# 隐写术

隐写术是关于信息隐藏,即不让计划的接收者之外的任何人知道信息的传递事件（而不只是信息的内容）的一门技巧与科学。隐写术英文作“Steganography”，来源于约翰尼斯·特里特米乌斯一本看上去是有关黑魔法，实际上是讲密码学与隐写术的一本书 Steganographia 中。此书书名来源于希腊语，意为“隐秘书写”。

有两种办法可用来隐藏明文信息。隐写术，它可以隐藏信息的存在；而密码学则是通过对文本信息的不同转换而实现信息的对外不可读。

## 隐写术

字符标记 :选择一些印刷字母或打字机打出的文本,用铅笔在其上书写一遍。这些标记需要做得在一般场合下辨识不出，除非将纸张按某个角度对着亮光看。

不可见墨水 :有些物质用来书写后不留下可见痕迹,除非加热或加之以某种化学物质。

针刺 :在某些字母上刺上小的针孔,这一般是分辨不出来的,除非对着光线。

打字机的色带校正 :用黑色的色带在行之间打印。用这种色带打印后的东西只有在强光下可见。

用 CD 每一帧的最后一位来隐藏信息：例如，柯达 CD 格式的最大分辨率是 3096×6144，其中每一个像素包含有 24 位的 RGB 颜色信息。改动这 24 位像素的最低一位对整个画质影响不大。结果是你可以在每张数字快照中隐藏 130KB 的信息。

## 隐写术的优缺点：

需要许多额外的付出来隐藏相对较少的信息。

尽管采用一些诸如上述方案也许很有效；但是一旦被破解，整个方案就毫无价值。(改进：具体的加入方法由秘钥决定；先加密再隐写)

隐写术适合：通信双方宁愿内容丢失，也不愿意它们进行秘密通信的事物被人发现。加密标志信息也是重要和秘密的，通过它可以找出想进行消息隐藏的发送方或接收方。

弗兰西斯·培根提出过一种隐藏消息的方法。

来自现代实践的一个例子

掩饰文本相对隐秘文本的大小（指数据含量，以比特计）越大，隐藏后者就越加容易。

因为这个原因，数字图像（包含有大量的数据）在因特网和其他传媒上被广泛用于隐藏消息。这种方法使用的广泛程度无从查考。例如：一个 24 位的位图中的每个象素的三个颜色分量（红，绿和蓝）各使用 8 个比特来表示。如果我们只考虑蓝色的话，就是说有 2^8 种不同的数值来表示深浅不同的蓝色。而像 11111111 和 11111110 这两个值所表示的蓝色，人眼几乎无法区分。因此，这个最低有效位就可以被(在某种程度上检测不到地)用来存储颜色之外的某些信息。如果我们对红色和绿色进行同样的工作的话，我们可以在（差一点不到）三个的像素中存储一个字节的信息。

更正式一点地说，使隐写的信息难以探测的，也就是保证“有效载荷”（需要被隐蔽的信号）对“载波”（即原始的信号）的调制对载波的影响看起来（理

想状况下甚至在统计上）可以忽略。这就是说，这种改变应该无法与载波中的噪声加以区别。

（从信息论的观点来看，这就是说信道的容量必须大于传输“表面上”的信号的需求。这就叫做信道的冗余。对于一幅数字图像，这种冗余可能是成像单元的噪声；对于数字音频，可能是录音或者放大设备所产生的噪声。任何有着模拟放大级的系统都会有所谓的热噪声（或称“1/f”噪声)，这可以用作掩饰。另外，有损压缩技术（如 JPEG）会在解压后的数据中引入一些误差，利用这些误差作隐写术用途也是可能的。）

隐写术也可以用作数字水印，这里一条消息（往往只是一个标识符）被隐藏到一幅图像中，使得其来源能够被跟踪或校验。实际上在日本，“……内容标识符论坛和日本数字内容协会已经开始试验一套数字水印系统来‘防止盗版’（日本时报在线，2001 年 8 月 26 日）。”

## 隐写术的研究与应用

近几年来,隐写术领域已经成为了信息安全的焦点。因为每个 Web 站点都依赖多媒体,如音频、视频和图像。隐写术这项技术可以将秘密信息嵌入到数字媒介中而不损坏它的载体的质量。第三方既觉察不到秘密信息的存在,也不知道存在秘密信息。因此密钥、数字签名和私密信息都可以在开放的环境(如 Internet,或者内联网)中安全的传送。

