北京邮电大学网络空间安全学院

大 作 业 报 告

课程名称： 信息隐藏与数字水印

实验名称： 回声隐藏算法的研究

实验完成人（姓名、学号）：

金竹君2018110997

　王泽2018140757

　徐子潇2018110956

　华锐2018111029

　张弼伦2018140817

　罗丹2018140775

　杨帅鹏2018140755

指导教师： 杨榆

日 期： 2018 年 1 月

**目录**

[一、成员分工](#_Toc7168_WPSOffice_Level1) [1](#_Toc7168_WPSOffice_Level1)

[二、研究背景](#_Toc32286_WPSOffice_Level1) [1](#_Toc32286_WPSOffice_Level1)

[三、研究目标](#_Toc1589_WPSOffice_Level1) [2](#_Toc1589_WPSOffice_Level1)

[四、研究方法](#_Toc27050_WPSOffice_Level1) [2](#_Toc27050_WPSOffice_Level1)

[五、关键设计](#_Toc31375_WPSOffice_Level1) [2](#_Toc31375_WPSOffice_Level1)

[5.1简单回声隐藏算法性能分析](#_Toc29569_WPSOffice_Level2) [3](#_Toc29569_WPSOffice_Level2)

[5.1.1 分段大小对算法性能的影响研究](#_Toc32286_WPSOffice_Level3) [3](#_Toc32286_WPSOffice_Level3)

[5.1.2 衰减系数对算法性能的影响研究](#_Toc1589_WPSOffice_Level3) [3](#_Toc1589_WPSOffice_Level3)

[5.1.3 回声延迟对算法性能的影响研究](#_Toc27050_WPSOffice_Level3) [3](#_Toc27050_WPSOffice_Level3)

[5.1.4 回声隐藏算法稳健性](#_Toc31375_WPSOffice_Level3) [3](#_Toc31375_WPSOffice_Level3)

[5.2多回声与前后向回声隐藏算法原理和要求](#_Toc1913_WPSOffice_Level2) [4](#_Toc1913_WPSOffice_Level2)

[5.2.1 多回声隐藏算法原理和要求](#_Toc19135_WPSOffice_Level3) [4](#_Toc19135_WPSOffice_Level3)

[5.2.2 前后向回声隐藏算法原理和要求](#_Toc29569_WPSOffice_Level3) [4](#_Toc29569_WPSOffice_Level3)

[5.3 加窗回声隐藏算法的原理和要求](#_Toc21064_WPSOffice_Level2) [4](#_Toc21064_WPSOffice_Level2)

[5.3.1 对数窗函数](#_Toc21064_WPSOffice_Level3) [5](#_Toc21064_WPSOffice_Level3)

[5.3.2 sin三角窗函数](#_Toc2405_WPSOffice_Level3) [6](#_Toc2405_WPSOffice_Level3)

[5.3.3 直线窗函数](#_Toc23134_WPSOffice_Level3) [6](#_Toc23134_WPSOffice_Level3)

[5.3.4 平方窗函数](#_Toc3507_WPSOffice_Level3) [6](#_Toc3507_WPSOffice_Level3)

[5.4 衰减系数自适应回声隐藏算法](#_Toc2405_WPSOffice_Level2) [6](#_Toc2405_WPSOffice_Level2)

[六、实验结果分析](#_Toc19135_WPSOffice_Level1) [7](#_Toc19135_WPSOffice_Level1)

[6.1简单回声隐藏算法性能分析](#_Toc23134_WPSOffice_Level2) [7](#_Toc23134_WPSOffice_Level2)

[6.1.1 分段大小对算法性能的影响研究](#_Toc9576_WPSOffice_Level3) [7](#_Toc9576_WPSOffice_Level3)

[6.1.2 衰减系数对算法性能的影响研究](#_Toc7130_WPSOffice_Level3) [8](#_Toc7130_WPSOffice_Level3)

[6.1.3 回声延迟对算法性能的影响研究](#_Toc18370_WPSOffice_Level3) [9](#_Toc18370_WPSOffice_Level3)

[6.1.4 回声隐藏算法稳健性](#_Toc32387_WPSOffice_Level3) [10](#_Toc32387_WPSOffice_Level3)

[6.1.5低通滤波攻击详细分析内容：](#_Toc12864_WPSOffice_Level3) [10](#_Toc12864_WPSOffice_Level3)

[6.2多回声和前后向回声隐藏算法](#_Toc3507_WPSOffice_Level2) [12](#_Toc3507_WPSOffice_Level2)

[6.2.1 算法稳健性](#_Toc14526_WPSOffice_Level3) [12](#_Toc14526_WPSOffice_Level3)

[6.2.2多回声隐藏算法低通滤波攻击详细分析](#_Toc791_WPSOffice_Level3) [13](#_Toc791_WPSOffice_Level3)

[6.2.3前后向回声隐藏算法低通滤波攻击详细分析](#_Toc448_WPSOffice_Level3) [14](#_Toc448_WPSOffice_Level3)

[6.2.4 总结](#_Toc18200_WPSOffice_Level3) [15](#_Toc18200_WPSOffice_Level3)

[6.3 实验内容](#_Toc9576_WPSOffice_Level2) [15](#_Toc9576_WPSOffice_Level2)

[6.3.1对数窗函数对信噪比、误比特率和误码率的影响](#_Toc25540_WPSOffice_Level3) [16](#_Toc25540_WPSOffice_Level3)

[6.3.2 sin三角窗函数对信噪比、误比特率和误码率的影响](#_Toc13854_WPSOffice_Level3) [17](#_Toc13854_WPSOffice_Level3)

[6.3.3 直线窗函数对信噪比、误比特率和误码率的影响](#_Toc2869_WPSOffice_Level3) [18](#_Toc2869_WPSOffice_Level3)

[6.3.4 平方窗函数对信噪比、误比特率和误码率的影响](#_Toc26014_WPSOffice_Level3) [20](#_Toc26014_WPSOffice_Level3)

[6.3.5 男声四种加窗方式SNR、误比特率和误码率的对比研究](#_Toc8265_WPSOffice_Level3) [22](#_Toc8265_WPSOffice_Level3)

[6.3.6 女声四种加窗方式SNR、误比特率和误比特率的对比研究](#_Toc16380_WPSOffice_Level3) [23](#_Toc16380_WPSOffice_Level3)

[6.3.7总结](#_Toc30976_WPSOffice_Level3) [24](#_Toc30976_WPSOffice_Level3)

