设计隐写代价函数，通过STC编码选择最佳的嵌入路径。

（3）帧选择方案设计：

为了解决传统隐写算法在顺序嵌入时在静音帧和敏感帧进行嵌入导致音频感知失真的问题，提出了帧选择方案。在进行信息嵌入前对载体音频进行预编码，计算每一帧的可以嵌入比特数和当前帧的修改代价，选择代价最小的帧最为可用帧。算法正式嵌入过程中，对可用帧按照上述的两种自适应隐写算法进行嵌入，实现帧内自适应隐写。

（4）消息协议头设计：

在实际应用中，当需要嵌入较长的消息文件时，单个载体音频可能无法完全嵌入，导致信息提取时消息不完整。因此，需要设计消息协议头，包括消息文件的长度，隐写算法嵌入和提取的相关参数等。在嵌入时先嵌入协议头，在提取过程中参照协议头按顺序提取秘密信息。协议头的格式如图3-1所示



图3-1 消息头格式

3.2具体实施方案

3.2.1技术方案选择及调整情况

系统的流程图如图3-2所示，首先对载体音频进行预编码，按照帧选择方案选择出适合嵌入的音频帧组成可用帧集合，再将待嵌秘密消息文件利用项目组提出的AHCM自适应隐写算法或者ACS算法嵌入到音可用帧中，实现帧内自适应隐写。在嵌入消息文件之前，先嵌入消息协议头，包括秘密消息长度，采用的隐写算法及参数等信息。信息提取时，首先提取出消息头文件，并根据消息头文件按顺序提取出各个载密音频中的秘密信息，合成完整的消息文件。



图3-2 系统技术路线图

系统遵循计算机软件工程的原则进行开发。根据需求确定技术方案后，做出系统的数据流程图。在软件设计阶段，完成模块的划分、模块间的接口设计以及决定每一模块内部的实现算法。根据需求分析，本系统应具备信息嵌入和信息提取两部分。系统集成多中隐写方法，包括基于等长码字替换的隐写方法和基于符号位修改的隐写方法等。根据每种方法的不同，需要实现不同的子模块。基于码字替换方式的隐写算法需要映射表构造子模块。信息嵌入模块可实现多种参数的嵌入，并支持多种码率的音频隐写。如图3-3所示是音频隐写系统的逻辑框架图。在程序编制阶段，用软件模块实现软件设计阶段确定的算法与方案。在系统测试阶段，对已编制好的程序进行测试以便找出隐藏在软件内部的各种差错，并加以纠正。在系统维护阶段，及时解决开发时期的遗留问题。项目采用C++与C#编程环境开发，其中，C++主要用于开发核心算法模块，C#主要用于编制交互界面。



图3-3 音频隐写系统的逻辑框架图

3.2.2技术实现过程

根据技术路线确定的“基于等长熵码字替换自适应隐写算法设计”、“基于符号位修改的MP3自适应隐写方法”和“帧选择方案”三方面内容，具体技术实现过程如下

**（1）基于等长熵编码字替换的MP3自适应隐写方法：**

该算法以熵编码域为嵌入域，对嵌入失真进行量化，并且采用STC编码实现自适应隐写，能够在嵌入时选择总失真最小的路径进行嵌入。采用STC编码方式进行信息嵌入，减弱了传统哈夫曼码字替换方式带来的码字分布值对效应。由于对小值区修改会造成较大的扰动，因此只在大值区进行嵌入。嵌入操作在MP3编码器的频域系数量化过程和哈夫曼编码过程之间完成，主要流程图如图3-1所示。隐写算法主要分成四个步骤：从哈夫曼码字到二进制比特的映射实现过程，失真函数计算、校验格编码过程和二进制比特至哈夫曼码字的映射过程。首先，原始哈夫曼码字串经过码字至二进制映射过程得到原始二进制串。接着，根据心理声学模型和哈夫曼码字替换距离计算嵌入失真。将秘密信息通过校验格编码STC转换成为载密的哈夫曼码字串。因此，隐写算法的嵌入操作可以归纳为：

|  |  |
| --- | --- |
|  | (3-1) |
|  | (3-2) |

图3-1 基于等长熵码字替换自适应隐写算法流程图

**（2）基于符号位修改的MP3自适应隐写方法：**

在MP3编码过程中，非零的频域系数大于零的时候，符号位用“0”表示；频域系数小于零的时候，符号位用“1”表示。隐写算法的流程如图3-2所示。算法主要分为四个部分，即代价函数构造模块、系数符号位选择模块，信息嵌入模块与系数符号位重写模块。该算法首先对每一颗粒的QMDCT系数向量进行符号位提取,形成符号位比特向量，同时根据心理声学模型设计代价函数,计算每个嵌入位置的失真。然后利用STC编码将待嵌入信息嵌入到原始符号位比特向量中，得到载密符号位比特向量。最后将载密符号位比特向量重新分配给非零QMDCT系数，即可得到载密系数向量。隐写算法可以被模型化为：

|  |  |
| --- | --- |
|  | (3-3) |
|  | (3-4) |

图3-2基于符号位修改的MP3自适应隐写算法流程图

**（3）帧选择方案：**

为了避免采用传统的顺序嵌入的方式，在信息嵌入之前选择一部分可用帧嵌入信息。音频中的每个帧都具有不同的负载，其中一些帧在相同的嵌入容量下更适合进行信息嵌入。因此，在隐写算法中设计了帧级感知失真(Frame-level Preception Distortion,FDP)，以FDP衡量每个帧的嵌入失真，以确定该音频帧是否适合嵌入信息，并且基于FDP实现了最优帧的嵌入路径选择。