## 工具：

（1）Stegsolve 图片分析软件： 用于分析图片，图片是由各种不同颜色的像素点构成的（涉及 LSB 等图片图形学内容，感兴趣的可以自己去查），这个工具可以很容易的把不同颜色通道的图片信息显示出来。

（2） 二维码扫描： 在图片隐写中，扫描二维码得到答案的题目是比较常见的，但是有时候扫描之后出现的也不一定是最后答案，往往需要我们进一步的去破解，所以用手机扫描注定不方便，有个电脑上的软件会方便很多。

（3）十六进制分析工具：与这个相同的还有 winhex，winhex 更常用，且功能更强大，想使用哪个看个人喜好。计算机的世界，所有的东西都是由 1 和 0 组成的，二进制也可以转成十六进制，所以利用这个工具可以看到构成图片的最原始的数据，同时可以找到隐藏在图片里的秘密。

4）binwalk:这是在 kali 下自带的一个命令行工具，可以用来分析目标文件里是否有夹带其他东西，这在除了隐写以外的其他类型的题也是常用的工具。命令：binwalk –n 加文件 。比如说一张图片里面隐藏了一个压缩包，从表面上你是看不出什么的。但是使用 binwalk 命令，就可以分析出来。同样，把图片丢到十六进制查看器里面也可以看出来，但是新手对这些不熟悉很容易出错。毕竟压缩文件除了 rar 还有 zip，又或许图片里面藏的是个 txt。

另外，分析之后我们需要把这附带的其他文件提取出来，这就需要另外的一个命令，

binwalk –e 加文件。同样可以使用十六进制查看器，通过分离切割来得到，有兴趣的同样可以自己试试。

（5）PS:这个东西大家肯定不会陌生，有关图片隐写，ps 有时候会用到，但几率不大。因为前面介绍的几种工具基本已经够用了，ps 无非也就是有更进一步的能力而已。与 ps 相应的还有一个叫做 FW 的工具，也是 Adobe 系列的。要是一张图片真的什么都分析不出来，丢到 PS 里，说不定就会发现惊喜了，但是这样的题至今我也只遇过三题，其中两题都是跟 FW 有关的。

（6）密码学：这就涉及到一个很大的方面了。有时候我们找到了图片里面藏的密码，但是出题人不会很直白的告诉我们答案，就会进行加密。常见的密码有 md5,base64，当然还有各种各样奇怪的密码。不过野不用着急，这都是一个积累的过程，先去了解 md5 和 base64 的特征，然后拿解到的密码去网上搜索。大部分常见的密码类型网上都有在线解码网站

二、一些经验技巧：我一直认为看再多的东西都不如实际做几题来的印象深刻，不然很多东西都是看了就忘的。但是一些经验技巧也可以让后面学习的人少走些弯路（PS:这些都是我以前做题的时候总结的，也许不一定都是对的，毕竟接触这块还不是很久，还有很多地方要学习的，但是也可以参考一下，找到自己的一个做题思路才是最重要的）

（1）一般拿到一张图片，先看图片格式。常见的有 JPG，PNG 和 BMP。JPG 比起 PNG，是有过压缩的图片，所以 JPG 格式的图片通常是没必要放到图片分析器里去看的。由于进过压缩，所以里面是不能放下二维码的。而我们使用图片分析器来分析图片，60%是为了找到里面隐藏的二维码。

（2）JPG 格式的图片通常里面都有藏着另外的东西，大体上是压缩文件之类的，当然，也有往里面放音频的……所以先丢去 binwalk 分析才是正确的。

（3）PNG 格式的图片首先就可以考虑藏二维码的问题了，不过也不是说他里面不会藏有其他文件哟。

（4）BMP 是位图文件,能放的东西就更多了，可以拿去 PS 里看一下，说不定在就出现了两个图层了。

（5）无格式的东西，图片隐写的题，出题人很喜欢绕一个弯。有时候下载下来的东西是没有后缀格式的，这时候需要手动去添加。丢到十六进制查看器里

去看它的头部十六进制，取前四个到百度搜一下就知道是什么格式了。同理，也有人会把头部文件给删除，这时候要靠他的后缀手动添加头部。这些都是在十六进制查看器里完成的。

（6）遇到音频的时候，音频也是可以藏东西的。一般是喜欢用 AU，当然也有其他比较专门的工具，可以自己去找找。查看音频的波形，有时候里面会藏有一段莫尔斯电码。