[6.4 衰减系数自适应回声隐藏算法](#_Toc7130_WPSOffice_Level2) [25](#_Toc7130_WPSOffice_Level2)

[七、总结与展望](#_Toc29569_WPSOffice_Level1) [25](#_Toc29569_WPSOffice_Level1)

[7.1 总结](#_Toc18370_WPSOffice_Level2) [25](#_Toc18370_WPSOffice_Level2)

[7.2 展望](#_Toc32387_WPSOffice_Level2) [25](#_Toc32387_WPSOffice_Level2)

# 一、成员分工

金竹君 2018110997 制作音频，低通滤波攻击分析；

王泽 2018140757 多回声，前后向回声，稳健性分析；

徐子潇 2018110956 稳健性分析-高斯，重采样，AU；

华锐 2018111029 加窗函数，透明性、稳健性分析（SNR, 误比特率,误码率）；

张弼伦 2018140817 衰减系数自适应算法研究；

罗丹 2018140775 制作PPT，报告整理，重采样攻击分析；

杨帅鹏 2018140755 分段，衰减系数，延迟对性能影响研究；

# 二、研究背景

研究发现，HAS（Human Audio System，人类听觉系统）存在感知掩蔽效应，即强信号的存在会使其附近的弱信号难以被感知。因此，当回声与原声的间隔充分接近时（如图1所示），人耳难以区别回声和原声。

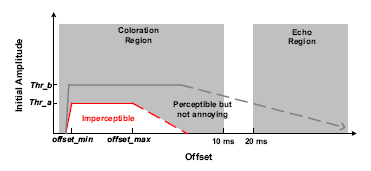


图1 回声感知区域

由图1可知，回声和原声间的延迟在一定范围内人耳都难以察觉，因此，可人为添加不同延迟的回声表征要“隐藏”（嵌入）的0、1比特。

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（如图2所示）。设原信号为x(t)，时延为δ，衰减为α，则叠加回声的信号为:y(t)= x(t) + αx(t- δ)。

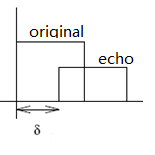


图2 原始信号和回声信号

通过上述方法嵌入秘密信息后，在接收端，要提取秘密信息（即0、1比特），只需要检测回声延迟。

根据数字信号处理相关知识可知，检测回声可计算隐写载体的倒谱自相关系数，在回声位置处，倒谱自相关系数将出现局部最大值。这个过程可以进一步简化，根据隐藏步骤，回声只可能出现在特定位置，故而，只需比较特定位置处倒谱自相关系数大小即可判决。

一段音频可以嵌入若干比特信息，即将原始音频分段，每个分段叠加不同延迟（表征0、1比特）的回声。这个过程如图3所示。



图3 a产生延迟为d0和d1的回声表征比特0和1

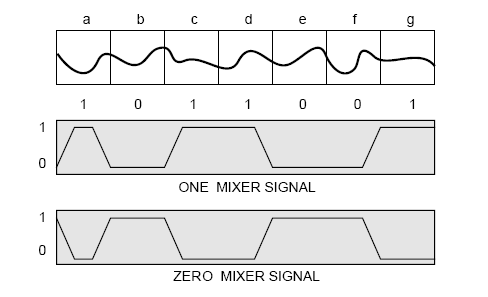


图3 b根据要嵌入的消息产生混频器（用于截取回声）

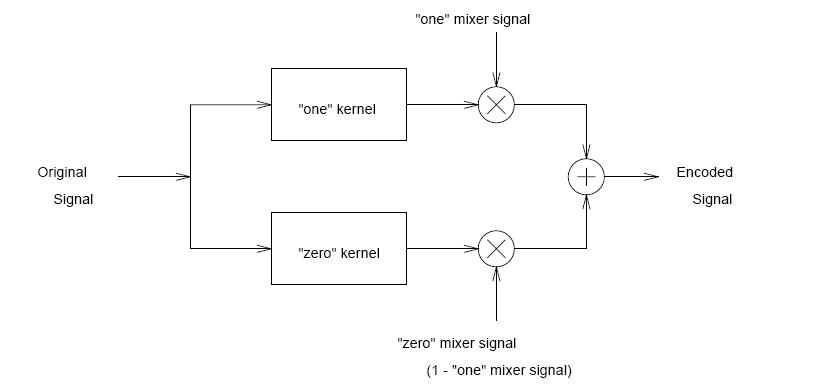


图3 c根据要嵌入的消息产生叠加于不同分段的回声信号

# 三、研究目标

简单回声隐藏算法设计与分析（分段、衰减系数、延迟、稳健性）

多回声+前后向回声隐藏算法设计与分析（稳健性）

加窗回声隐藏算法设计与分析（对数、sin三角、直线、平方窗函数、透明性、稳健性）

衰减系数自适应回声隐藏算法设计与分析（Python、稳健性）

# 四、研究方法

音频 男、女声

攻击手法分析 高斯白噪声 | 重采样 | AU | 低通滤波

加窗分析对数、sin三角、直线、平方窗函数(4窗函数)

衰减系数自适应分析

# 五、关键设计

准备一段单声道，采样频率为8000Hz，时长60秒，每样点用16比特有符号数表示的话音文件（WAV格式）。

## 5.1简单回声隐藏算法性能分析

参考代码实现了简单回声隐藏。其中，检测回声时，仅使用了信号倒谱，而不是倒谱自相关系数。

算法实现涉及到若干参数，关键参数分别是回声延迟、衰减系数和音频分段大小。调整这些参数，将会对算法透明性、稳健性和容量产生不同影响。

### 5.1.1 分段大小对算法性能的影响研究

要求:

固定回声延迟和衰减系数（例如，延迟为8、12个样点，衰减系数为0.6），依次设置分段大小为64、128、256、512、1024、2048个样点，记录该参数下，算法的容量（bit/s）、透明性（主观评价：MOS，客观评价：SNR）、稳健性（无攻击以及叠加25dB高斯噪声情况下的误码率）。

请汇总实验数据为表格（可利用xlswrite将matlab数据写入excel），并绘制各参数水平（衰减系数、分段大小）下，有无攻击两种情况下的误码率。

### 5.1.2 衰减系数对算法性能的影响研究

要求:

固定回声延迟和分段大小（例如，延迟为8、12个样点，分段大小为1024个样点），依次设置衰减系数为0.3:0.1:0.9，记录该参数下，算法的容量（bit/s）、透明性（主观评价：MOS，客观评价：SNR）、稳健性（无攻击以及叠加25dB高斯噪声情况下的误码率）。