3.2.3关键技术与实现

3.2.3.1 基于等长熵码字替换的MP3自适应隐写方法

在MP3编码过程中，会产生大量的频域系数，但是这些频域系数并不是很好的嵌入域。由于MP3是以帧为单位进行编码，每个帧在编码之前会预分配一定大小的空间，编码器通过熵编码将频域系数编码为哈夫曼码字。但是哈夫曼编码是变长编码，直接修改频域系数会导致编码后哈夫曼码字长度发生变化，进而导致码流长度大于预分配的空间，造成了编码失败。而哈夫曼码字是由量化域系数编码而成，数量较多，可以选择等长的码字进行替换，实现信息嵌入。

**（1）码字映射表的构造**

量化的频域系数需要进行哈夫曼编码，在大值区两个量化频域系数编码成一个码字，在小值区四个量化频域系数编码成一个码字。由于哈夫曼编码是变长编码，所以哈夫曼码字之间不能随意替。两个可相互替换的码字需要在码字替换前后保证编码单元的长度与结构不发生变化。令表示第*k*张哈夫曼码表中的第*i*个码字，表示与码字对应的频域系数对。因此，，可相互替换的两个码字对和必须满足以下三个条件：

1）哈夫曼码字长度。哈夫曼码字和的码字长度相等，

|  |  |
| --- | --- |
|  | (3-5) |

2）系数符号位个数相等。频域系数对和有相同的符号位个数，

|  |  |
| --- | --- |
|  | (3-6) |

3）Linbits位标志。频域系数linbits位的存在性和一致，同样的和也要满足此条件。

|  |  |
| --- | --- |
|  | (3-7) |

哈夫曼码字相互替换之后，其对应的频域系数也随之发生变化。为了使码字替换对频域系数变化造成的影响尽可能变低，在进行可替换码字搜索时，对搜索空间采用zig-zag的方式遍历。映射表的具体构造方式吐下：

集合包含第*k*张码表中所有的码字，被分为两个子集：和。集合中的码字都是可用码字，被用来嵌入信息，而集合中包含的都是不可以进行隐写的哈夫曼码字。其中，和是通过迭代生成的。被初始化为，对于，如果满足限定条件(3-5)至(3-7)，就将和放入，否则的话将和放入。重复上述过程，直到。

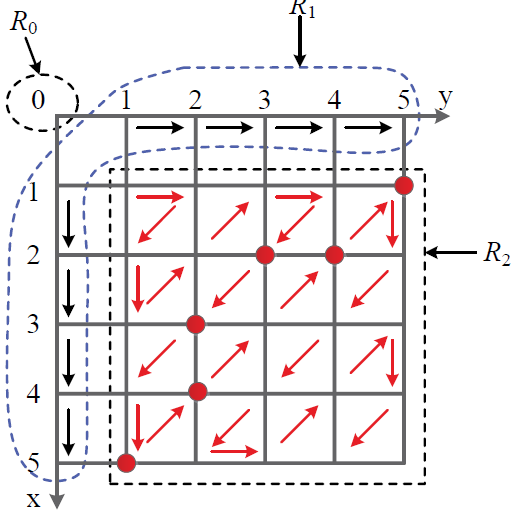


图3-3 7号码表的Zigzag搜索

可用码字空间中的每个哈夫曼码字按照其被放入的顺序进行编号。将划分为两个子空间，和。当哈夫曼码字被放入的序号是奇数，则将放入，否则的话将放入。集合中的哈夫曼码字表示比特‘0’，相反的，集合中的哈夫曼码字表示比特‘1’。根据码字长度的分布特征，两个可相互替换的码字，在以zig-zag顺序进行搜索时距离更近，即曼哈顿距离更小。以第7号码表为例，其搜索顺序如图3-3所示，根据公式3-6，量化的频域系数被划分为和三个区域。这三个区域互相独立，各自执行上述迭代搜索的过程。图中主要表述区域的搜索过程，所搜顺序以图中箭头方向表示，以实心点标注的哈夫曼码字分别是、、、、、，这六个哈夫曼码字的长度等于8。根据搜索顺序，将这六个哈夫曼码字组成三个哈夫曼码字对：，，。、和被划分入，、和被划分入。因此，哈夫曼码字到二进制比特的映射可以公式化为：

