

北京邮电大学网络空间安全学院

信息安全认知实习

实验报告

课程名称： 信息安全认知实习

单元名称： 数字内容安全实验

姓名： 任子恒

学号： 2017522133

班级： 2017661801

专业： 信息安全

指导教师： 颀夏青

成绩：

日期： 2018 年 9 月 20 日

一、 实验目的

通过两则隐写的例子，体验信息隐藏的过程，简单从信息隐藏的方面认识数字内容安全的部分内容。

二、 实验原理

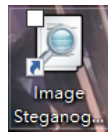
简单来说，信息隐藏技术是将一小段特定信息隐藏在大量信息中的方法，利用大量不相关的信息来掩盖这段信息，起到一些特定目的。隐写是最常见的信息隐藏技术。

图片和音频有一些存储密度较低的部分，经常可以被压缩利用隐藏信息。

三、 实验环境

一台装有 Windows Powershell v1.0 和 Adobe Audition CC2018 的 Windows 10 电脑。

音频隐写软件使用 MP3Stego_1_1_18，图片隐写软件使用 Image Steganography。



四、 实验过程及遇到的问题分析

4.1 实验过程

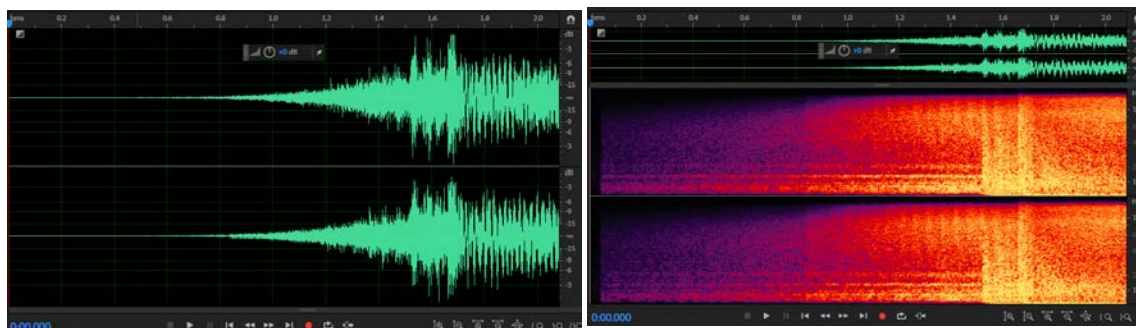
4.1.1 音频隐写

欲隐藏的文件（hidden.txt）内容：

hidden - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

2017522133 任子恒



实验前源文件的波形图（上左）频谱图（上右）

1. 进入 Windows Powershell，并进入 MP3隐写软件所在目录。

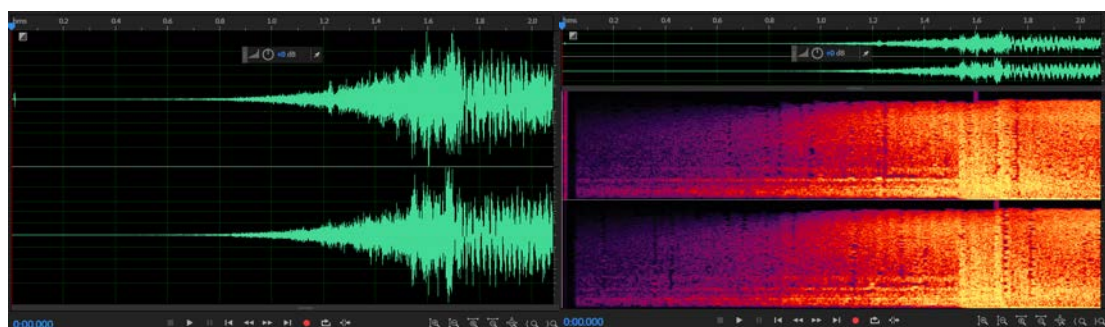
```
Windows PowerShell
PS E:\MP3Stego_1_18\MP3Stego>
```

