音频信息隐藏与水印算法

雷敏

北京邮电大学网络空间安全学院

leimin@bupt.edu.cn

鲁棒性

在实际水印算法鲁棒性评价应用中，常用水印的误码率(BER)来衡量水印抵抗攻击能力，即在各种攻击后提取得到的水印与原始水印之间不同比特数所占的百分比。BER的定义如下：

$$BER = \frac{\text{错误的比特数}}{\text{总比特数}} \times 100\%$$

如果含水印音频未经过任何音频信号处理的攻击，提取出来的水印图像和原始图像的误码率为0；当含水印信息的隐写载体在传输过程中经过一些信号处理，提取的水印图像和原始水印图像之间的误码率会增加。当含水印信息的音频经过某种信号处理后提取的水印图像和原始水印图像之间的误码率越低，表示该算法抵抗该种音频信号处理能力的鲁棒性越强。

归一化系数

如果在音频信号中嵌入的水印信息为二值图像，可采用归一化相关系数（NC）来判断提取水印图像和和原始水印图像的相似性作为评价标准，其定义为：

$$NC(W,W') = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i,j)^2} \times \sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W'(i,j)^2}}$$

其中：W为原始水印，W'为提取的水印。

如果含水印音频未经过任何音频信号处理的攻击，提取出来的水印图像和原始图像的归一化系数一般都为1.0；当含水印信息的隐写载体在传输过程中经过一些信号处理后，提取的水印图像和原始水印图像之间的归一化的系数会下降。当含水印信息的音频经过某种信号处理后提取的水印图像和原始水印图像之间的归一化系数越大，表明该算法抵抗该种音频信号处理能力的鲁棒性越强。

音频数字水印的应用

（1）版权保护

将版权所有者的信息，嵌入在要保护的数字多媒体作品中，然后公开发布水印版本作品。当该作品出现版权纠纷时，可以从含水印载体中提取嵌入的版权信息，从而防止其他团体对该作品宣称拥有版权。即数字作品的所有者可生成一个水印，并将其嵌入原始音频，然后公开发布水印版本作品。对此种应用领域来说，信息隐藏算法必须有较好的鲁棒性，因为盗版者一定会对这些数字作品进行攻击。目前已经有许多用于版权保护的音频水印算法。

音频数字水印的应用

（2）盗版追踪

为避免未经授权的拷贝制作和发行，作品发布人可以将不同购买者的独一无二的数字指纹信息嵌入作品的合法拷贝中。当某一个作品出售给卖家时，出售者不仅要在作品中嵌入版权所有者信息，而且还嵌入了购买者信息，当市场一旦发现未经授权的拷贝，可以通过某种算法提取数字作品中嵌入的指纹信息，可以根据此拷贝中恢复出的指纹来确定盗版的来源，也就是知道是哪个用户泄露的拷贝。在此类应用中，水印必须是不可见的，而且能抵抗恶意的擦除、伪造以及合谋攻击等。例如，游戏制作公司可在分发给测试者使用的测试版本游戏的图像中加入水印用以警告和跟踪泄密的游戏测试者。

音频数字水印的应用

（3）使用控制

在数字化信息中嵌入特定的控制信息，只有满足条件的使用者才能访问(如播放或拷贝)含有水印的数据。水印与作品的使用工具相结合（如软硬件播放器等），使得盗版的作品无法使用。比较典型的例子是iTunes上的音乐仅仅能够在iPod上播放。又如，在一个封闭式或私有的电视点播系统中，可以把电影分级信息嵌入到电影的音频中，从而实现电影的分级播放控制。

音频数字水印的应用

(4) 完整性鉴定

当音频在某些特殊场合使用时，经常需要确定它们的内容是否被修改、篡改或经过特殊处理。数据完整性鉴定是指对某一对象完整性和真实性进行判定，也经常称为“认证”或者“篡改提示”，主要是确认该对象在传输或存储过程中并没有被篡改、破坏或丢失。利用数字水印来进行认证和完整性校验的优点在于，认证同内容是密不可分的。在实际应用中，这类水印对特定的修改(如常用MP3压缩操作)可以具有一定的稳健性，而对于恶意篡改具有脆弱性(俗称半脆弱水印)。当对插入了水印的数字内容进行检验时，对提取出水印的完整性来验证数字内容的完整性。

音频数字水印的应用

（5）注释

将作品的标题、注释等内容以秘密信息的形式嵌入该作品中，用于解释这些作品。如：在音乐中隐藏该乐曲的简介、作者简介等；这种方式可以抵抗常规的信号处理或操作，不需要额外的带宽，且标注信息不易丢失。

音频数字水印的应用

（6）广播监控

在商家委托广告制作商，制作符合要求的广告视频，在广告视频制作完成，交与广告播出商（电视台等）之前，将预先经过特殊处理的数字水印信息嵌入广告中。嵌入水印信息以后，一个自动监测系统能判断广告是否如合约履行。可以监控广告是否在要求的时间进行了播出；在该时段播出的广告内容，是否是要求的广告；播出的广告时间长度是否符合要求等等；广播监测系统能监视所有频道，并能根据发现指证电视台的违反合约行为。音频水印也可隐藏到实时演奏的音乐中。技术上可以将各不相同的数字水印嵌入到各个音乐片段中，并设立一个自动监控的接收站，用以接收监控电台播放的影片或声音等媒体，并自动在媒体中搜寻这个唯一的数字水印，这样便可以确切知道这些媒体被播放的时间、次数等相关信息。

隐藏算法分类方法

- 根据载体分类
  - 图像、语音、视频、文本、协议等等中的信息隐藏
- 根据隐藏算法分类
  - 文件格式法
  - 时域算法
  - 变换域算法
  - 扩频算法
  - 统计方法