|  |  |
| --- | --- |
|  | (3-8) |

类似的，从二进制比特向哈夫曼码字映射的过程：

|  |  |
| --- | --- |
|  | (3-9) |

其中，是一个可相互替换的码字映射对。

**（2）隐写代价函数设计**

通过哈夫曼码字替换进行信息嵌入会导致音频频域系数发生改变，带来感知或统计上的失真。假定由码字替换带来的失真是相互独立的， 隐写操作的总失真为：

|  |  |
| --- | --- |
|  | (3-10) |

其中，是有互相替换造成的失真，*n*是在嵌入操作中被替换的哈夫曼字的总数。

心理声学模型在音频压缩编码算法中起核心作用，这一模块模仿人类听觉感知灵敏系统生成了一种时间自适应的频谱模式。MP3 音频编码器通过移除感知无关的组件和数据达到数据压缩的目的。这一功能是利用了人耳听觉的掩蔽效应实现的。心理声学模块通过分析音频信号，计算信掩比。音频信号成分的掩蔽特性依赖于此成分在频域所处的位置以及频线幅值。音频编码器会估计每个子带的掩蔽阈值，在此阈值之下的音频信号人耳无法感知到。编码器根据每个子带的掩蔽阈值决定音频信号使用多少比特表示既能节省空间又能保持较高的音质。另外，编码器会在心理声学模块计算音频的感知熵，感知熵用来决定窗口类型的转换。子带划分、临界频带、信掩比、感知熵和绝对静音曲线等都是心理声学模型在音频压缩编码中重要的特性。合理利用这些性质可以有效移除音频信号中感知无关的成分，在保证音频高音质的前提下实现音频压缩。算法中，代价函数设计过程使用心理声学模型中的绝对静音阈值衡量人耳对每个频带的敏感度。

人耳可感知的音频范围主要是20Hz 至20KHz 之间，低于这个范围或高于这个范围的音频信号一般很难被人耳捕获感知到。在此频率范围内的信号，人耳对每个频率的感知敏感度也是不同的。一般来说，人耳最敏感的频率范围为3KHz-4KHz 之间，在高频或者低频部分人耳对音频的感知敏感度将会降低。绝对静音阈值曲线可以衡量人耳对音频的感知敏感度。绝对静音阈值是通过大量实验得到的结果，能反应绝大多数人对音频的感知，它描述的是在一个安静的环境中，人耳在不同的频率范围一个纯音需要多少能量值才能被人耳感知到。人耳绝对静音阈值曲线与频率值*f*的关系可以用公式3-11表述：

|  |  |
| --- | --- |
|  | (3-11) |

在信息嵌入操作中，哈夫曼码字替换会造成码字解码得到的频域系数对发生相应的改变。如图3.4所示，哈夫曼码字 经过隐写操作被替换为，相应的，频域系数对变为。信息嵌入对载体造成的失真主要受两个方面的影响，其一是哈夫曼码字替换造成的频域系数的变化幅度，主要取决于码字映射表的构造；其二是受心理声学模型的影响，即人耳对发生改变的频域系数的敏感度，主要取决于频域系数在频谱中的位置。频域系数对的距离作为衡量指标，曼哈顿距离可以有效计算两个频域系数对之间的距离。以为例，信息嵌入之后系数对变为，两个系数对之间的差 计算方法如下：

|  |  |
| --- | --- |
|  | (3-12) |

其中，表示表示哈夫曼码字替换之后频域系数对的修改幅度，同时，是嵌入失真产生的

根本原因。

人耳对不同频段的音频敏感度不同。在人耳较敏感的频段嵌入信息，轻微的修改就可能导致较大的感知失真，而在高频或者低频等人耳不敏感的区域，嵌入操作对音频感知带来的影响将微乎其微。因此，嵌入操作修改的频域系数在频谱中所在的位置也将对隐写失真带来较大的影响。绝对静音阈值可以衡量在安静的环境下，人耳感知到纯音所需要的最小能量，同时也可以作为人耳对不同频段音频的感知灵敏度。不同的频域系数，对应频谱上不同的频率。在编码过程中，窗口类型为短窗的时候，会出现频线重叠的情况，除此之外，频域系数和频谱上的频率值可一一对应。统计表明，MP3 编码过程中，90% 以上的窗口都不是短窗，因此，可以近似认为频域系数是从频率值从低到高排列的。综合上述分析，修改代价函数定义如下：