2. 在命令行中输入 `./encode -E .\hidden.txt -P 123 .\h.wav testencode.wav`

其中-E 指定了被隐藏文本的文件名，-P 指定了加密密码。

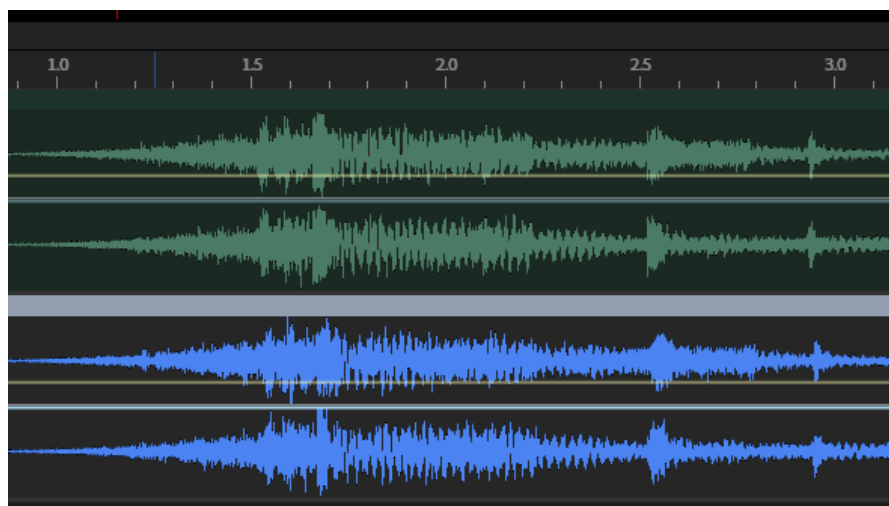
```
Windows PowerShell
PS E:\MP3Stego_1_18\MP3Stego> ./encode -E .\hidden.txt -P 123 .\h.wav testencode.wav
MP3StegoEncoder 1.1.17
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, stereo 44100Hz 16bit, Length: 0: 0:26
MPEG-I layer III, stereo Psychoacoustic Model: AT&T
Bitrate=128 kbps De-emphasis: none CRC: off
Encoding ".\h.wav" to "testencode.wav"
Hiding ".\hidden.txt"
[Frame 1027 of 1027] (100.00%) Finished in 0: 0: 0
PS E:\MP3Stego_1_18\MP3Stego>
```

3. 打开加密后的音频文件，用 audition 等其他波形查看工具查看其波形和频谱。



上图是加密后的音频文件的波形（左）和频谱（右）

下图是加密前后的波形的对比，若不打开波形查看软件仔细去看，二者几乎一致

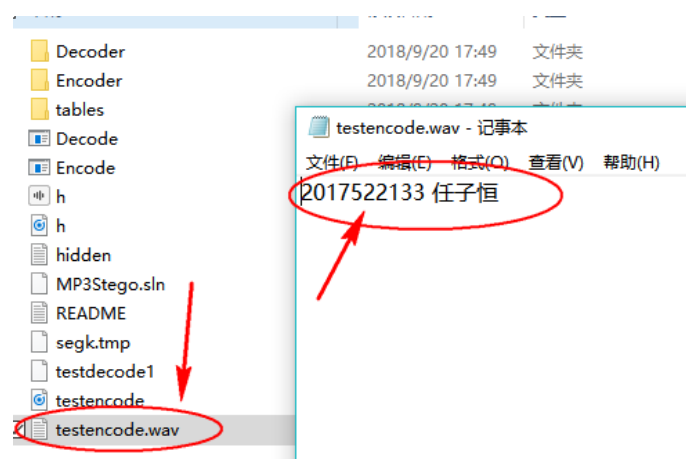


4. 命令行中输入 `./decode -X -P 123 .\testencode.wav .\testdecode1` 以得到隐藏在音频中的信息。

```
PS E:\MP3Stego_1.1.18\MP3Stego> ./decode -X -P 123 .\testencode.wav .\testdecode1
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = '.\testencode.wav' output file = '.\testdecode1'
Will attempt to extract hidden information. Output: .\testencode.wav.txt
the bit stream file .\testencode.wav is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 1027]Avg slots/frame = 417.555; b/smp = 2.90; br = 127.876 kbps
Decoding of ".\testencode.wav" is finished
The decoded PCM output file name is ".\testdecode1"
```