音频信息隐藏技术

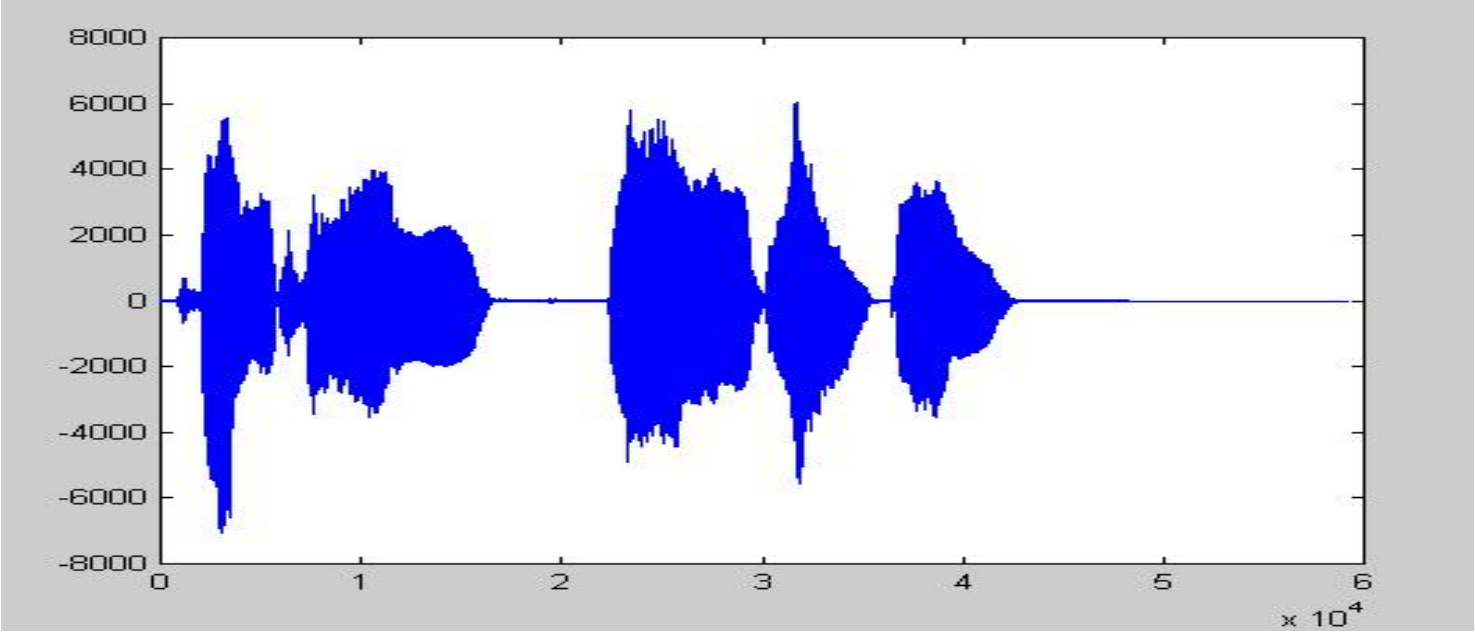
- 音频信号的特点
  - 一维信号
  - 人耳听觉系统（HAS）比人眼视觉系统（HVS）灵敏得多
- 对音频信息隐藏技术的要求
  - 透明性
  - 鲁棒性（强鲁棒，抗模数转换）
  - 同步要求
  - 盲检测