请汇总实验数据为表格（可利用xlswrite将matlab数据写入excel），并绘制各参数水平（衰减系数、分段大小）下，有无攻击两种情况下的误码率。

### 5.1.3 回声延迟对算法性能的影响研究

要求:

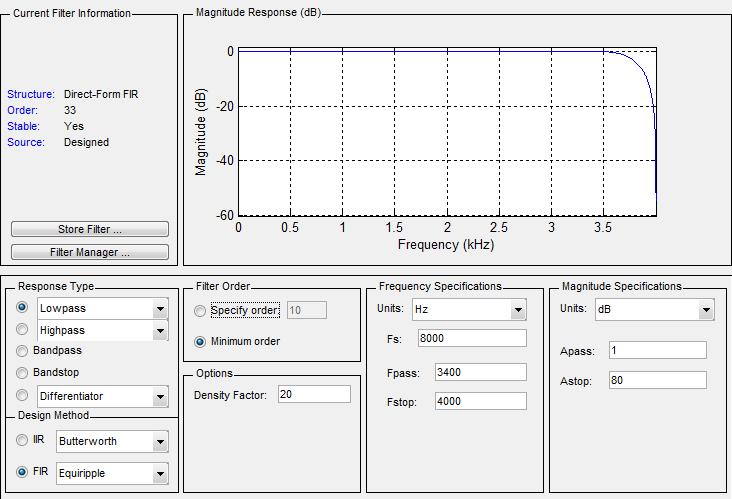
固定衰减系数和分段大小（例如，衰减系数为0.6，分段大小为2048个样点），依次设置回声延迟对为：（1，2），（8，12），（40，60），（800，1000），记录该参数下，算法的容量（bit/s）、透明性（主观评价：MOS，客观评价：SNR）、稳健性（无攻击以及叠加25dB高斯噪声情况下的误码率）。

请汇总实验数据为表格（可利用xlswrite将matlab数据写入excel），并绘制各参数水平（衰减系数、分段大小）下，有无攻击两种情况下的误码率。

### 5.1.4 回声隐藏算法稳健性

固定参数（分段：1024，延迟：8和12，衰减系数：0.7），分析稳健性。主要检测隐写对象经下述攻击后的误码率（误码率低于20%则可接受，可经由纠错编码恢复），攻击包括：叠加高斯白噪、重采样（函数:resample）、A/mU压缩编码解编码（函数AU）、低通滤波（截止频率3k，可利用GoldWave或matlab来做）。

**低通滤波攻击简介：**使用matlab的Filter Design设计FIR低通滤波器，其中Fs设置为8000Hz，Fpass设置为3400Hz，Fstop设置为4000Hz，使用filter函数调用设计的滤波器完成攻击，并且使用频谱图分析攻击效果，低通滤波器设计界面如图所示。



请汇总实验数据为表格（可利用xlswrite将matlab数据写入excel），并绘制各种攻击下的误码率。

## 5.2多回声与前后向回声隐藏算法原理和要求

### 5.2.1 多回声隐藏算法原理和要求

每一个音频分片，如果嵌入1比特信息，那么只要选择两个回声延迟位置即可，即：比特‘0’对应延迟0，比特‘1’对应延迟1。如果嵌入2比特信息，那么可以选择四个回声延迟位置，比特‘00’对应延迟0，比特‘01’对应延迟1，‘10’对应延迟2，‘11’对应延迟3。

上述分析显示，要增加每个分段能够隐藏的信息数目，一种方式是引入多个回声延迟位置。

请据此对简单回声隐藏算法进行改造，使得每个分段可以隐藏2个比特信息。

### 5.2.2 前后向回声隐藏算法原理和要求

叠加单一后向回声后，在混合音频回声位置处的理论倒谱系数值约为，若叠加一个数学意义上的前向回声，这一位置处的理论倒谱系数峰值约为。这意味着，选择较小的回声衰减系数时（透明性更好），包含前后向回声的音频能被更加准确的检测回声。基于上述原理，请对简单回声隐藏算法进行改造，使其叠加前后向回声。

## 5.3 加窗回声隐藏算法的原理和要求

一个影响回声隐藏算法的透明性的主要因素是不同延迟回声的交替。相邻的语音片段，若叠加相同延迟的回声，比起叠加不同延迟的回声，听觉效果要更好。问题在于，相邻的语音片段叠加的回声取决于要隐藏的信息，秘密信息0、1比特交替越频繁，隐写音频（包含秘密信息的音频）的透明性越低。针对这个问题，先对回声加权，再叠加回声到原始音频，可以有效平滑语音片段之间的过渡。对回声加权的过程称为加窗。普通回声隐藏可表示为：

其中，为自然音频，为其回声，为隐写音频。加窗回声隐藏可表示为：

|  |  |
| --- | --- |
|  | *g(t)*  *t*  1  0  *a*  *b*  *l* |

其中，为窗函数。为研究哪种加权函数对平滑语音片段之间的过渡效果最好，此处采用四种不同的窗函数进行实验对比，其中窗函数和图形如下，其中四种窗函数的组合图如下图所示。

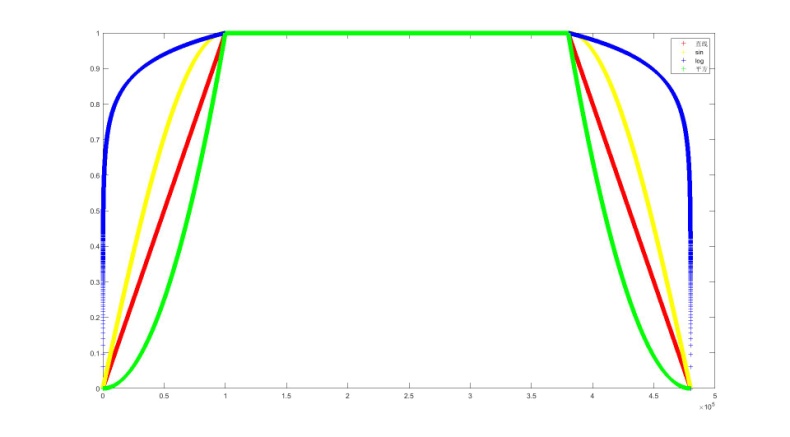


图5.3.1 四种窗函数图形

### 5.3.1 对数窗函数

### 5.3.2 sin三角窗函数

g(t)

t

1

0

a

b

l

### 5.3.3 直线窗函数

g(t)

t

1

0

a

b

l

### 5.3.4 平方窗函数

g(t)

g(t)

tt

11

00

aa

bb

ll

## 5.4 衰减系数自适应回声隐藏算法

衰减系数的变化影响算法的透明性和稳健性（这里只考虑无攻击的情况）。在简单回声隐藏算法中，衰减系数是一个定值，作用于全局，为提高算法的透明性必然会使稳健性降低，反之亦然。