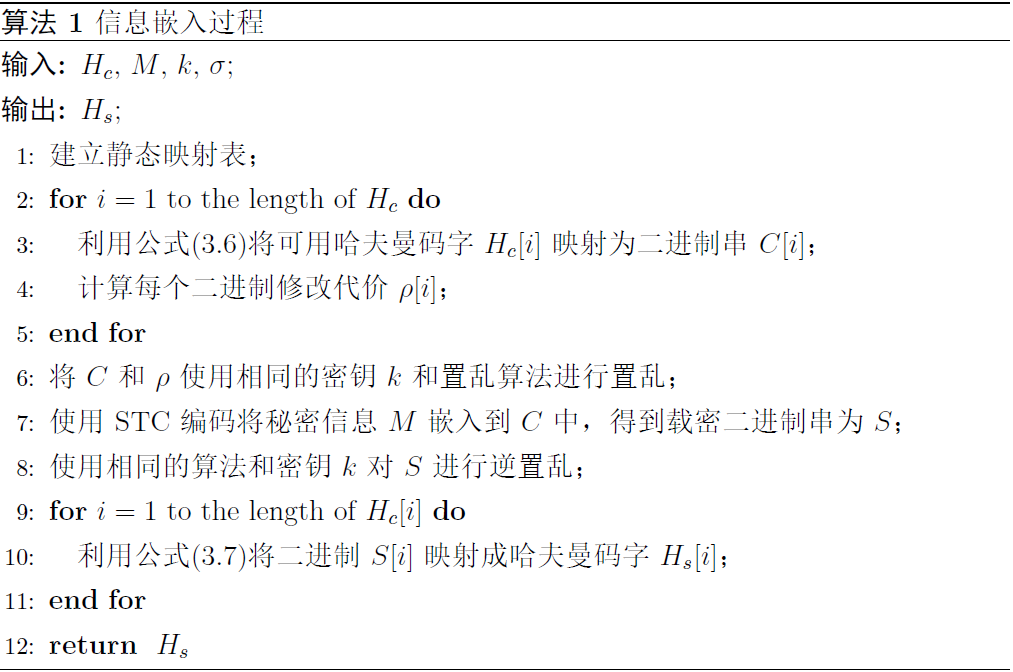
|  |  |
| --- | --- |
|  | (3-13) |

其中，是哈夫曼码字在整个码字串中的索引值；表示第2i根频线处的听觉阈值，即在第2i根频线处的取值；为常数，用来确保的值大于1，而 取对数操作是为了减少一些极端值的影响。

**（3）信息嵌入和提取的过程**

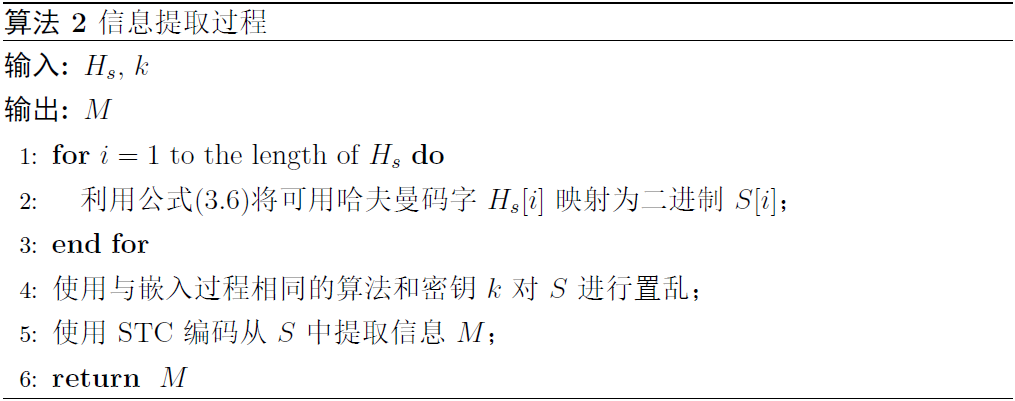
**信息嵌入过程：**

本章提出的隐写算法嵌入操作在MP3编码器频域系数量化模块和哈夫曼编码模块之间。信息嵌入具体流程如下：首先，原始的哈夫曼码字串根据公式3-8转换成二进制比特串C，根据公式3-13计算载体的修改代价。其次，将二进制串C和隐写代价以相同的置乱函数和密钥进行置乱，置乱的目的是为了让修改代价小的嵌入点能够均匀分布在载体中。使用STC编码将秘密信息比特M嵌入到二进制比特串C 中，得到载密的二进制比特串S。将S以相同的置乱函数和密钥进行逆置乱，逆置乱的目的是能够使二进制比特正确的逆映射成哈夫曼码字。根据公式3-9将逆置乱后的二进制比特串映射为载密哈夫曼码字，此过程需要使用原始哈夫曼码字串。信息嵌入操作的伪代码如算法1描述。



**信息提取过程：**

本章提出的算法其信息提取操作在哈夫曼解码与反量化之间。首先，读取每一帧中载密哈夫曼码字，根据公式3-8将其转换成载密的二进制比特串S。其次，利用与嵌入模块相同的置乱算法与置乱密钥将S 进行置乱。利用STC 编码从S中提取信息M。信息提取模块的伪代码如算法2所示。



3.2.3.2 基于符号位修改的MP3自适应隐写算法设计

在MP3编码过程中,编码器会为每一帧分配一定数目的可用空间。如果实际编码后帧长度大于预分配的空间，会导致编码器出现编码错误。Huffman编码是一种变长熵编，不同系数编码后的Huffman码字长度不固定。因此,通过修改QMDCT系数的绝对值实现信息嵌入往往会导致帧长度发生改变，造成编码错误.为保证嵌入操作的正确执行，帧长度在信息嵌入前后需要保持一致。项目组通过分析MP3编解码过程，提出了一种基于QMDCT系数符号位修改的自适应隐写算法(Adaptive Coefficient Sign, ACS).该算法首先对每一颗粒的QMDCT系数向量进行符号位提取，形成符号位比特向量.同时根据心理声学模型设计代价函数，计算每个嵌入位置的失真。然后利用STCs编码将待嵌入信息嵌入到原始符号位比特向量中，得到载密符号位比特向量。最后将载密符号位比特向量重新分配给非零QMDCT系数，即可得到载密系数向量。

**（1）符号位选择**

每个颗粒包含576个QMDCT系数，大值区和小值区的系数都需要进行哈夫曼编码， 由于零区系数全部为零，所以不需要编码。在编码过程中，用“0”或“1”表示每个非零系数的符号位。嵌入操作需要改变QMDCT系数的符号位，而符号位的改变其本质是QMDCT系数值的改变。对于绝对值较大的QMDCT系数，改变其符号位造成的频域系数变化较大，往往会引起较严重的感知失真。因此，算法中通过设置阈值的方式，控制嵌入时选用的QMDCT系数的范围。表1列出在不同阈值下符合条件的系数比例。