时间域音频算法

- 最低有效位方法
  - LSB(Lease Significant Bit)
- 回声隐藏法

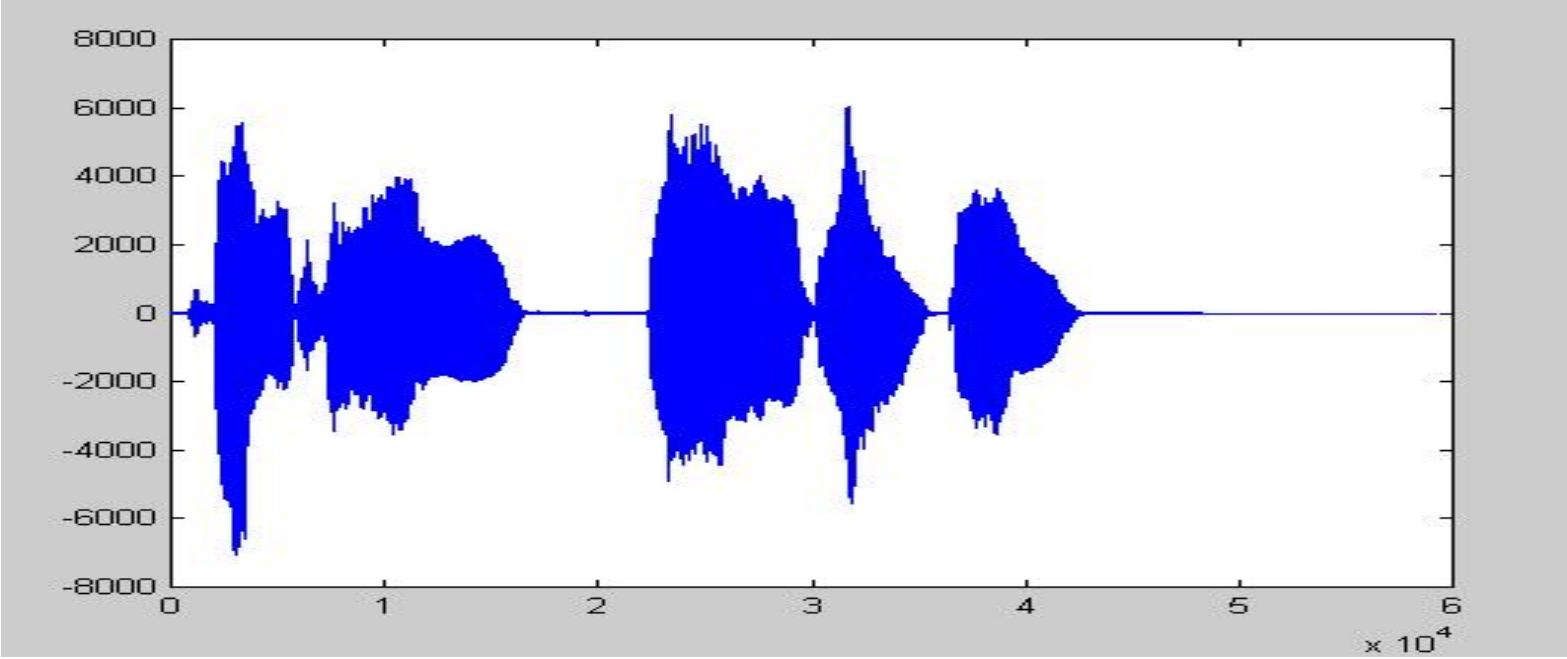
LSB原理

- 原始语音信号（“床前明月光”）



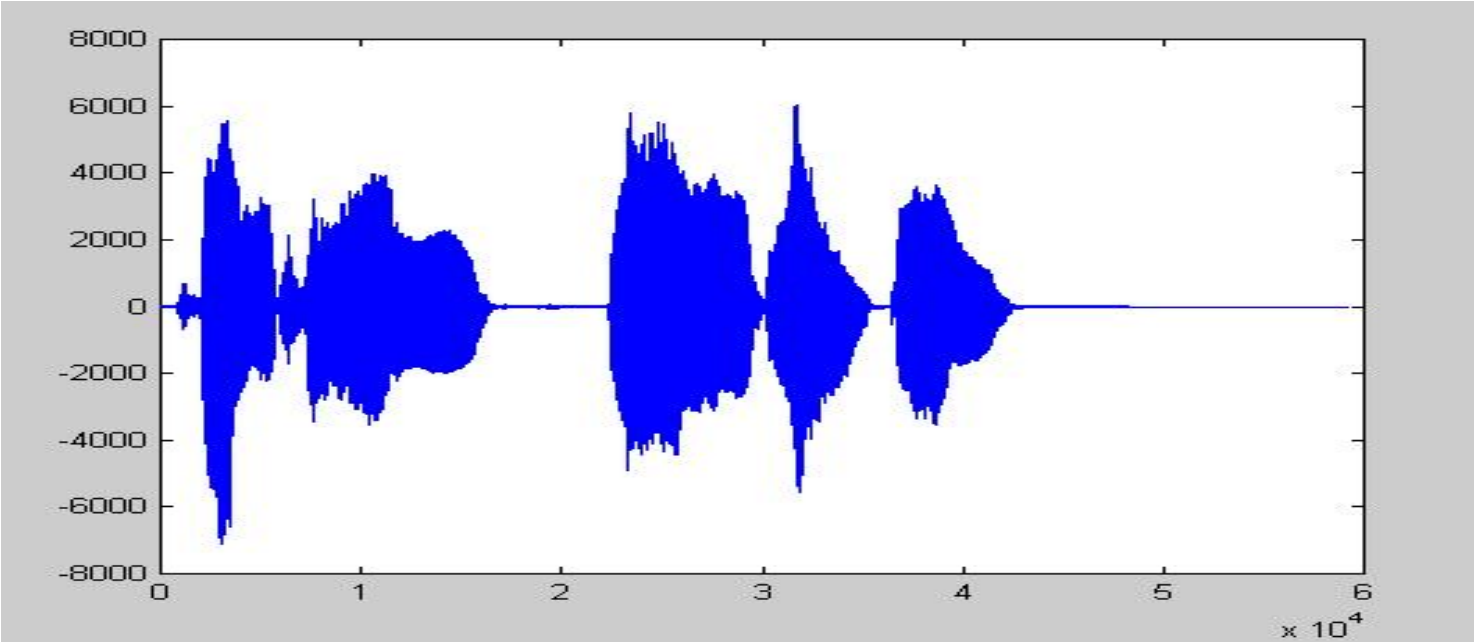
LSB原理（1）

- 去掉低2比特位的语音信号（声音信号听不出差别）



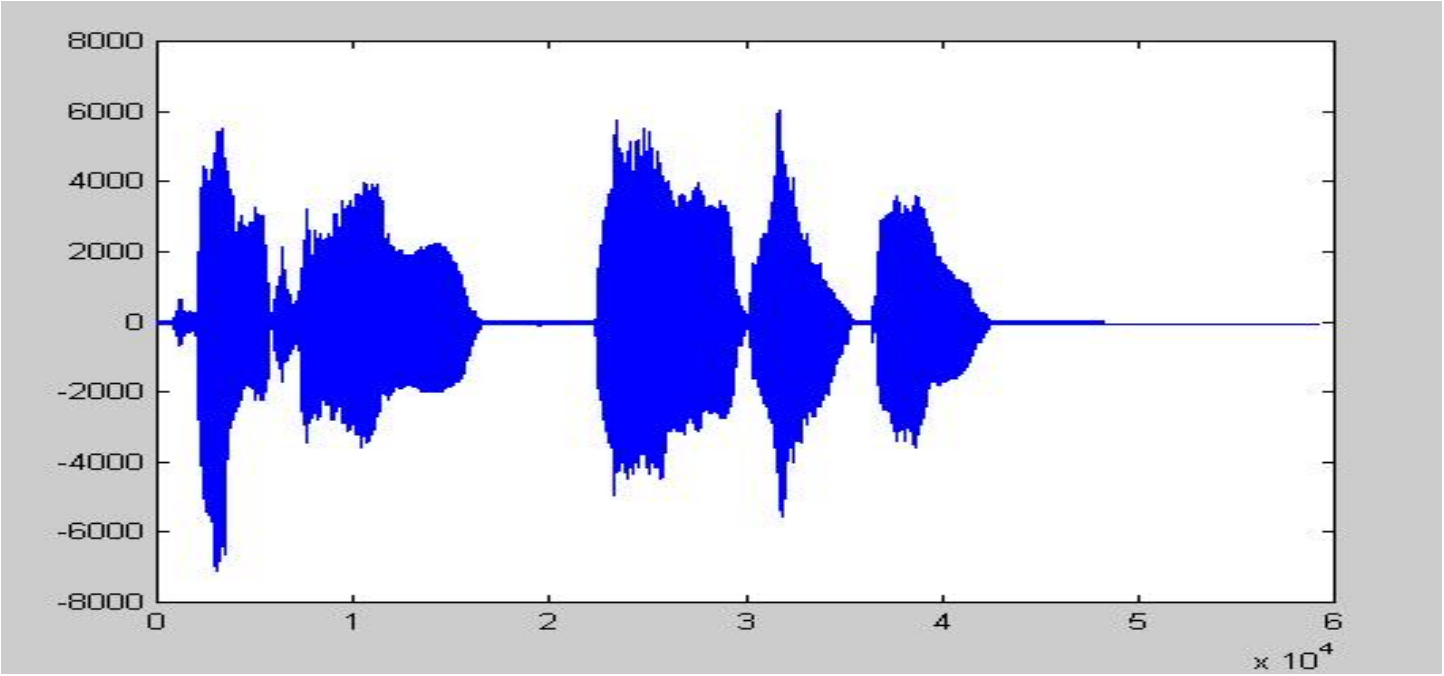
LSB原理（2）

- 去掉低4比特位的语音信号（声音信号听不出差别）



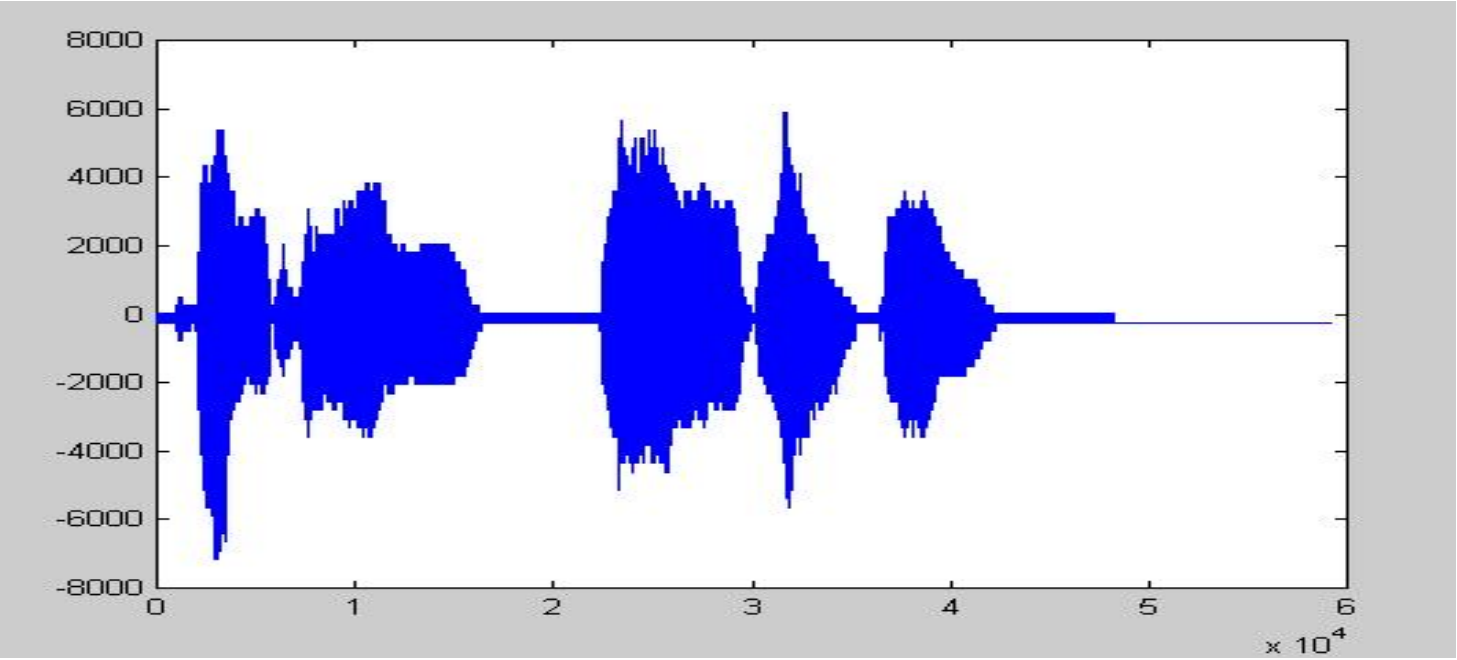
LSB原理（3）

- 去掉低6比特位的语音信号（声音中有极少的背景噪音，不易被察觉）



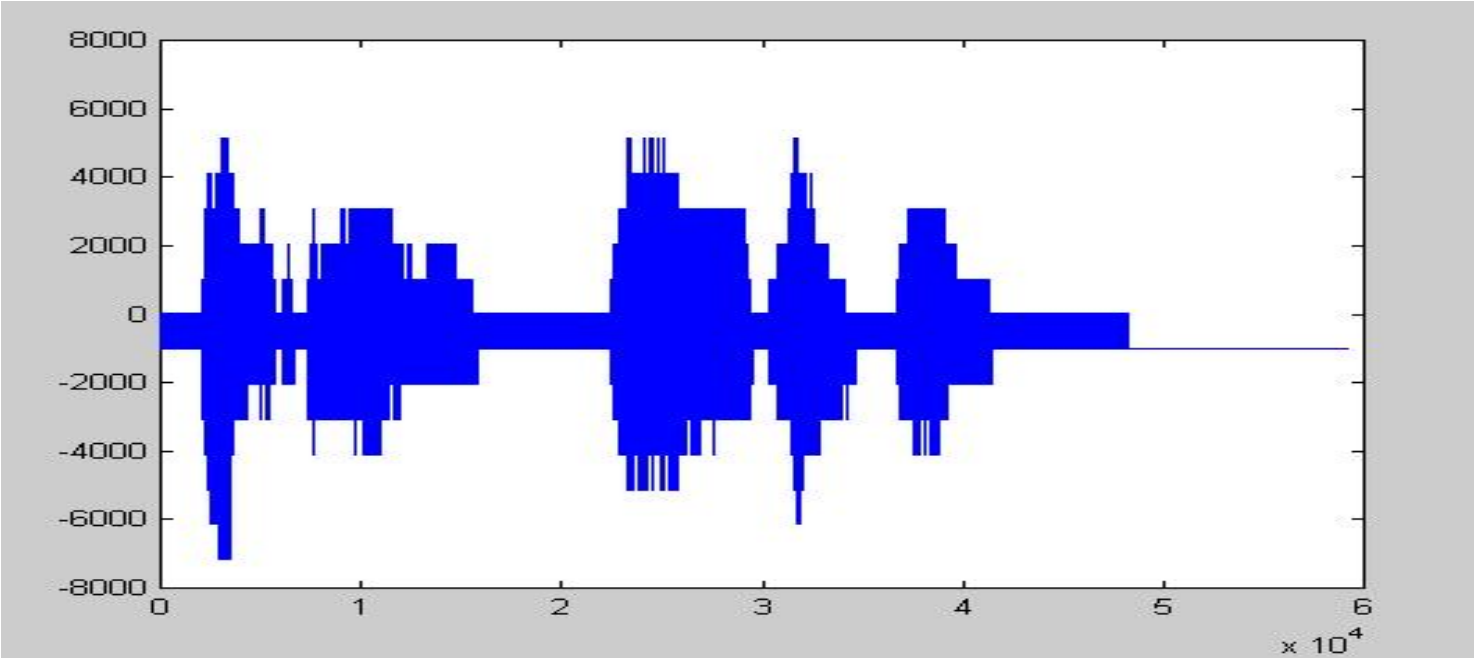
LSB原理（4）

- 去掉低8比特位的语音信号（声音中有较明显的背景噪音）



LSB原理（5）

- 去掉低10比特位的语音信号（声音中有很强的噪音，但话音仍较清晰）