5. 打开在同一目录下生成的 `testencode1.wav.txt` 文件，其内容如下。

正是之前隐藏在里面的文件。

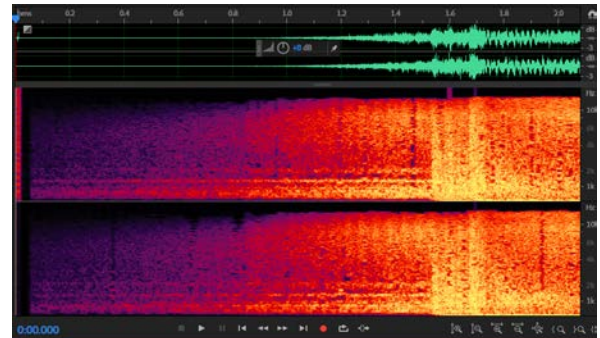


6. 如果不使用密码进行加密呢？

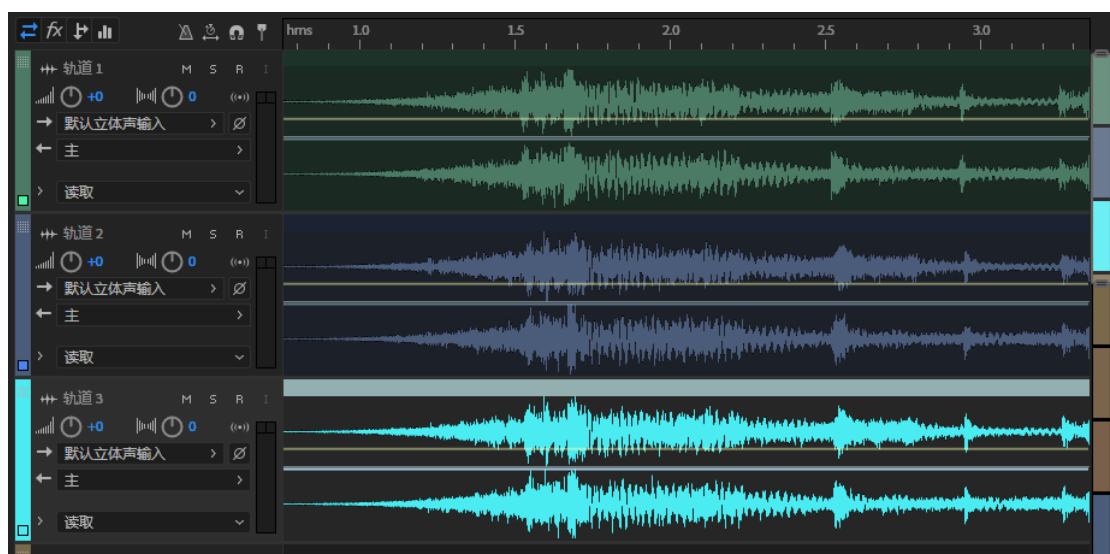
在命令行中输入 `./encode -E .\hidden.txt .\h.wav test2.wav`，在接下来询问密码时均直接按 Enter 键跳过。

```
PS E:\MP3Stego_1.1.18\MP3Stego> ./encode -E .\hidden.txt .\h.wav test2.wav
MP3StegoEncoder 1.1.17
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, stereo 44100Hz 16bit, Length: 0: 0:26
MPEG-I layer III, stereo Psychoacoustic Model: AT&T
Bitrate=128 kbps De-emphasis: none CRC: off
Encoding ".\h.wav" to "test2.wav"
Hiding ".\hidden.txt"
Enter a passphrase:
Confirm your passphrase:
[Frame 1027 of 1027] (100.00%) Finished in 0: 0: 0
```