表1 不同阈值可用系数比例

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | *T*=1 | *T*=2 | *T*=3 | *T*=4 |
| 128kbps | 6.4% | 14.6% | 17.2% | 18.4% |
| 320kbps | 7.8% | 17.5% | 20.5% | 22.9% |

对于每个颗粒，从大值区开始按照顺序遍历QMDCT系数，符号位用表示。如公式3-14所示，如果值大于零且小于等于，系数符号位为0，令；如果值小于零且大于等于，系数符号位为1，令；否则此系数符号位不可用，跳过此系数继续遍历下一个系数。最后将大值区与小值区的符号位进行拼接，得到只包含“0”和“1”的向量，以此向量作为秘密信息嵌入的载体。

|  |  |
| --- | --- |
|  | (3-14) |

秘密信息嵌入完成后，得到载密的二进制向量,需要将中的载密符号位重新分配给QMDCT系数,表示分配后的QMDCT系数.从大值区开始,依次从载密向量中取出1比特,如果等于0,当前系数不为零且绝对值小于等于,则将符号位设置为正；如果等于1,当前系数不为零且绝对值小于等于,则将符号位设置为负.

|  |  |
| --- | --- |
|  | (3-15) |

**（2）代价函数设计**

隐写算法在嵌入过程中,修改了QMDCT系数的符号位，其本质上是改变了QMDCT系数值,会造成音频一定程度的失真。因此,构造合理的代价函数是十分有必要的。

MP3音频失真主要受两个因素影响：QMDCT系数的修改幅度和心理声学模型。人耳可听到的频带范围通常为20Hz到20KHz之间。但是，人耳对不同的频带具有不同的敏感度。由大量实验得到的绝对听觉阈值描述了在静音环境中，一个纯音被人耳听见需要具备的能量。因此，可以用绝对听觉阈值曲线反应人耳对各个频带音频的敏感度。绝对听觉阈值曲线可以用公式3-13描述。如果需要修改QMDCT系数的符号位,的值将会变为原来值的相反数,用表示系数值的修改幅度,则有