LSB原理（5）

- 结论
  - 数字化音频中，低有效比特对音质贡献弱。
  - 改变低有效比特不会显著影响音质。

LSB算法

- LSB算法实现
  - 嵌入：用水印替换最低（或次低等）有效比特

0110 0011 0101 0111 0111 0110

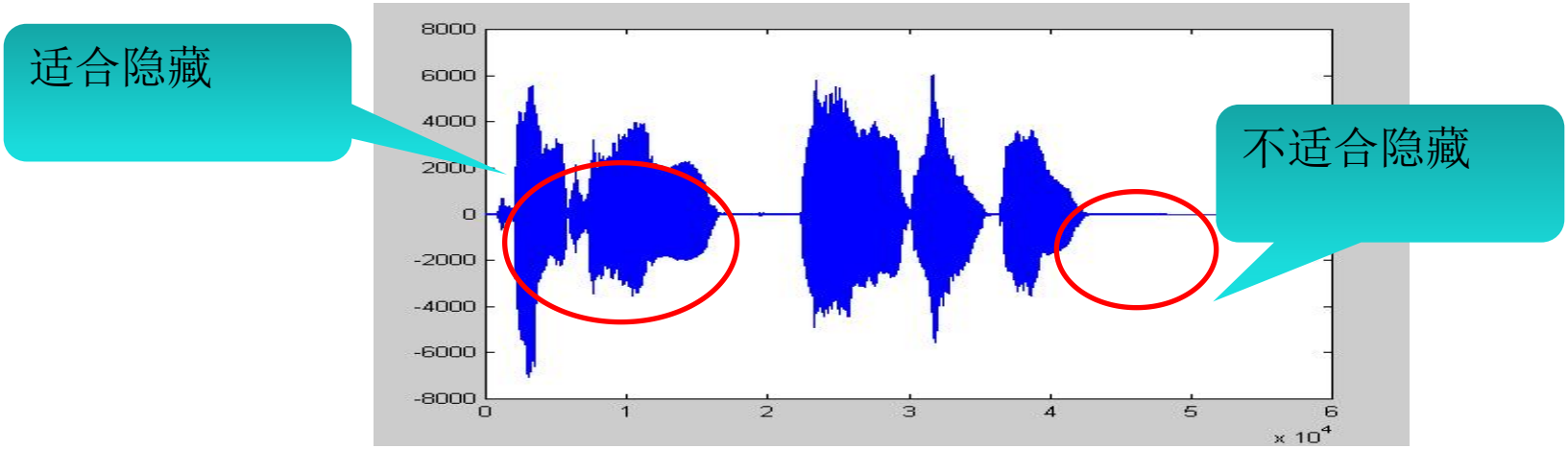
0 0 1

0110 0010 0101 0110 0111 0111

  - 提取：提取最低（或次低等）有效比特组合为水印。

LSB算法

- LSB算法设计
  - 选择样点
    - 样点幅值大小与其掩蔽能力有关
    - 静音段——幅值较小的样点不宜用于隐藏。



LSB算法

- LSB算法设计
  - 选择比特位
    - 低比特位对音质影响小，但容易受到干扰。
    - 例如：幅值为6(110B)的样点，哪怕幅度仅变化1，其多个比特位也会发生变化，
    - 若幅值减小1，变为5（101B），则最低、次低有效比特位变化；

LSB算法

- LSB算法设计