7. 打开隐写完成的 `test2.wav` 文件，其波形图（下左）和频谱图（下右）如图所示。



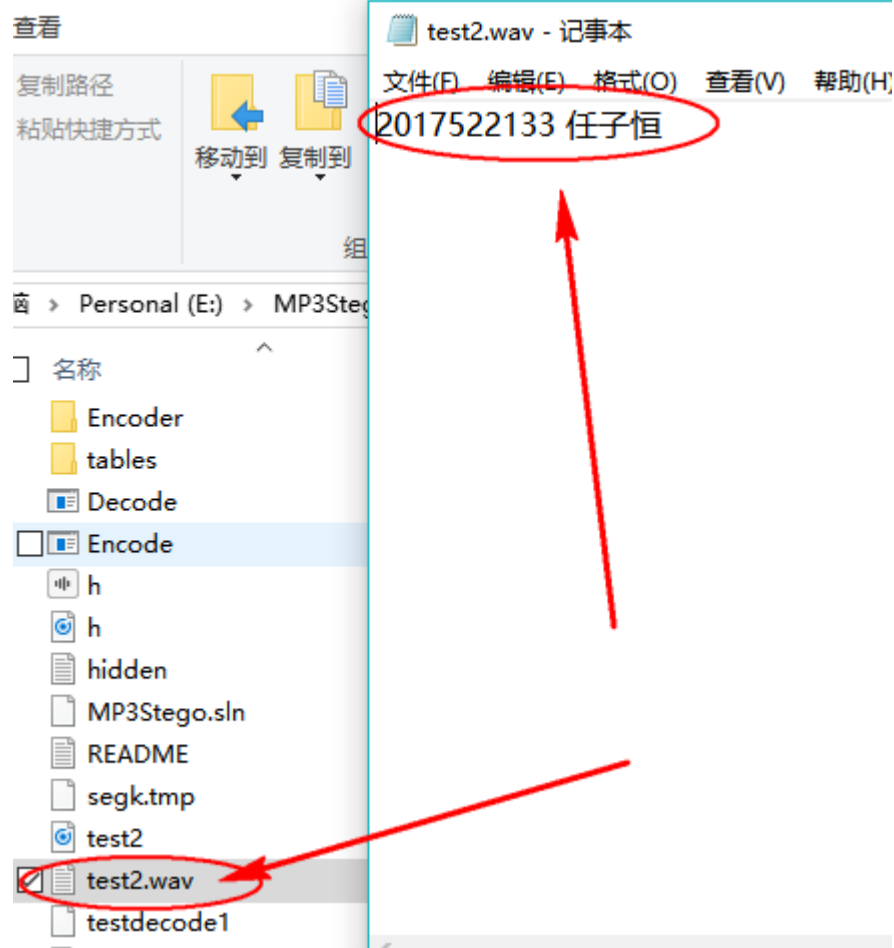
三种方式的部分波形对比图如下。（轨道1：源文件，轨道2：用密码加密隐写，轨道3：非加密隐写）



8. 命令行中输入 `./decode -X .\test2.wav .\whatintest2`，得到隐藏在其中的文件。

```
PS E:\MP3Stego_1_1_18\MP3Stego> ./decode -X .\test2.wav .\whatintest2
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = '.\test2.wav' output file = '.\whatintest2'
Will attempt to extract hidden information. Output: .\test2.wav.txt
Enter a passphrase:
Confirm your passphrase:
the bit stream file .\test2.wav is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 1027]Avg slots/frame = 417.555; b/smp = 2.90; br = 127.876 kbps
Decoding of ".\test2.wav" is finished
The decoded PCM output file name is ".\whatintest2"
```