|  |  |
| --- | --- |
|  | (3-16) |

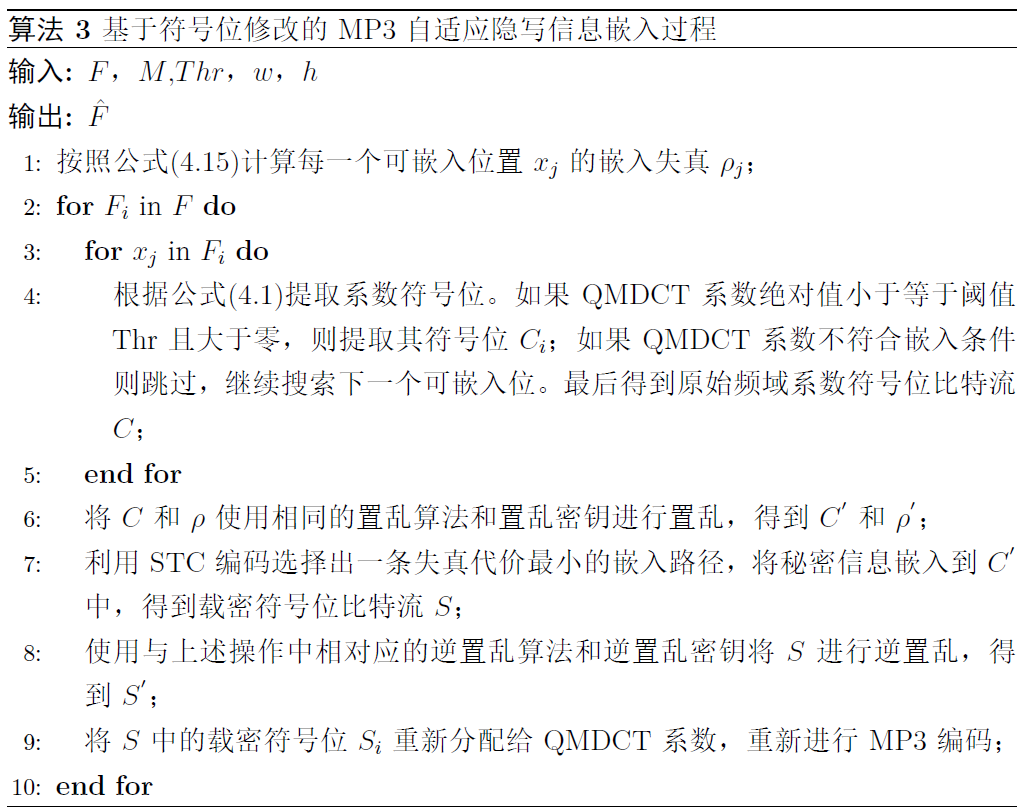
通过上述分析,代价函数可以定义为：

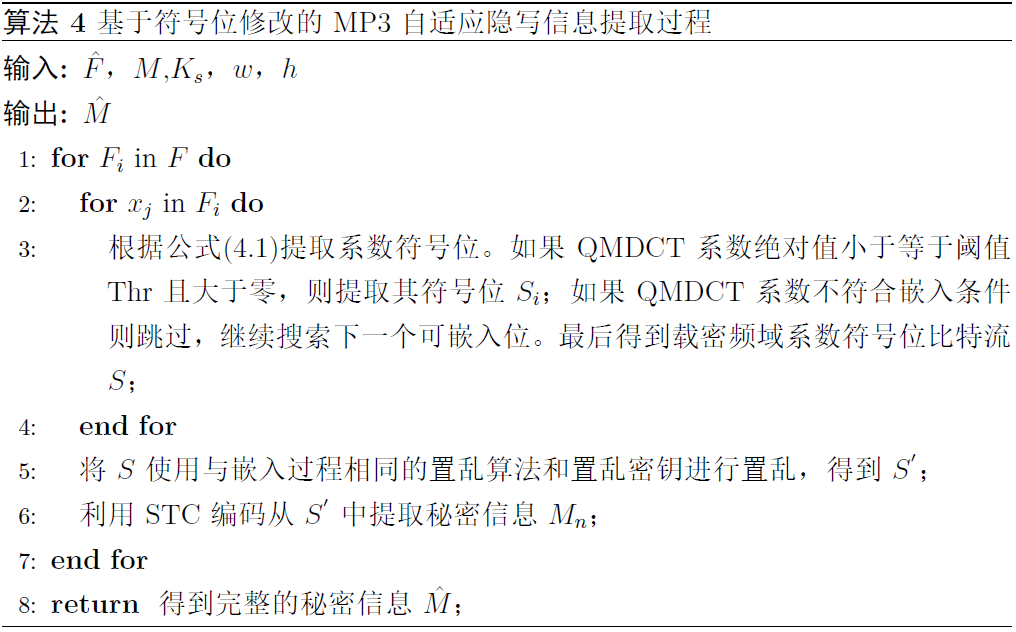
|  |  |
| --- | --- |
|  | (3-17) |

其中，是符号位被修改的QMDCT系数的在当前颗粒中的索引值，表示第个频线处的绝对听觉阈值，即为第个频线时对应的取值；是常数以确保大于1；对数运算起平滑作用，减小一些极端值的影响。

**（3）嵌入过程和提取过程**

隐写算法由嵌入算法和提取算法两个部分组成。在嵌入算法中，首先根据公式(2)按顺序提取大值区和小值区符合条件的QMDCT系数的符号位作为载体；其次，结合失真代价函数和秘密信息比特向量，利用STCs选择一条失真最小的嵌入路径，通过修改QMDCT系数的符号位完成秘密信息的嵌入。提取秘密信息时，搜索大值区和小值区的所有非零且绝对值小于等于的QMDCT系数，按照嵌入规则提取QMDCT系数的符号位得到载密二进制比特向量。具体嵌入和提取过程如算法3和算法4所示。





3.2.3.3 帧选择方案设计

双层自适应隐写算法主要包含帧间自适应和帧内自适应。帧间自适应主要根据帧级感知失真FPD与每帧的嵌入容量选择最优嵌入帧路径，使得整个音频的总失真最小；帧内自适应主要依据嵌入操作的原理计算每个修改点的嵌入失真，利用STC编码实现帧内最优嵌入路径的选择。帧选择方案主要进行代价函数的设计，即帧级感知失真，并根据帧级感知失真实现嵌入帧选择。

音频中的每个帧都具有不同的负载，有些帧更适合嵌入信息，在相同的嵌入容量下更难以被检测。因此，在本章中定义了FPD衡量每帧嵌入信息时的失真，以此确定音频帧是否适合嵌入信息，并且基于FPD实现了最优帧嵌入路径选择。从隐写分析的角度看，当嵌入操作对载体的修改越集中，隐写算法的不可检测性越高。根据payload-limited sender (PLS) 模型，优先选择负载能力高的帧能够提高帧间修改的聚合度，使嵌入修改更集中。因此，第帧的帧级感知失真如公式3-18，它用来计算每一帧内修改位置的聚合程度。

|  |  |
| --- | --- |
|  | (3-18) |

其中，分母表示帧对应的载体比特串的长度，是调节系数，计算方式如公式3-19所示。正常情况下，可被看做是一个常数，当FPD值非常接近的时候，使用公式3-19进行计算。

|  |  |
| --- | --- |
|  | (3-19) |

其中，是计数函数。如公式3-19所示，表示在帧中，可隐写码字占总码字个数的比例。

公式3-18的目的是寻找合适的帧间嵌入路径使得整个音频的总嵌入失真，FDP最小。这一过程可用公式3-20来表示。

|  |  |
| --- | --- |
|  | (3-20) |

在(5.14)中，是一个关于嵌入路径的滤波函数，定义如公式3-21；是帧的负载大小；是待嵌信息的大小。

|  |  |
| --- | --- |
|  | (3-20) |

如图3-4所示，嵌入帧路径选择算法主要包含两个步骤：(1) 原始音频帧序列为，首先计算每一帧的FPD，并且将音频帧按照FPD从小到大的顺序进行排序，假设排序结果为。(2) 按照排序结果进行帧遍历，将每一帧的嵌入容量进行累加，直到容量的累加和不小于待嵌信息的长度或者已经遍历了所有帧。在图3-4中，因为最小，所以作为起始帧；因为并且所以 作为结束帧；箭头方向指示帧的遍历顺序。因此，最终的嵌入路径从起始帧到结束帧是。由于MP3 编码器按顺序逐帧编码，所以在信息嵌入时无法按照顺序进行。选定的嵌入帧都需要嵌入信息，可以