  - 选择比特位
    - 若幅值增大1，变为7（111B），则最低有效比特位发生变化。
    - 若在次低或第3比特位隐藏水印，则不容易受噪声干扰，但嵌入前后样点幅值的变化幅度由1上升到2或4。

LSB小结

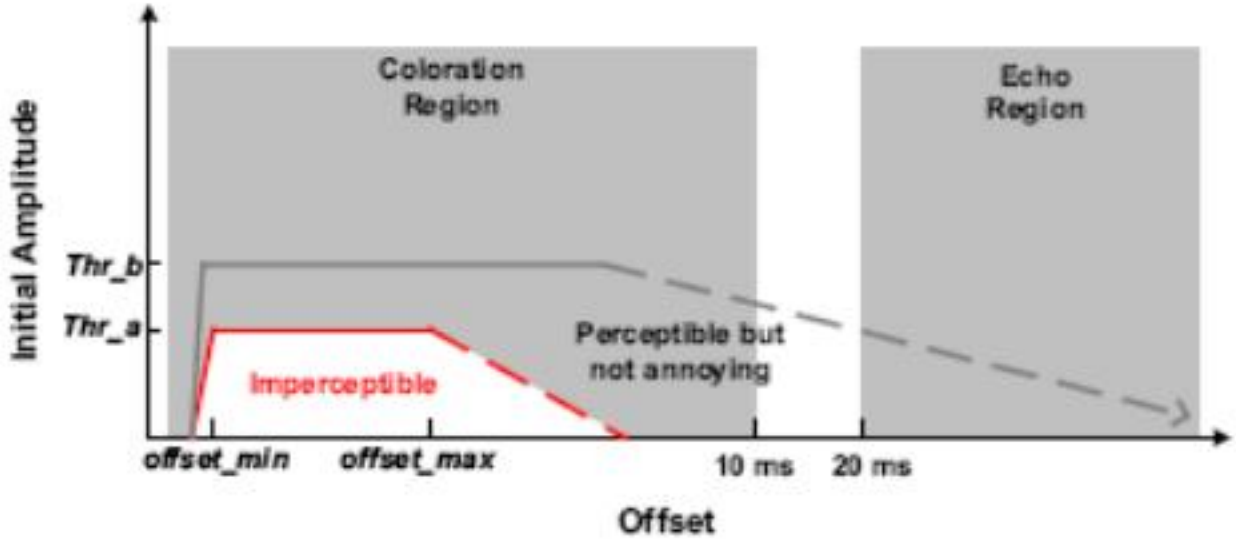
- LSB算法参数包括:
  - 样点和比特位置的选取
- LSB算法性能:
  - 透明度高
  - 容量大
  - 鲁棒性差

LSB算法

- 思考题
  - 某音频采用8比特无符号数量化，已知该音频使用了LSB算法嵌入了秘密信息，且部份样点值为127，125，110，则可从中提取的3位秘密信息是?

回声隐藏

- 原理
  - 掩蔽效应：强信号的存在会使其附近的弱信号难以被感知。
  - 当回声与原声的间隔充分接近时，人耳难以区别回声和原声。



回声隐藏

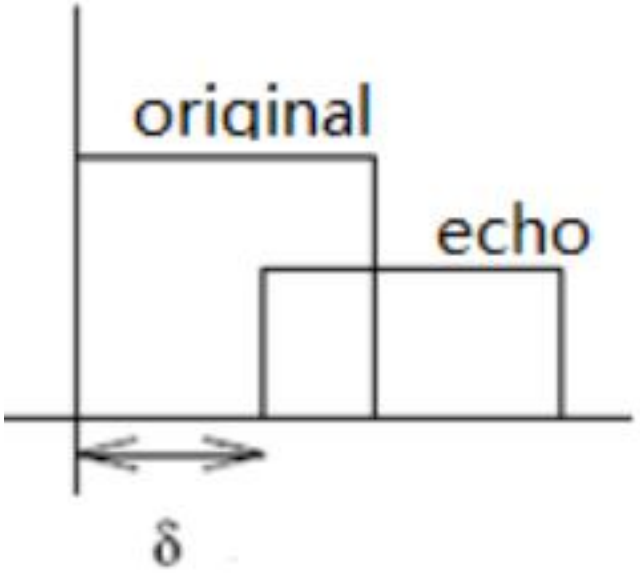
- 如何应用掩蔽效应隐藏秘密信息?
  - 回声和原声间的延迟在一定范围内人耳都难以察觉，
  - 亦即可以人为添加不同延迟的回声。