一个静态的衰减系数，难以同时实现算法的透明性和稳健性最大化。应根据信号序列的特点，自适应调整衰减系数，在保证稳健性前提下，尽量减小衰减系数的值，使透明性提高。通过对不同信号序列使用不同的衰减系数，达到总体性能的最优化。

# 六、实验结果分析

## 6.1简单回声隐藏算法性能分析

参考代码实现了简单回声隐藏。其中，检测回声时，仅使用了信号倒谱，而不是倒谱自相关系数。

算法实现涉及到若干参数，关键参数分别是回声延迟，衰减系数，和音频分段大小。调整这些参数，将会对算法透明性、稳健性和容量产生不同影响。

### 6.1.1 分段大小对算法性能的影响研究

固定回声延迟和衰减系数（例如，延迟为8、12个样点，衰减系数为0.6），依次设置分段大小为64、128、256、512、1024、2048个样点，记录该参数下，算法的容量（bit/s）、透明性（主观评价：MOS，客观评价：SNR）、稳健性（无攻击以及叠加25dB高斯噪声情况下的误码率）。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **音频** | **分段大小** | **容量（bit/s）** | **透明性** | | **稳健性（误码率）** | |
| **MOS** | **SNR** | **无高斯攻击** | **高斯攻击** |
| 男声 | 64 | 125 | 5 | 4.436391 | 0.833333 | 0.972222 |
| 128 | 62.5 | 5 | 4.436766 | 0.416667 | 0.638889 |
| 256 | 31.25 | 5 | 4.435938 | 0.388889 | 0.611111 |
| 512 | 15.625 | 5 | 4.436812 | 0.361111 | 0.472222 |
| 1024 | 7.8125 | 5 | 4.437013 | 0.555556 | 0.638889 |
| 2048 | 3.90625 | 5 | 4.437597 | 0.750000 | 0.861111 |
| 女声 | 64 | 125 | 5 | 4.437940 | 0.777778 | 0.916667 |
| 128 | 62.5 | 5 | 4.436956 | 0.388889 | 0.777778 |
| 256 | 31.25 | 5 | 4.436003 | 0.166667 | 0.472222 |
| 512 | 15.625 | 5 | 4.437125 | 0.055556 | 0.444444 |
| 1024 | 7.8125 | 5 | 4.437626 | 0.555556 | 0.222222 |
| 2048 | 3.90625 | 5 | 4.436495 | 0.000000 | 0.138889 |

当延时和衰减系数固定的时候，分段大小对透明性影响不大，从SNR可以看出当分段大小变大的时候，SNR的值也随着变大，说明分段大小在测试的范围内和SNR成正相关的关系，即分段大小越大透明性越好。分段大小对误码率的影响较大，从BER和STACK\_BER两列均可以看出随着分段大小的不断增大，误码率在有无攻击的情况下均先减小后增大。

### 6.1.2 衰减系数对算法性能的影响研究

固定回声延迟和分段大小（例如，延迟为8、12个样点，分段大小为1024个样点），依次设置衰减系数为0.3:0.1:0.9，记录该参数下，算法的容量（bit/s）、透明性（主观评价：MOS，客观评价：SNR）、稳健性（无攻击以及叠加25dB高斯噪声情况下的误码率）。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **音频** | **分段大小** | **容量（bit/s）** | **透明性** | | **稳健性（误码率）** | |
| **MOS** | **SNR** | **无高斯攻击** | **高斯攻击** |
| 男声 | 0.3 | 7.8125 | 5 | 10.45761 | 0.833333 | 0.972222 |
| 0.4 | 7.8125 | 5 | 7.958838 | 0.638889 | 0.833333 |
| 0.5 | 7.8125 | 5 | 6.020638 | 0.666667 | 0.722222 |
| 0.6 | 7.8125 | 5 | 4. 437013 | 0.555556 | 0.611111 |
| 0.7 | 7.8125 | 5 | 3.098077 | 0.222222 | 0.472222 |
| 0.8 | 7.8125 | 4 | 1.938238 | 0.083333 | 0.250000 |
| 0.9 | 7.8125 | 4 | 0.915188 | 0 | 0.083333 |
| 女声 | 0.3 | 7.8125 | 5 | 10.45822 | 0.777778 | 0.944444 |
| 0.4 | 7.8125 | 5 | 7.959451 | 0.638889 | 0.750000 |
| 0.5 | 7.8125 | 5 | 6.021251 | 0.666667 | 0.527778 |
| 0.6 | 7.8125 | 5 | 4.437626 | 0.555556 | 0.277778 |
| 0.7 | 7.8125 | 5 | 3.098690 | 0.000000 | 0.083333 |
| 0.8 | 7.8125 | 4 | 1.938851 | 0.000000 | 0.111111 |
| 0.9 | 7.8125 | 4 | 0.915800 | 0.000000 | 0.083333 |

当回声延迟和分段大小固定的时候，随着衰系数的不断增加，SNR值越来越小说明透明性随着衰减系数的增减而减弱，此处结果显然，添加的回声强度越大，对原来音频的影响也就越大，透明性也就越低。同时随着衰减系数的不断增加，误码率在有无攻击的情况下均越来越低，说明回声的强度越大，抵抗干扰的能力越强，但是被发现的可能性越大。

### 6.1.3 回声延迟对算法性能的影响研究

固定衰减系数和分段大小（例如，衰减系数为0.6，分段大小为2048个样点），依次设置回声延迟对为：（1，2），（8，12），（40，60），（800，1000），记录该参数下，算法的容量（bit/s）、透明性（主观评价：MOS，客观评价：SNR）、稳健性（无攻击以及叠加25dB高斯噪声情况下的误码率）。

容量：3.90625 bit/s

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **音频** | **分段大小** | **容量（bit/s）** | | **透明性** | |
| **MOS** | **SNR** | **无高斯攻击** | **高斯攻击** |
| 男声 | （1，2） | 5 | 4.436846 | 1.000000 | 1.000000 |
| （8，12） | 5 | 4.437597 | 0.750000 | 0.833333 |
| （40，60） | 5 | 4.441020 | 0.000000 | 0.055556 |
| （800，1000） | 4 | 4.359760 | 0.000000 | 0.083333 |
| 女声 | （1，2） | 5 | 4.437000 | 0.972222 | 0.972222 |
|  | （8，12） | 5 | 4.436495 | 0.000000 | 0.138889 |
| （40，60） | 5 | 4.435864 | 0.000000 | 0.027778 |
| （800，1000） | 4 | 4.476075 | 0 | 0.055556 |