按照编码顺序在选定的帧中嵌入信息，即实际嵌入帧顺序为。

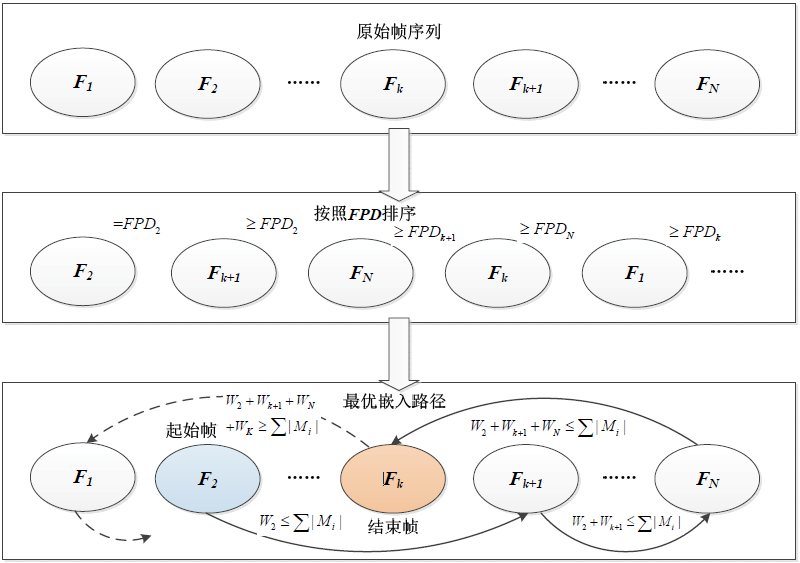


图3-4 帧选择流程

3.3与已有成果的比较

（具体说明本成果在原成果基础上进行了哪些转化与改进）

# 技术特点、创新性及达到的指标

4.1技术特点

项目开展了基于MP3的自适应隐写技术研究，实现了两种基于MP3的自适应隐写方法。基于研究成果，开发了“ES05音频自适应隐写系统”软件一套。其操作简单，功能强大，安全性较高。主要技术特点包括以下方面：

**（1）通过协议头实现了长消息文件嵌入到多文件**

在信息嵌入之前，县嵌入协议头，协议头自第一帧开始按照顺序进行嵌入，知道完全嵌入到载体音频中。消息协议头包括消息文件的长度、STC编码参数、帧选择方案、嵌入域的选择、文件索引等。在提取过程中先提取协议头，参照协议头中信息按顺序提取秘密信息。

**（2）采用了加性模型下的自适应隐写**

在限定负载率下，加性模型的自适应隐写基于STC比那吗最小化各个样点上的失真和，主要包括了失真函数的设计和STC编码两个环节。项目组结合心理声学模型中绝对静音阈值和对频域系数的修改幅度构造了失真函数。基于输入的参数与每个样点的失真度量，进行STC编码，其中输入参数中的小矩阵宽度决定了预设的负载率。

**（3）具有良好安全性和较高隐写容量的隐写方案**

项目组设计了两种帧内自适应隐写方法，基于等长熵码字码字替换的MP3自适应隐写方法和基于符号位修改的MP3隐写方法。这两种方法分别以哈夫曼码字和频域系数符号位作为嵌入域进行修改，具有很大的隐写空间。并且两种隐写方法均采用了STC编码方式嵌入秘密信息，使隐写嵌入的失真最小化，提高了安全性。同时，项目组还设计帧选择方案，构造了帧间代价函数，避免了在敏感帧和静音帧嵌入信息，实现了双层自适应隐写。

4.2创新性

与国内外同类技术相比，本项目具有以下几点创新：

（1）**将自适应隐写引入到音频隐写当中**

由于音频编码技术的限制，隐写领域的最新成果自适应隐写技术在音频隐写领域发展缓慢，STC编码很难直接应用到压缩域音频，从而使得算法的抗隐写分析性能较低，限制了隐写算法的实用性。针对这种情况，项目组基于当前比较流行的音频编码标准，结合心理声学模型设计代价函数，应用STC进行消息嵌入，实现了基于MP3音频格式的自适应隐写方法，显著地提高了音频隐写的安全负载，使其更具有实用性。

**（2）提出了帧选择方案，实现了双层自适应隐写**

传统的音频隐写通常采用顺序嵌入的方式，从前往后嵌入秘密信息。顺序嵌入时无法避免在音频敏感帧或者静音帧嵌入，给载体带了较大的扰动。此外，采用顺序嵌入时，攻击者甚至可以通过分析算法预估出使用的帧和秘密信息的长度，降低了算法的安全性。为了解决这一问题，项目组提出了帧选择方案，通过帧间代价函数，计算嵌入时的帧间感知失真，并且对所有的帧按照帧间代价从小到大排序，选择代价小的帧作为可用帧。隐写操作通过上述的基于等长熵码字替换的隐写方法和基于符号位修改的隐写方法实现，提高了隐写算法的安全负载，实现了双层自适应隐写。

**（3）结合心理声学模型进行代价函数设计**

人耳对不同频段的音频敏感度不同。在人耳敏感的频段嵌入信息，轻微的修改就可能造成较大的感知失真，而在高频或者低频区等人耳不敏感区域，嵌入操作对音频感知带来的影响微乎其微。因此，嵌入操作的频域系数在频谱中所在的位置也将对隐写失真带来较大的影响。项目组结合心理声学模型中的绝对静音阈值构造了代价函数，降低了嵌入操作带来的感知失真。