回声隐藏

- 如何应用掩蔽效应隐藏秘密信息?
  - 要隐藏二进制信息，只需用两种不同延迟的回声分别代表0、1比特。
  - 例如，回声延迟为1毫秒代表比特“1”，回声延迟为2毫秒代表比特“0”，这样，要隐藏0，那么我们在原声上添加延迟为2毫秒的回声。

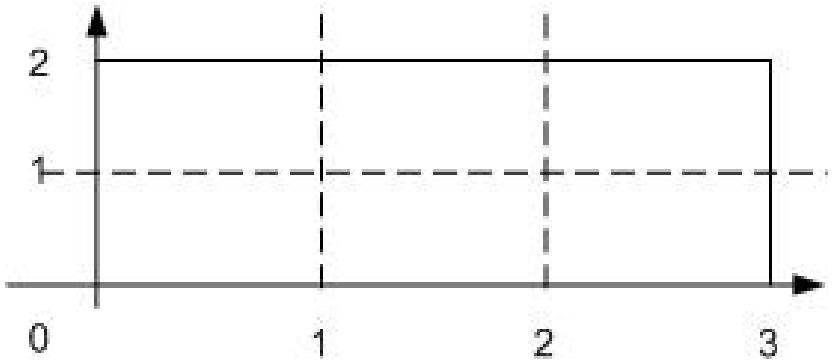
回声隐藏

- 如何“生成”回声信号?
  - 回声信号，可简单模拟为，原始信号经过时延和幅度衰减后产生的信号。
  - 设原信号为x(t)，时延为δ（德尔塔），衰减为α（阿尔法），
  - 则回声信号为:
  - $y(t)= \alpha x(t- \delta)$。

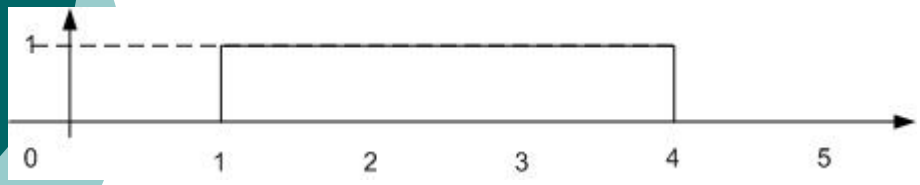


回声隐藏

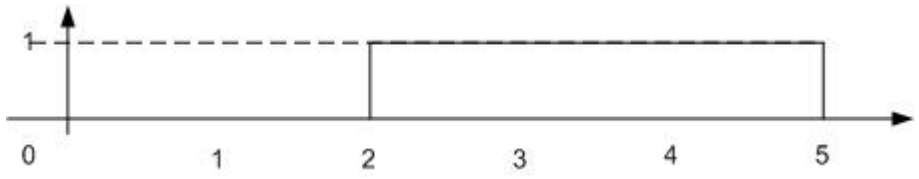
- 例：若回声延迟为1毫秒代表比特“1”，回声延迟为2毫秒代表比特“0”，回声幅度衰减系数为0.5，请给出下面信号对应的0、1回声信号，以及在这个信号上嵌入比特“1”以后所得信号



