按保护对象分类:主要可分为隐写术和水印技术等两大类。隐写术保护的是隐秘消息，水印技术的保护对象一般为载体。例如用于版权保护的鲁棒水印，用于保护数据完整性的易损水印等。

一种简单的替换思想就是用隐藏信息位替换载体中的一些最不重要位 (Least Significant Bit, LSB) ，只有知道隐藏信息嵌入的位置才能提取信息。比如说，若捏一个灰度圈像的某个像素点的灰度值由 180 变成 182，人一般没有察觉不出变化。，但其鲁棒性较差。对载体的较小的扰动，如有损压缩，都有可能导致整个信息的丢失。

因此，目前的多数信息隐藏方法都采用了变换域技术，即把待隐藏的信息嵌入到载体的一个变换空间(如频域)中。与空域方法相比，变换域方法的优点如下:

* 在变换域中嵌入的信号能量可以分布到空域的所有像素上。
* 在变换域中，人的感知系统的某些掩蔽特性可以更方便地结合到编码过程中。
* 变换域方法可与数据压缩标准，如 JPEG 等兼容，常用的变换包括离散余弦变换

和小波变换，一般来说，变换域方法对诸如压缩，修剪和某些自像处理等的攻击

的鲁棒'性更强。

目前已有的方法，主要集中在小波变换，频率变换， DCT 变换等等。

①空域算法 z 该类算法中典型的算法是将信息嵌入到随机选择的图像点中最不重

要的像素位 (LSB) 上，这可保证嵌入的水印是不可见的。 LSB 算法的主要优点是可以

实现高容量和较好的不可见性，但是该算法的鲁棒性差，容易被第三方发现和得到，遭

到破坏，对图像的各种操作如压缩，剪切等都会使算法的可靠性受到影响。为了增强算

法的性能，提出了各种改进的方法，如利用伪随机序列，以随机的顺序修改菌像的 LSB;

在使用密钥的情况下，才能得到正确的嵌入序列。另外一个常用方法是利用像素的统计

特征将信息嵌入像素的亮度值中。

② Patchwork 算法:该算法是随机选择N对像素点 Cai ， bD ，然后将每个a1点的亮

度值加1，每个 bi 点的亮度值减1，这样整个图像的平均亮度保持不变。适当地调整参

数， Patchwork 方法对 JPEG 压缩、 FIR 滤波以及商像裁剪有一定的抵抗力（因为点是随机选取的），但该方法嵌入的信息量有限。为了嵌入更多的水印信息，可以将图像分块，然后对每一个图像块进行嵌入操作。

③频域算法:该类算法中，大部分算法采用了扩展频谱通信 ( spread spectrum

communication) 技术。算法实现过程为:先计算图像的离散余弦变换 (DCT) ，然后将

水印叠加到 DCT 域中幅值最大的前 k 系数上(不包括直流分量)，通常为图像的低频分

量。若 DCT 系数的前 k 个最大分量表示为 D ={ di} , i=l,…, k，水印是服从高斯分布

的随机实数序列 W={wi} ， i=l,…, k，那么水印的嵌入算法为 di=di (1+awi) ，其中常数 a 为尺度因子，控制水印添加的强度。然后用新的系数做反变换得到水印图像 I。解码函数则分别计算原始图像 I 和水印图像 I\*的离散余弦变换，并提取嵌入的水印 W\* ,再做相关检验以确定水印的存在与否。该方法即使当水印围像经过一些通用的几何变形和信号处理操作而产生比较明显的变形后仍然能够提取出一个可信赖的水印拷贝。一个简单改进是不将水印嵌入到 DCT 域的低频分量上，而是嵌入到中频分量上以调节水印的健壮性与不可见性之间的矛盾。