9. 打开 test2.wav.txt，验证文件内容。结果与被隐藏的内容完全一致。



4.1.2 图片隐写

要隐写的图片

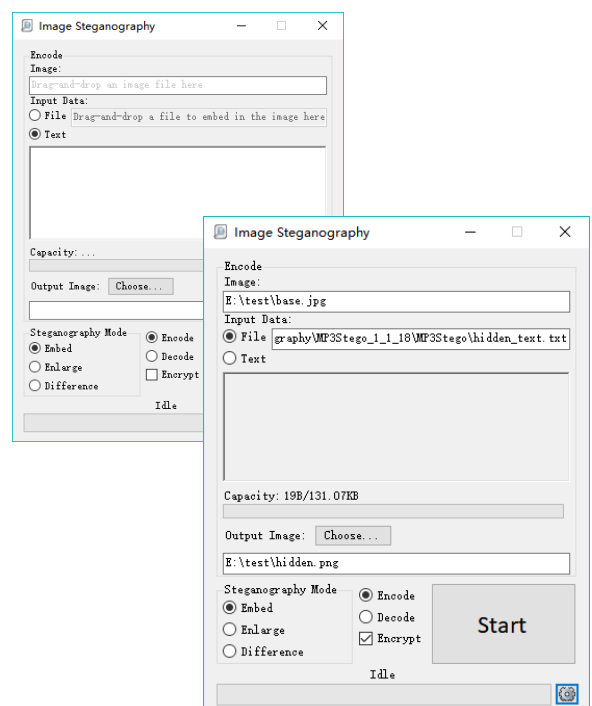


要隐写的文件: hidden.txt

(内容同4.1.1)

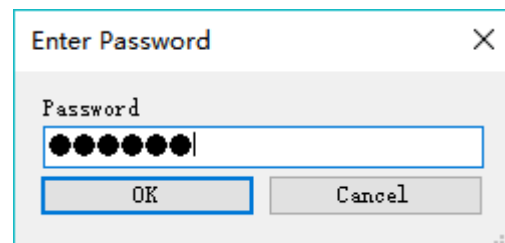
1. 打开图片隐写软件。

2. 选择欲隐写图片, 设置好输出目录, 选择 Encode, 必要时可以勾选 Encrypt 进行加密, 本例使用密码123456。



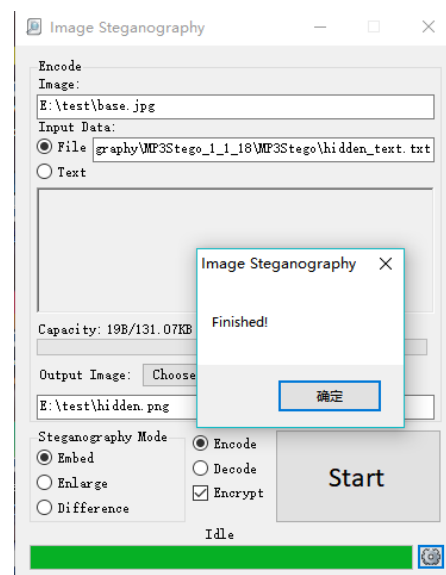
3. 点击 Start，然后输入你要设置的密码。

4. 点击 OK，等待进程完成。



5. 图片看起来跟原来没什么区别，不过文件大小大了不少。

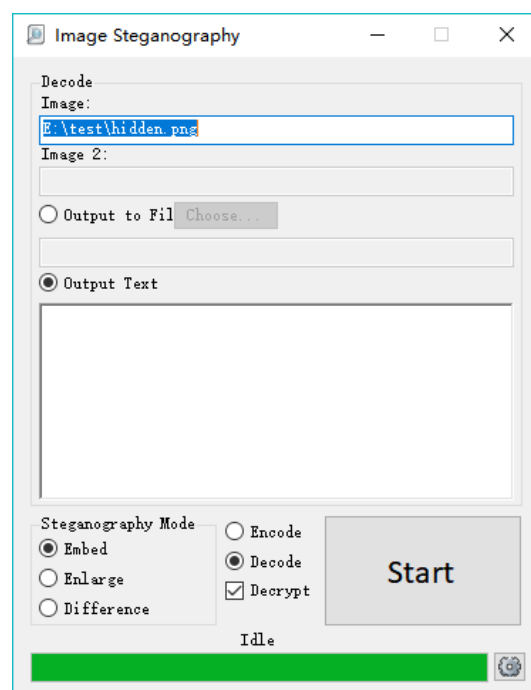
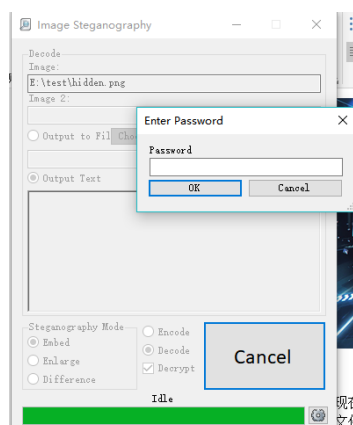
(原: 184kb, 新: 684kb)