4.3 总体性能及指标

4.3.1 总体性能

4.3.2 技术指标

# 总结

5.1研制过程的经验与教训

与一般项目开发相比，本隐写系统需要设计隐写方案和构造代价函数，而且系统开发规模相对较大，隐写模块实现较为复杂。在开发过程中遇到一些挑战，并且在合同规定日期内完成，通过所有的功能测试。从一定意义上来讲，项目的开发是取得了一定的成功的。

**（1）经验**

每周组会：在项目实施过程中，每周周四下午开发小组都要参加一个两个小时左右的会议，由项目负责人主持，听取每个成员的进度，并根据进展情况，对于进度和资源进行调整。

交叉审核：每天下班前，2人一组，对对方的代码进行Review，发现问题及时解决。代码Review的时候，语法与规则的检查，通过Check Style的工具进行；开发人员将审查的重点放在功能实现与性能优化等方面。

注重测试：完成一个功能之后，先对它进行测试。测试是够能够正常执行。先进行部分模块测试可以节省时间。通常说来，我们在整合不同的模块时也会出现问题，例如模块之间的接口不匹配。但是如果我们能够信任各个组件的话，那么跟踪集成问题就会变得简单得多。

分析与设计：由一名开发人员进行系统框架的设计，其它人员进行审核；在系统框架设计进行过程中，由于系统去除订单处理以外的其它部分比较独立，因此，将其它模块分配给开发人员，而将核心部分交与技术经理进行分析与设计。开发人员在每个迭代周期内，都会在分析与设计做完后，每2人一组进行审核。

**（2）教训**

明确成员任务：在项目开发时，明确每个项目组成员的具体任务和完成时间，定期交流完成情况，共同解决遇到问题，分享经验。这样能够提高开发效率。

注重备份：在项目开发过程中，要求小组成员每日将自己的工作成果备份到U盘或者上传至云端，避免硬件故障造成工作成果丢失。

项目阶段审核：在每个模块的开发过程中，应注意在完成全部功能前，督促模块负责人根据阶段完成的情况及时进行阶段审核讨论，发现问题并改正。

5.2技术成熟程度，推广应用的条件和前景

**（1）技术成熟度**

20世纪90年代，随着数字通信的极大发展，信息隐藏技术也随之迅速发展。国际很多知名机构如麻省理工学院，美国新泽西理工大学都在信息隐藏领域进行了深入研究。国内很多科研机构如中国科学院信息工程研究所，中山大学，武汉大学和解放军信息工程大学都在信息隐藏领域张开了深入研究，并取得了丰硕的科研成果。

其中音频隐写作为信息隐藏技术的重要分支也成为了国内外学者重点研究对象之一。历经了时域隐写，到变换域隐写，最后到压缩域隐写，音频隐写方法也越来越成熟。2009年Fridrich提出了自适应隐写，结合STC编码，能够最小化嵌入操作对载体造成的失真。这种自适应隐写方法已经在图像上得到了成熟的发展和应用。项目组将自适应隐写方法应用到音频领域，解决音频编码器对STC编码的限制，并结合心理声学模型和系数修改幅度构造了代价函数，有效的提高了安全负载，实验结果表明，在128kbps码率下，相对负载为0.25的情况下，使用隐写分析方法检测准确率低至55%。

**（2）推广应用的条件和前景**

因为电子通信容易受到监听和恶意干扰，安全和隐私问题在今天比以往更容易受到关注。传统得解决方案是基于密码学的，但是一旦加密信息被截获，尽管加密的内容受到了保护，但是正在进行的秘密通信的事实的显然的。因此，为了保证通信的完整性，避免引起注意是十分重要的，因此需要利用隐写术对秘密信息实现隐蔽通信，在第三方不察觉的情况完成通信。目前隐写术主要应用在国防安全、军事通信领域，在其他进行需要敏感数据传输的领域也具有十分重要的实用价值。

音频作为常见的多媒体形式，应用十分广泛。其中，大多数的音频以MP3的格式存在，这为了基于MP3的隐蔽通信提供了良好的信道。首先，载体音频容易获得。互联网上的MP3音频为隐写提供了大量的载体。其次，大数据掩蔽效应。MP3是目前使用最广泛的音频格式，以MP3音频作为载体不会引起太大关注，检测者很难对所有的MP3文件进行检测。

但是目前音频隐技术手编码技术和嵌入方案等因素的影响，还没有与当前信息隐藏领域最新成果自适应隐写相结合，导致现存的音频隐写方法安全性较差，实用性较低。项目组首次提出了音频自使用隐写方法，提高了音频隐写的安全负载，具有广阔的应用前景。

5.3存在的问题及后续工作展望

MP3自适应隐写代价研究。目前，文中提到的MP3自适应隐写算法，载体修改代价构造比较单一，只考虑心理声学模型的影响或者只考虑了音频的统计特性。隐写算法需要考虑算法的不可感知性与抗检测能力。以心理声学模型为基础构造的代价函数能够提高隐写算法的不可感知性；以音频的统计特性为基础的代价函数能够提高隐写算法抗检测能力。下一步工作可以将两者相结合，对两种模型设置不同的权重值，计算隐写操作的修改代价，提高隐写算法的安全性。