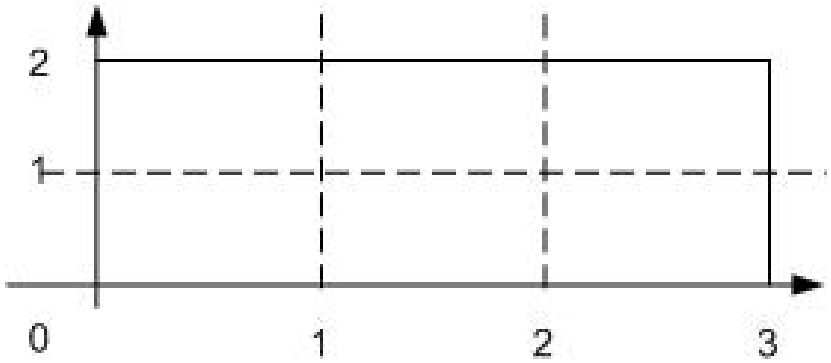
回声隐藏



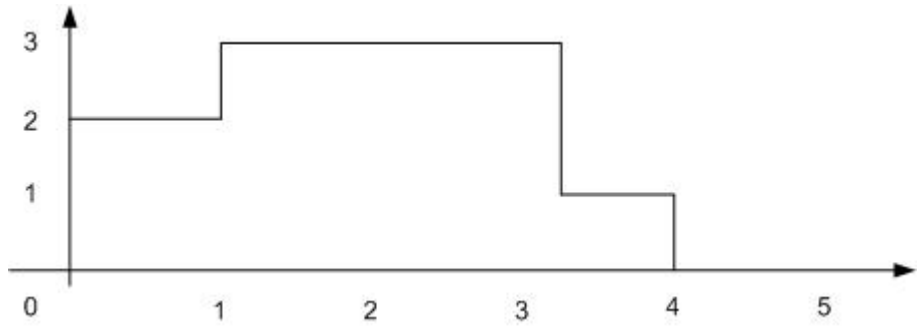
标识比特“1”的回声信号



标识比特“0”的回声信号



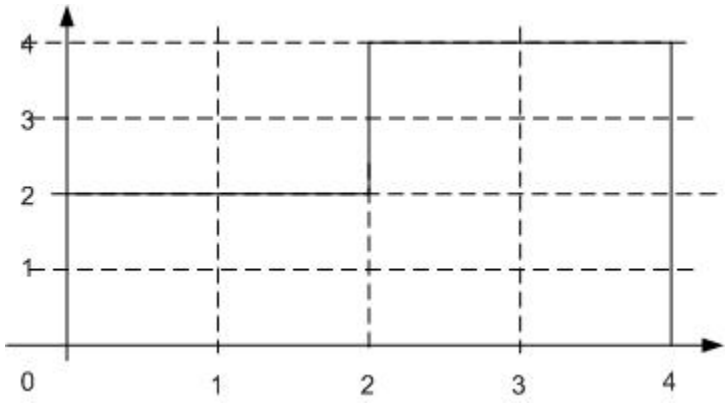
原始信号

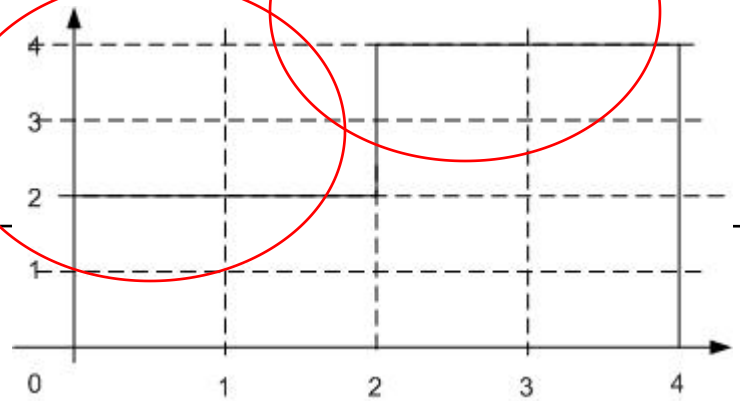


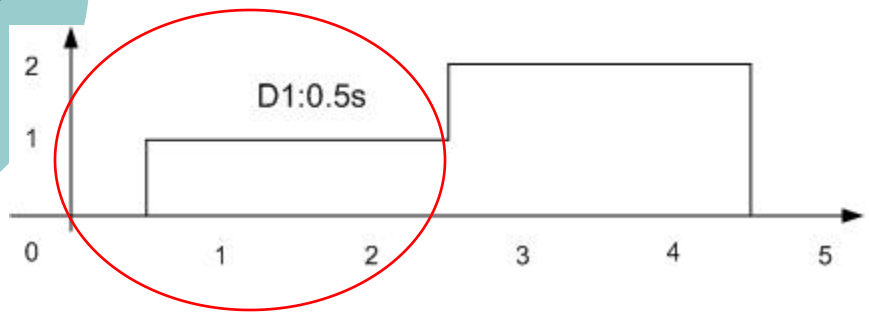
叠加回声“1”后的合成信号

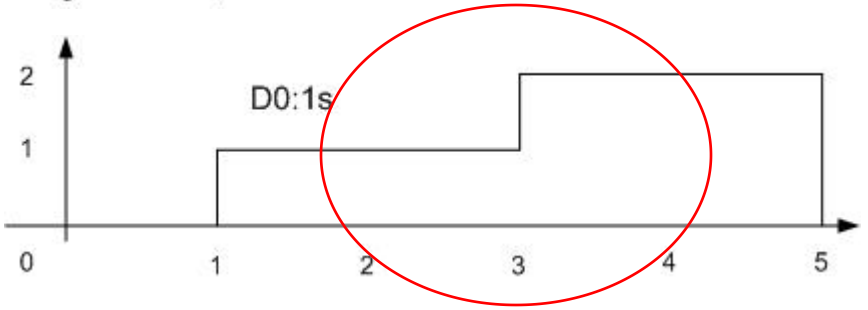
回声隐藏

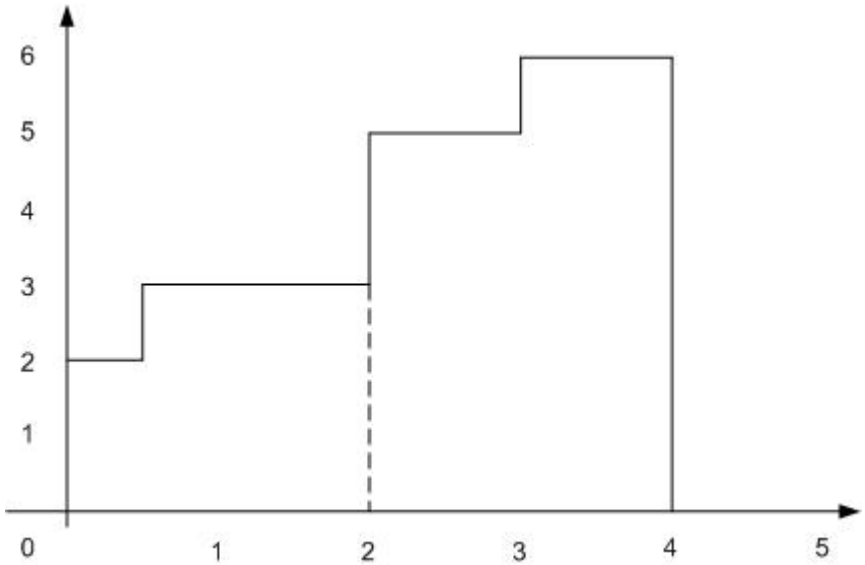
- 如何隐藏多个比特?
  - 语音信号分为多个片段，每个分段加入对应不同回声
- 例：若回声延迟为0.5毫秒代表比特“1”，回声延迟为1毫秒代表比特“0”，回声幅度衰减系数为0.5，分段长度为2毫秒，请给出下面信号嵌入信息 “10”以后所得信号