随着回声延迟的时间和延迟之间的间距越来越大的时候，透明性成下降的趋势，在回声延迟为（8000,1000）时可以明显的听到有回声在原来的音频上播放，虽然不影响获取信息，但是已经能发现有回声。从最后两列可以看出随着回声延迟的增加，误码率越来越低。

### 6.1.4 回声隐藏算法稳健性

固定参数（分段：1024，延迟：8和12，衰减系数：0.7），分析稳健性。主要检测隐写对象经下述攻击后的误码率（误码率低于20%则可接受，可经由纠错编码恢复），攻击包括：叠加高斯白噪、重采样（函数:resample）、A/mU压缩编 码解编码（函数AU）、低通滤波（截止频率3k，可利用GoldWave或matlab来做）。

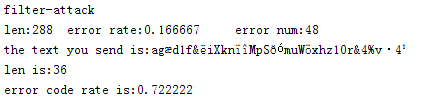
隐藏的消息：'abcdefghijklmnopqrstuvwxyz0123456789'

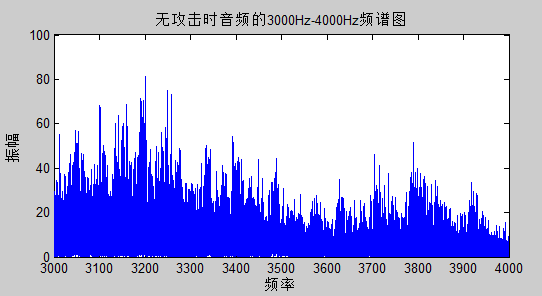
|  |  |  |  |
| --- | --- | --- | --- |
| **攻击手法** | **参数** | **误码率** | |
| **男声** | **女声** |
| 高斯白噪 | awgn(x,25%,’measured’) | 0.090278 | 0.010417 |
| 重采样 | 8000-6000 | 0.482639 | 0.517361 |
| A/mU压缩编码解编码 | yA=compand(y,89,1,'A/compressor');  yq = uencode(yA,10);  yqd = udecode(yq,10);  yAD=compand(yqd,89,1,'A/expander'); | 0.055556 | 0.000000 |
| 低通滤波攻击 | Fs设置为8000Hz，Fpass设置为3400Hz，Fstop设置为4000Hz | 0.166667 | 0.020833 |

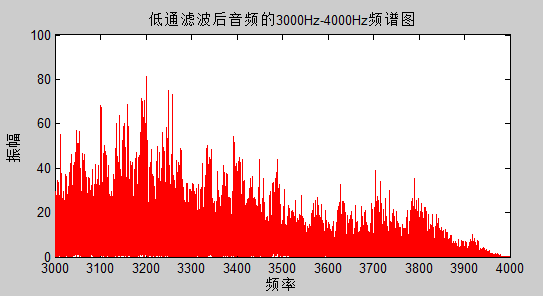
受到这四种攻击后，两个音频的误码率均小于20%，可经由纠错编码恢复，因此在上述参数情况下，该算法能够抵抗低通滤波攻击，女声音频的误码率明显低于男声音频的误码率。

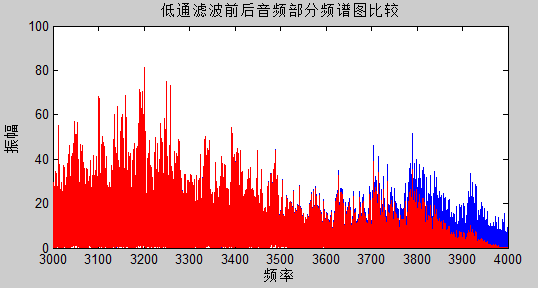
### 6.1.5低通滤波攻击详细分析内容：

（1）男声实验数据及频谱图分析：

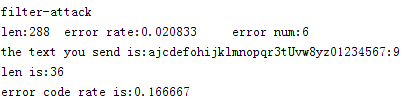


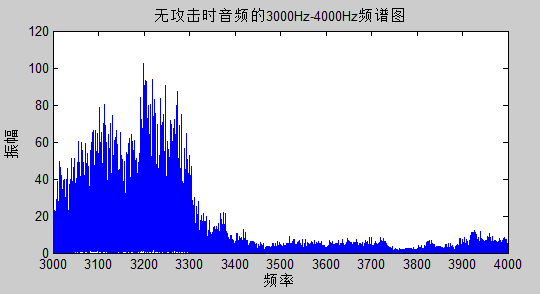


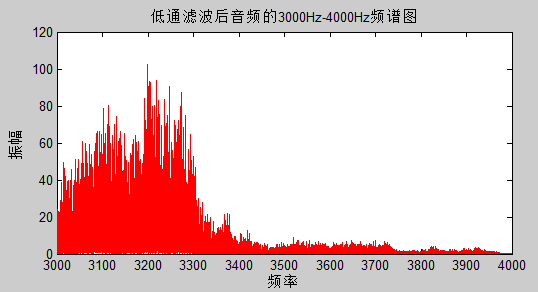


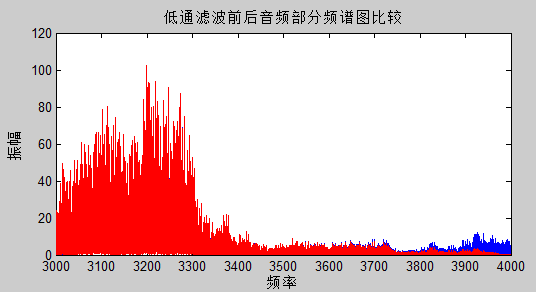


（2）女声实验数据及频谱图分析：









分析频谱图可发现滤波前后，小于3400Hz的振幅基本无变化，大于3400Hz处的振幅均有一定程度的减小，滤波后，4000Hz附近的振幅基本降为0，因此低通滤波器生效。

可知，在衰减系数为0.7，分段大小为1024个样点，回声延迟对为（8,12）情况下，受到低通滤波攻击后的两个音频的误码率均小于20%，可经由纠错编码恢复，因此在上述参数情况下，该算法能够抵抗低通滤波攻击。