名称	修改日期	类型	大小
base	2018/9/5 8:30	JPG 文件	184 KB
hidden	2018/9/20 10:04	PNG 文件	684 KB

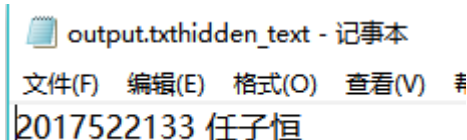
6. 现在来取出这个隐藏文件，选择 Decode 模式，把刚才生成的文件拖进来，顺便勾选上 Decrypt。

7. 点击 Start，并输入密码。

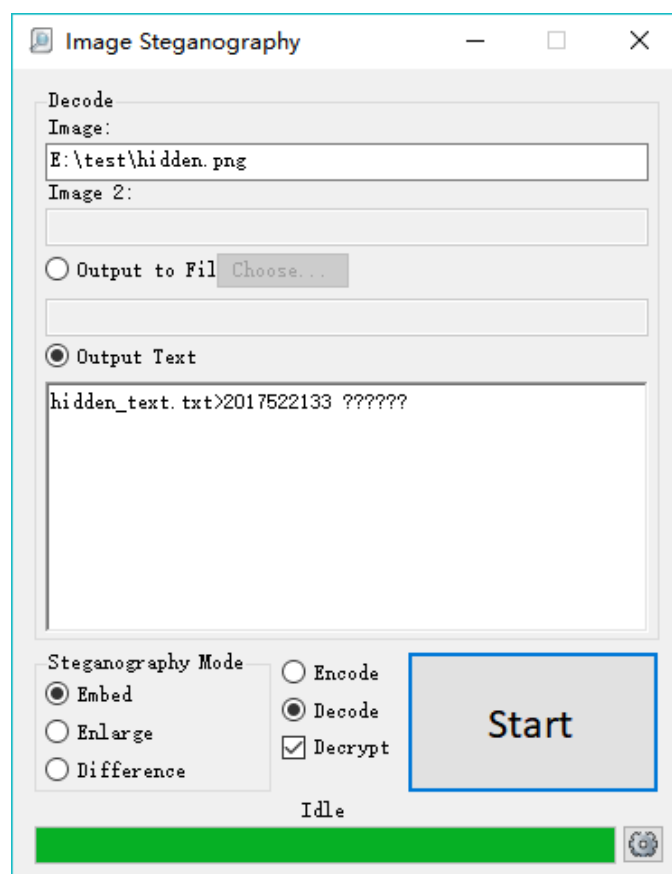


8. 刚才选的是输出文字模式，所以 output text 文本框部分有部分乱码，内容不太全，但学号部分正确（可能是编码原因），现在我们换作 output to file 重新试一下。

9. 提取成功，正是之前所隐藏的内容。



output.txthidden_text - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2017522133 任子恒



4.2 过程中遇到的问题

1. 关于 MP3Stegno 的一些吐槽

-叫做 MP3Stegno，却只能用于向 wav 文件的隐写？

```
PS E:\MP3Steganography\MP3Stego_1_1_18\MP3Stego> .\encode -E hidden_text.txt base.mp3 hidden.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
[ERROR] Input not a MS-RIFF file
```

-似乎只有特定文件才行，由 MP3转来的 wav 文件运行不下去，报错为
[ERROR]Can' t find data chunk

```
PS E:\MP3Stego_1_1_18\MP3Stego> .\encode base.wav basetest.wav
MP3StegoEncoder 1.1.17
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, stereo 44100Hz 16bit, [ERROR] Can't find data chunk
```

-命令行细节要求繁琐，比如我的个人电脑不能直接用 encode，需要加./或改用 exe 路径（怀疑为个人系统权限问题）。

2. 至今未解决的疑问

某些音频在隐写工作结束后，会直接导致音频崩坏，变为杂音，听不出任何源文件的样子，到底是在什么样的过程中出了问题？