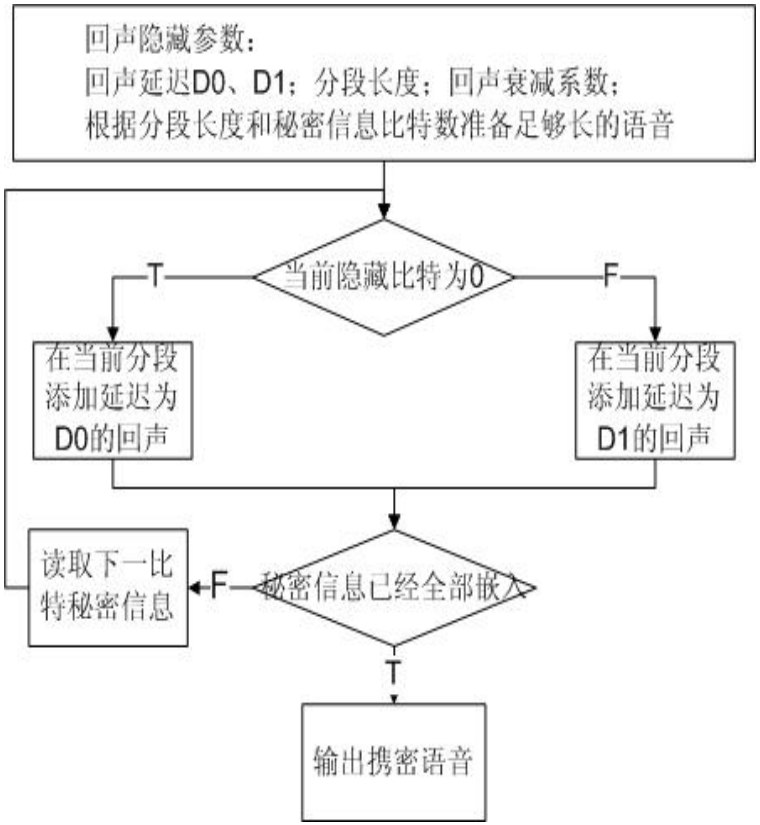

4
3
2
1
0
1
2
3
4

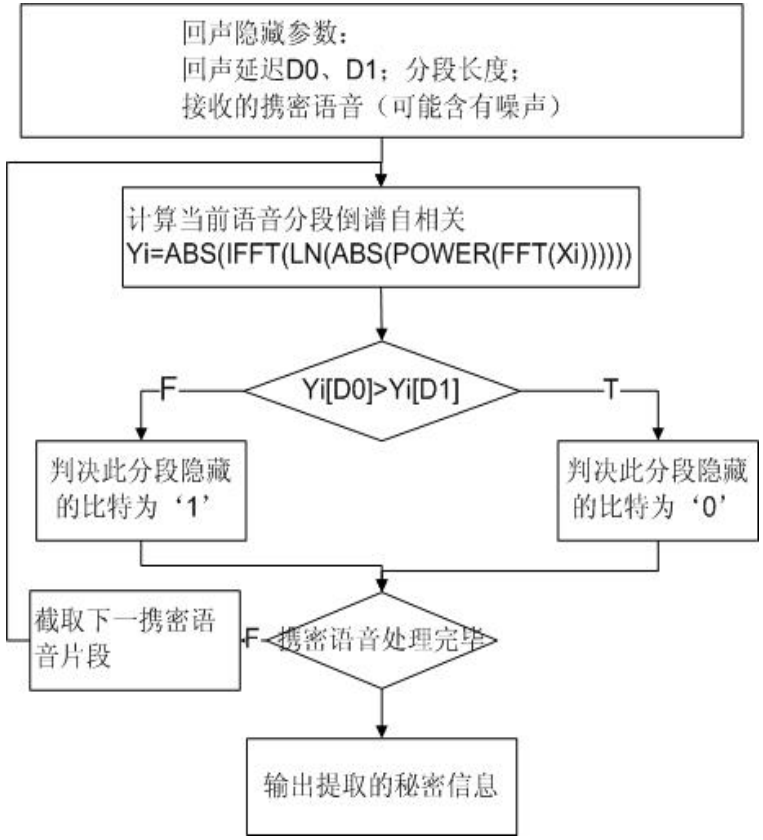

2
1
D1:0.5s
0
1
2
3
4
5


2
1
D0:1s
0
1
2
3
4
5


6
5
4
3
2
1
0
1
2
3
4
5

回声隐藏


回声隐藏参数：
回声延迟D0、D1；分段长度；回声衰减系数；
根据分段长度和秘密信息比特数准备足够长的语音
当前隐藏比特为0
T
F
在当前分段添加延迟为D0的回声
在当前分段添加延迟为D1的回声
秘密信息已经全部嵌入
F
读取下一比特秘密信息
T
输出携密语音


回声隐藏参数：
回声延迟D0、D1；分段长度；
接收的携密语音（可能含有噪声）
计算当前语音分段倒谱自相关
Yi=ABS(IFFT(LN(ABS(POWER(FFT(Xi)))))))
Yi[D0]>Yi[D1]
F
T
判决此分段隐藏的比特为‘1’
判决此分段隐藏的比特为‘0’
截取下一携密语音片段
F
携密语音处理完毕
输出提取的秘密信息

回声隐藏

- 如何提取水印？
  - 使用倒谱自相关系数检测。
  - 倒谱自相关系数在回声延迟位置处有峰值

变换域音频水印

- 傅氏变换
- DCT变换
- 小波变换

基于小波变换的音频水印算法

- 嵌入
  - 数字水印为一个随机信号
  - 选择适当的小波基对原始语音信号进行L级分解，在第L级的小波细节分量中嵌入水印
  - 水印嵌入算法

$$d_L'(i) = d_L(i)(1 + \alpha x(i))$$

基于小波变换的音频水印算法

- 提取
  - 在水印检测端（作品所有者或第三方认证机构），原始的语音信号以及水印信号需要保留以备检测时用
  - 对L级分解的细节分量，利用原始语音信号找到隐藏了N个随机数的位置，求

$$x'(i) = (d_L'(i) / d_L(i) - 1) / \alpha$$

  - 计算提取水印与原始水印的相关值，判断是否有水印信号存在

基于小波变换的音频水印算法

- 算法特点
  - 一方面语音信号遮盖了水印的影响，使其不易被发觉
  - 另一方面即使受到一定的破坏，只要语音信号有一定的可懂度，水印信号就可以检测出来

算法特点

- 单比特算法
- 非盲检测

前沿问题

- 合成分析在信息隐藏中的应用
- 抗低比特率压缩编码算法的信息隐藏算法
- 信息隐藏中的同步问题

前沿问题

- 合成分析在信息隐藏中的应用
- 抗低比特率压缩编码算法的信息隐藏算法
- 信息隐藏中的同步问题

抗低比特率压缩编码算法
音频水印的分类

- 在原始音频信号中嵌入
- 在音频编码器中嵌入
  - 这种方法稳健性较高，但需要复杂的编码和解码过程，运算量大，实时性不好。

抗低比特率压缩编码算法
音频水印的分类

- 在压缩后的音频数据流中直接嵌入
  - 这种方法避免了复杂的编解码过程，但稳健性不高，而且能够嵌入的水印容量不大（压缩域数字水印）。

相邻分段能量比算法

- 基于语音能量比的隐藏算法
  - 可以有效抵抗GSM压缩编码
  - 统计压缩编码前后分段能量比，90%小于1.5
  - 调整相邻分段能量比，使之大于1.5，则90%的分段所隐藏的信息能够被正确提取

前沿问题

- 合成分析在信息隐藏中的应用
- 抗低比特率压缩编码算法的信息隐藏算法
- 信息隐藏中的同步问题

语音同步问题研究

- 在PSTN网、GSM网中的语音传输，语音信号经过数模、模数转换，同步信息丢失，要求一种模拟同步的算法
- 同步算法的思想：利用噪声的自相关和互相关性。在接收端可以利用滑动相关来进行同步检测

音频水印需解决的问题

- 缺乏有效的同步技术。
- 完善对数字水印方案的评价研究。
- 寻找与新一代压缩标准MP3、MPEG相适应的数字音频水印算法 。

音频水印需解决的问题

- 研究音频与视频结合的数字水印，达到对多媒体数据的完整保护。
- 在实用性方面，研究数字水印的网络快速自动验证技术，降低水印提取算法的复杂性。