同时通过实验数据发现女声音频的误码率明显低于男声音频的误码率，本实验中使用的低通滤波器Fpass为3400Hz，Fstop为4000Hz，受到影响的频率范围为3400Hz至4000Hz，无论是男声还是女声的基准音区都不在该范围内，因此主要原因不在于男声和女声的频率差异。分析隐藏信息后两个音频未受攻击时的频谱图发现，第一个音频（男声）隐藏信息后3400Hz至4000Hz范围的振幅明显高于第二个音频（女声），低通滤波器对第一个音频的影响大于对第二个音频的影响，因此判断此原因使得第一个音频受到低通滤波攻击后的误码率高于第二个音频的误码率。

## 6.2多回声和前后向回声隐藏算法

参数：

简单回声隐藏参数：分段大小1024，延迟8和12，衰减系数0.7

多回声隐藏参数：分段大小1024，延迟8、12、40、60，衰减系数0.7

前后向回声隐藏参数：分段大小1024，延迟8和12，衰减系数0.4

### 6.2.1 算法稳健性

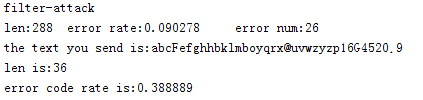
固定参数（分段：1024，延迟：8和12，衰减系数：0.7），分析稳健性。主要检测隐写对象经下述攻击后的误码率（误码率低于20%则可接受，可经由纠错编码恢复），攻击包括：叠加高斯白噪、重采样（函数:resample）、A/mU压缩编 码解编码（函数AU）、低通滤波（截止频率3k，可利用GoldWave或matlab来做）。

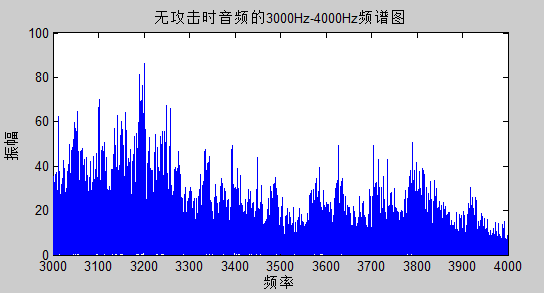
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **攻击手法** | **参数** | **误码率** | | | |
| **多回声** | | **前后向回声** | |
| **男声** | **女声** | **男声** | **女声** |
| 高斯白噪 | awgn(x,25%,’measured’) | 0.072917 | 0.017361 | 0.003472 | 0.000000 |
| 重采样 | 8000-6000 | 0.034722 | 0.000000 | 0.000000 | 0.000000 |
| A/mU压缩编码解编码 | yA=compand(y,89,1,'A/compressor');  yq = uencode(yA,10);  yqd = udecode(yq,10);  yAD=compand(yqd,89,1,'A/expander'); | 0.027778 | 0.000000 | 0.000000 | 0.000000 |
| 低通滤波 | Fs设置为8000Hz，Fpass设置为3400Hz，Fstop设置为4000Hz | 0.090278 | 0.003472 | 0.006944 | 0.000000 |

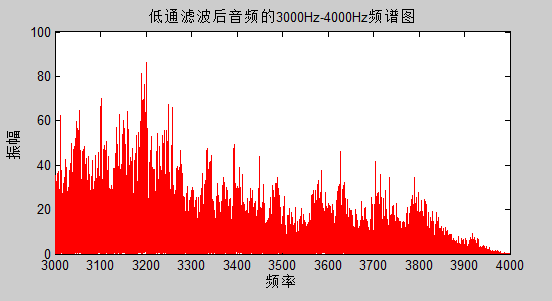
这两种算法受到这四种攻击后，两个音频的误码率均小于20%，可经由纠错编码恢复，因此在上述参数情况下，该算法能够抵抗低通滤波攻击，女声音频的误码率明显低于男声音频的误码率。