另外，还可以将数字图像的空间域数据通过离散傅里叶变换 (DFT) 或离散小波变

换 (DWT) 转化为相应的频域系数:其次，根据待隐藏的信息类型，对其进行适当编码

或变形:再次，根据睡藏信息量的大小和其相应的安全目标，选择某些类型的频域系数

序列(如高频或中频或低频);再次，确定某种规则或算法，用待隐藏的信息的相应数据

去修改前面选定的频域系数序列;最后，将数字图像的频域系数经相应的反变换转化为

空间域数据。该类算法的隐藏和提取信息操作复杂，隐藏信息量不可能很大，但抗攻击

能力强，很适合于数字作品版权保护的数字水印技术中。

④压缩域算法:基于 JPEG、 MPEG 标准的压缩域数字水印系统不仅节省了大量的

完全解码和重新编码过程，而且在数字电视广播及 VOD (Video on Demand) 中有很大

的实用价值。相应地，水印检测与提取也可直接在压缩域数据中进行。下面介绍一种针

对 MPEG-2 压缩视频数据流的数字水印方案。虽然 MPEG-2 数据流语法允许把用户数据

加到数据流中，但是这种方案并不适合数字水印技术，因为用户数据可以简单地从数据

流中去掉，同时，在 MPEG-2 编码视频数据流中增加用户数据会加大位率，使之不适于

固定带宽的应用，所以关键是如何把水印信号加到数据信号中，即加入到表示视频帧的

数据流中。对于输入的MPEG-2 数据流而言，它可分为数据头信息、运动向量(用于运

动补偿)和 DCT 编码信号块 3 部分，在方案中只有 MPEG-2 数据流最后一部分数据被

玫变，其原理是，首先对 DCT 编码数据块中每一输入的 Huffman 码进行解码和逆量化，

以得到当前数据块的一个 DCT 系数:其次，把相应水印信号块的变换系数与之相加，

从而得到水印叠加的 DCT 系数，再重新进行量化和 Huffman 编码，最后对新的 Huffman码字的位数 n1 与原来的无水印系数的码字 n0 进行比较，只在 n1 不大于n0的时候，才能传输水印码字，否则传输原码字，这就保证了不增视频数据流位率。该方法有一个问题值得考虑，即水印信号的引入是一种引起降质的误差信号，市基于运动补偿的编码方案会将一个误差扩散和累积起来，为解决此问题，该算法采取了漂移补偿的方案来抵消因水印信号的引入所引起的视觉变形。

⑤ NEC 算法:该算法由 NEC 实验室的 Cox 等人提出，该算法在数字水印算法中占

有重要地位，其实现方法是，首先以密钥为种子来产生伪随机序列，该序列具有高斯 N

(0, 1)分布，密钥一般由作者的标识码和Iæ像的哈希值组成，其次对图像做 DCT 变换，

最后用伪随机高斯序列来调制(叠加)该图像除直流 (DC) 分量外的 1000 个最大的 DCT

系数。该算法具有较强的鲁棒性、安全性、透明性等。由于采用特殊的密钥，因此可防

止 IBM 攻击，而且该算法还提出了增强水印鲁棒性和抗攻击算法的重要原则，即水印信

号应该嵌入源数据中对人感觉最重要的部分"这种水印信号由独立同分布随机实数序列

构成，旦该实数序列应该具有高斯分布 N (0, 1)的特征。

⑥生理模型算法:人的生理模型包括人类视觉系统 HVS (Human Visual System)

和人类昕觉系统 HAS。该模型不仅被多媒体数据压缩系统利用，闰样可以供数字水印系

统利用。利用视觉模壁的基本思想均是利用从视觉模型导出的 JND (Just Noticeable

Difference) 措述来确定在自像的各个部分所能容忍的数字水印信号的最大强度，从而能

避免破坏视觉质量。也就是说，利用视觉模型来确定与周像相关的调制掩模，然后再利

用其来插入水印。这一方法同时具有好的透明性和强健性。

隐写：

binwalk 7z.exe show file in this binary file

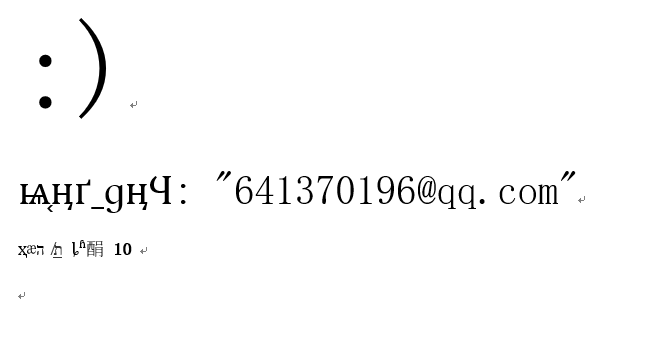
binwalk -c 7z.exe get inner file in this

用StegSolve(基于Java开发的流行图片隐写分析软件)打开图片，浏览图片各个颜色通道，发现Blue plane 0通道时图片左上角突然多了一些内容，应该就是隐藏的二进制信息。所以使用StegSolve中Analyse选项下Data Extract功能查看Blue plane 0通道。如果图片的灰色通道有特殊信息，或者图片就是灰度图像，那么你用py得到01序列，然后视为二进制（有编码转换器或者放到WinHex等）没准就可以得到你想要的隐写内容。

音频：

打开之后播放几次没有听出什么异常，然后分析一波，既然是基于提示是语音认证，那么解题方向应该不是数字隐藏（应该是指在里面藏文件或者其他内容），然后试着改变音频轨道和效果，分析音频频谱，也没有发现什么，之后观察音频波形，发现波形很有规律，总共就两种波形，刚好对应二进制01。

txt改成word： 里面的笔记变成这个



raspistill -w 800 -h 600 -tl 0 -t 0 -o - | tee -a %d.jpeg > /dev/null

通过tee不断向原图片中追加，却还能按照正常的图片进行显示。

winhex使用指南：

搜索有好几种，不要使用C-F快捷键，自己点工具栏中的Search，按F3搜索下一个。

PE文件的最后一个段后面是可以添加附加数据（称之为overlay），实际应用：软件要处理一些数据流文件，这些数据文件被单独的保存在硬盘上，当我们使用notepad的打开功能的时候，就可以去读取数据文件了。如果将这些需要读取的数据放到pe文件的后面，让程序自动的运行打开的功能，而不需要打开操作。如果数据不在PE的区段中，代码执行时就不会从磁盘被映射到内存，就是说如果在文件中存在不在区段里面的数据，这部分数据就被认为是附加数据(overlay). overlay是不映射到内存的，他将被程序以打开自己的方式来读取数据。通过PEID查壳可以查出来是否在末尾包含overlay。