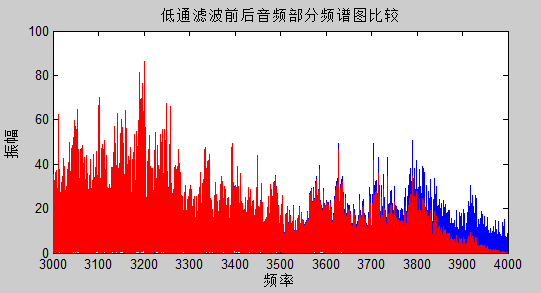
### 6.2.2多回声隐藏算法低通滤波攻击详细分析：

（1）男声实验数据及频谱图分析：

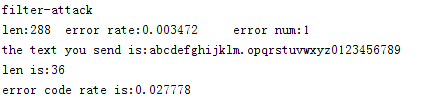


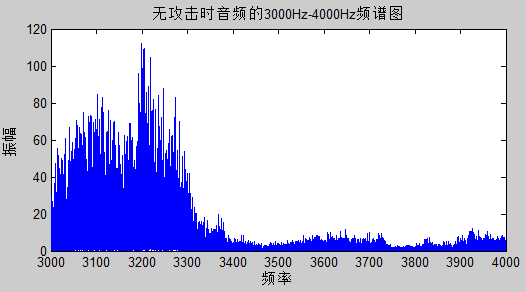


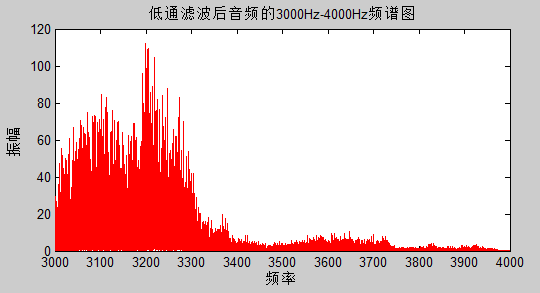


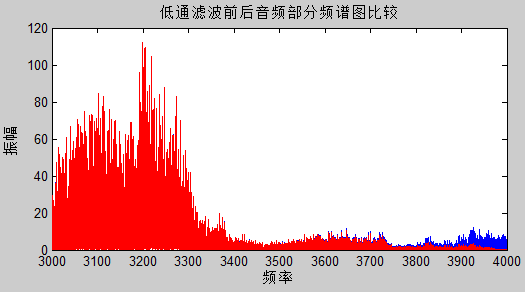


（2）女声实验数据及频谱图分析：

****

****

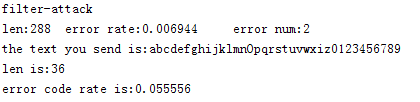
****

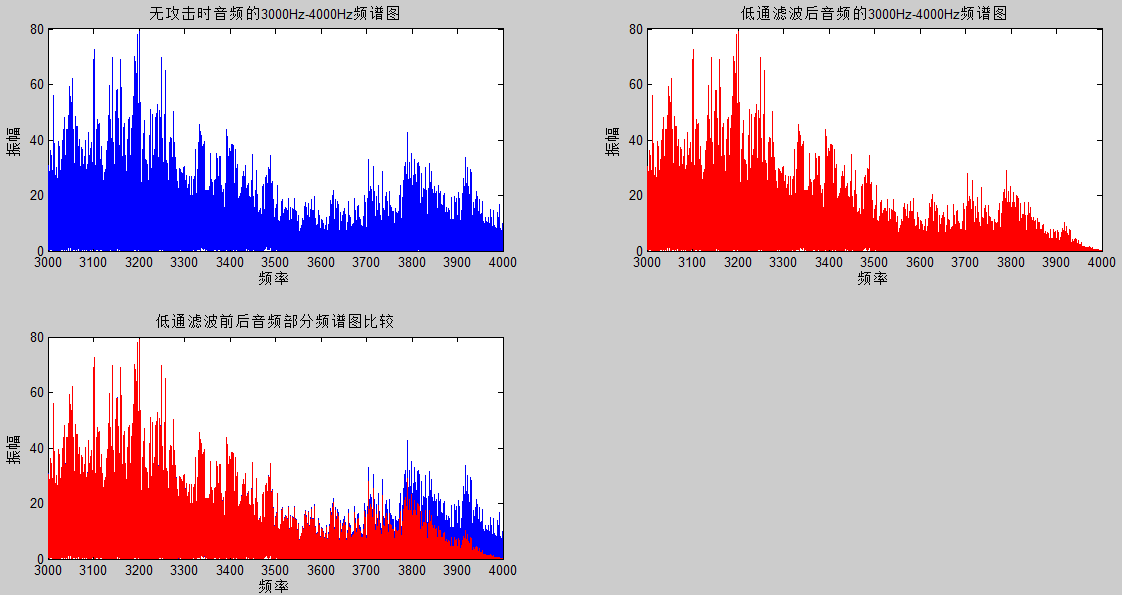
****

分析可知，在上述参数情况下，受到低通滤波攻击后的两个音频的误码率均小于20%，可经由纠错编码恢复，该算法能够抵抗低通滤波攻击。

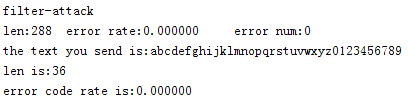
### 6.2.3前后向回声隐藏算法低通滤波攻击详细分析：

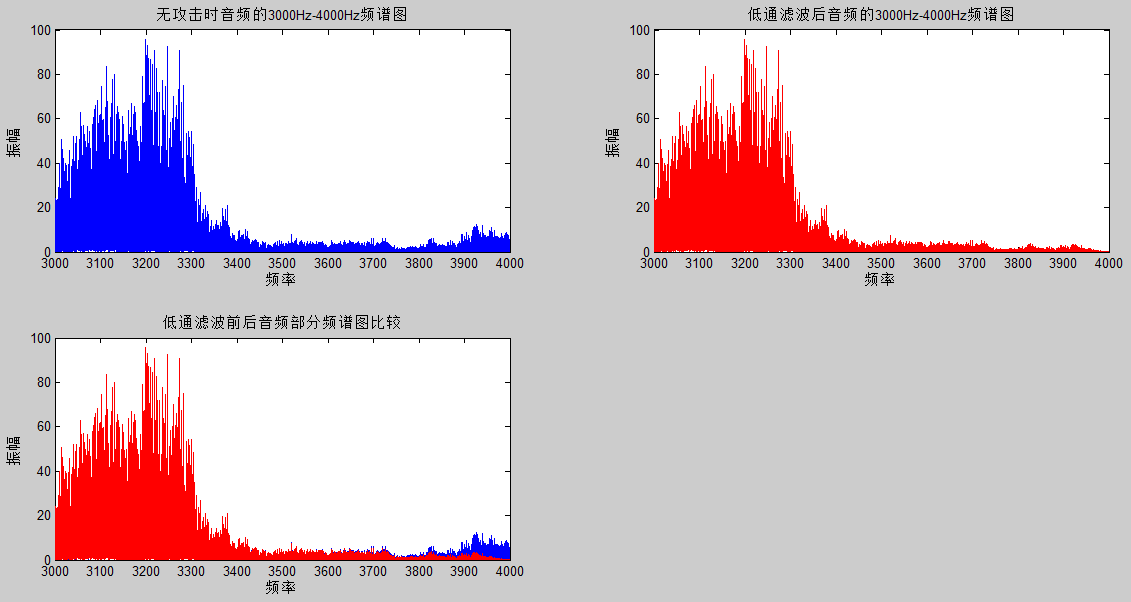
（1）男声实验数据及频谱图分析：





（2）女声实验数据及频谱图分析：





分析可知，在上述参数情况下，受到低通滤波攻击后的两个音频的误码率均小于20%，可经由纠错编码恢复，该算法能够抵抗低通滤波攻击。

### 6.2.4 总结

|  |  |  |  |
| --- | --- | --- | --- |
| 回声隐藏 | 误码率 | | 平均误码率 |
| 男声 | 女声 |
| 简单回声隐藏 | 0.166667 | 0.020833 | 0.093750 |
| 多回声隐藏 | 0.090278 | 0.003472 | 0.046875 |
| 前后向回声隐藏 | 0.006944 | 0.000000 | 0.003472 |

分析数据，可知简单回声隐藏算法、多回声和前后向回声隐藏算法均能抵抗这四种攻击，但抵抗能力前后向回声隐藏算法优于多回声隐藏算法，多回声隐藏算法优于简单回声隐藏算法。

## 6.3 实验内容

在研究加窗函数对透明性和可用性的过程中，首先设定一些不变的参数，回声衰减系数为0.7，0和1叠加的回声延迟分别为40和60样点，分段大小设定为1024。分为男、女不同声音对不同窗函数进行研究，为简化实验过程设置两端平滑部分的长度一致，此处设定窗两端平滑部分的长度取值范围为（0，10,100,1000,10000,100000,150000,200000），SNR、误码率和误比特率为因变量。SNR的大小代表透明性，SNR越大透明性越好。除SNR的值可以表征透明性外，平均意见分（MOS）可以主观的衡量隐藏的透明性，因根据产生的音频无法从主观上分出不同条件下隐藏音频产生的影响，因此此处仅仅使用SNR的值来衡量透明性。误码率和误比特率代表的是加窗函数对可用性的研究，两个比率越低可用性越好。

### 6.3.1对数窗函数对信噪比、误比特率和误码率的影响

研究对数窗函数在对信噪比、误比特率和误码率的影响，其中男、女声SNR折线图、误比特率折线图、误码率折线图如图6.1.1、6.1.2、6.1.3所示。

图6.1.1 对数窗函数男、女声SNR折线图

图6.1.2 对数窗函数男、女声误比特率折线图

图6.1.3 对数窗函数男、女声误码率折线图

### 6.3.2 sin三角窗函数对信噪比、误比特率和误码率的影响

研究sin三角窗函数在对信噪比、误比特率和误码率的影响，其中男、女声SNR折线图、误比特率折线图、误码率折线图如图6.2.1、6.2.2、6.2.3所示。

图6.2.1 sin三角函数窗函数男、女声SNR折线图

图6.2.2 sin三角函数窗函数男、女声误比特率折线图

图6.2.3 sin三角函数窗函数男、女声误码率折线图

### 6.3.3 直线窗函数对信噪比、误比特率和误码率的影响

研究直线窗函数在对信噪比、误比特率和误码率的影响，其中男、女声SNR折线图、误比特率折线图、误码率折线图如图6.3.1、6.3.2、6.3.3所示。

图6.3.1直线窗函数男、女声SNR折线图

图6.3.2直线窗函数男、女声误比特率折线图

图6.3.3直线窗函数男、女声误码率折线图

### 6.3.4 平方窗函数对信噪比、误比特率和误码率的影响

研究平方窗函数在对信噪比、误比特率和误码率的影响，其中男、女声SNR折线图、误比特率折线图、误码率折线图如图6.4.1、6.4.2、6.4.3所示。

图6.4.1 平方窗函数男、女声误码率折线图

图6.4.2 平方窗函数男、女声误码率折线图

图6.4.3 平方窗函数男、女声误码率折线图

从图6.1.1、6.2.1、6.3.1、6.4.1可以看出的男女声的音频对SNR没有影响，从图6.1.2、6.2.2、6.3.2、6.4.2可以看出男女声的音频在不同的窗函数的影响下误比特率相差不大，且误比特率在女声相对于男声来说相对较低。从图6.1.3、6.2.3、6.3.3、6.4.3可以看出误码率和误比特率在男女生不同窗函数的影响下的结果是一致的。

### 6.3.5 男声四种加窗方式SNR、误比特率和误码率的对比研究

图6.5.1 男声四种加窗方式SNR折线图

图6.5.2 男声四种加窗方式误比特率折线图

6.5.3男声四种加窗方式误码率折线图

从图6.5.1可以看出对数、三角函数、直线、平方窗函数在窗两端平滑部分的长度小于10000时四者没有明显的区别，当大于10000时呈现出依次增加的趋势。从图5.3.1可以看出四者函数图像之间的位置关系。由上两个结论可以得出函数越上凸SNR的值越小，也就意味着透明性越低。其中最极端的两种情况是没有加窗和没有添加回声，当没有加窗的时候透明性是最低的，相反没有添加回声的时候，透明性是最高的。从图6.5.2可以看出对数、三角函数、直线、平方窗函数在窗两端平滑部分的长度小于10000的时四者没有明显的区别，当大于10000时透明性对比呈现出依次减少的趋势。结合图6.5.2和图5.3.1可以看出函数越上凸误比特率的值越低，则信息隐藏的可用性越高。

### 6.3.6 女声四种加窗方式SNR、误比特率和误比特率的对比研究

6.6.1女声四种加窗方式SNR折线图

6.6.2女声四种加窗方式误比特率折线图

6.6.3女声四种加窗方式误码率折线图

### 6.3.7总结

窗函数的目的是为了有效平滑语音片段之间的过渡，平滑的程度越大，透明性越高。从本实验可以得出结论，窗两端的长度越长透明性越高同时引起的误码率和误比特率也相应的增加；当自变量的取值一定时，函数因变量的值越大即函数越上凸透明性越低同时引起的误码率和误比特率也相应的减少。比如在本实验中使用的对数函数和平方函数，对数函数相对比平方函数误码率和误比特率都较低但其透明性也比较低。综上所述，透明性和误码率之间处于一种相对的状态，应根据实际的需求找出两者的平衡点。

对数、三角函数、直线、平方窗函数的测试指标在窗两端平滑部分长度小于10000（1/4.75=21%）时没有明显区别，大于10000时测试指标（SNR、误比特率、误码率）呈现依次递增的趋势，即它们误比特率、误码率增加的同时透明性有所提升。

## 6.4 衰减系数自适应回声隐藏算法

算法实现见代码（selfAdaptive.py）。对比修改前后的算法性能，结果如下（每一段的衰减系数0-0.9）：

|  |  |  |
| --- | --- | --- |
|  | **误码率** | **PSNR(DB)** |
| **修改前（衰减系数固定0.6）** | 0.028 | 29.30 |
| **修改后（衰减系数自适应）** | 0.0035(1/288) | 35.16 |

结论：通过实验数据，可以看出，应用衰减系数自适应调整后的算法，在透明性和稳健性两方面都得到了较大提升。自适应算法的缺陷是，嵌入时的计算复杂度增加。

理论上，修改后的算法的误码率应为0。但是，由于程序需要从文件读写信号序列数值，程序运行时内存中的数值类型和文件中的数值类型不一致，两者相互转换时发生了精度损失，从而造成了误码的产生。

# 七、总结与展望

### 7.1 总结

在高斯白噪、重采样、AU和低通滤波这四种攻击下，简单回声、多回声和前后向回声隐藏算法均有良好的抵抗性，且就抵抗能力而言前后向回声隐藏算法优于多回声隐藏算法，多回声隐藏算法优于简单回声隐藏算法。

对数、三角函数、直线、平方窗函数的测试指标，在窗两端平滑部分长度小于窗总长21%时没有明显区别，大于21%时测试指标呈现依次递增的趋势，即它们误比特率、误码率增加的同时透明性有所提升。

衰减系数自适应算法能较好地改善透明性和稳健性。

### 7.2 展望

本实验窗函数研究未考虑矩形窗旁瓣高、有负旁瓣等问题，还可以从这一方向优化加窗回声隐藏算法。

衰减系数自适应算法的计算复杂度有待改善，还可优化文件数据读取带来的精度损失问题。