深入理解JPEG图像格式Jphide隐写

转载

Kelly_Young 于 2018-08-17 18:21:36 发布 2865 收藏 5

最近在看JPEG格式的LSB隐写，看到一篇很不错的博客。来自4ido10n's Blog文章《深入理解JPEG图像格式Jphide隐写》

0x00 隐写原理

Jphide是基于最低有效位LSB的JPEG格式图像隐写算法，使用JPEG图像作为载体是因为相比其他图像格式更不容易发现隐藏信息，因为JPEG图像在DCT变换域上进行隐藏比空间域隐藏更难检测，并且鲁棒性更强，同时Blowfish算法有较强的抗统计检测能力。

由于JPEG图像格式使用离散余弦变换（Discrete Cosine Transform，DCT）函数来压缩图像，而这个图像压缩方法的核心是：通过识别每个8×8像素块中相邻像素中的重复像素来减少显示图像所需的位数，并使用近似估算法降低其冗余度。因此，我们可以把DCT看作一个用于执行压缩的近似计算方法。因为丢失了部分数据，所以DCT是一种有损压缩（Loss Compression）技术，但一般不会影响图像的视觉效果。

0x01 隐写过程

Jphide隐写过程大致为：先解压压缩JPEG图像，得到DCT系数；然后对隐藏信息用户给定的密码进行Blowfish加密；再利用Blowfish算法生成伪随机序列，并据此找到需要改变的DCT系数，将其末位变为需要隐藏的信息的值。最后把DCT系数重新压回成JPEG图片，下面是个人对隐写过程理解画出的大致流程图。

0x02 隐写实现

（1）Stegdetect

实现JPEG图像Jphide隐写算法工具有多个，比如由Neils Provos开发通过统计分析技术评估JPEG文件的DCT频率系数的隐写工具Stegdetect，它可以检测到通过JSteg、JPHide、OutGuess、Invisible Secrets、F5、appendX和Camouflage等这些隐写工具隐藏的信息，并且还具有基于字典暴力破解密码方法提取通过Jphide、outguess和jsteg-shell方式嵌入的隐藏信息。

（2）JPHS

而这里介绍另一款JPEG图像的信息隐藏软件JPHS，它是由Allan Latham开发设计实现在Windows和Linux系统平台针对有损压缩JPEG文件进行信息加密隐藏和探测提取的工具。软件里面主要包含了两个程序JPHIDE和JPSEEK， JPHIDE程序主要是实现将信息文件加密隐藏到JPEG图像功能，而JPSEEK程序主要实现从用JPHIDE程序加密隐藏得到的JPEG图像探测提取信息文件，Windows版本的JPHS里的JPHSWIN程序具有图形化操作界面且具备JPHIDE和JPSEEK的功能。

1.Windows用户请下载JPHS-05 for Windows,同时也提供下载Linux版本。

2.分别准备一个JPEG格式的图片（example.jpg）和一个文本文件（flag.txt）。

由于JPEG文件使用的数据存储方式有多种不能一一演示，这里用最常用的JPEG格式-JPEG文件交换格式（JPEG File Interchange Format，JFIF）作为示例。

这里简单介绍JPEG文件交换格式的JPEG图片的图像开始标记SOI（Start of Image）和应用程序保留标记APP0（Application 0），JPEG文件交换格式的JPEG图片开始前2个字节是图像开始标记为0xFFD8，之后2个字节接着便是应用程序保留标记为0xFFE0，应用程序保留标记APP0包含9个具体字段，这里介绍前三个字段，第一个字段是数据长度占2个字节，表示包括本字段但不包括标记代码的总长度，这里为10个字节，第二个字段是标识符占5个字节0x4A46494600表示“JFIF0”字符串，第三个字段是版本号占2个字节，这里是0X0101，表示JFIF的版本号为1.1，但也可能为其它数值，从而代表了其它版本号。

3.Windows版本可以使用具有图形化操作界面的Jphswin，选择“Open jpeg”打开示例JPEG格式图片example.jpg

如果你选择的不是JPEG格式的图片程序会自动退出，你可以16进制编辑器如Winhex查看图片的图像开始标记SOI和应用程序保留标记APP0，当载入JPEG格式图片会显示一些图片的属性。

4.选择“Hide”选项之后在两次文本框输入相同的密码，这里以输入flag作为密码为例，然后输入要包含隐藏信息的文本。

5.选择将要隐藏的信息如flag.txt。

6.选择“Save jpeg as”选项将图片另存为jpeg格式并输入文件的名称为新的图像文件如C4n-u-find-f14g.jpg。

7.之后便可以看到生成结果和相关信息。

8.第2步到第7步做的是Jhide方式信息隐藏，接下来我们从C4n-u-find-f14g.jpg图片提取出隐藏信息。

9.如果之前你并不知道图片是基于什么方式进行信息隐藏，你可以使用Stegdetect先进行探测。

Stegdetect的主要选项如下：

-q 仅显示可能包含隐藏内容的图像。

-n 启用检查JPEG文件头功能，以降低误报率。如果启用，所有带有批注区域的文件将被视为没有被嵌入信息。如果JPEG文件的JFIF标识符中的版本号不是1.1，则禁用OutGuess检测。

-s 修改检测算法的敏感度，该值的默认值为1。检测结果的匹配度与检测算法的敏感度成正比，算法敏感度的值越大，检测出的可疑文件包含敏感信息的可能性越大。

-d 打印带行号的调试信息。

-t 设置要检测哪些隐写工具（默认检测jopi），可设置的选项如下：

- j 检测图像中的信息是否是用jsteg嵌入的。
- o 检测图像中的信息是否是用outguess嵌入的。
- p 检测图像中的信息是否是用jphide嵌入的。
- i 检测图像中的信息是否是用invisible secrets嵌入的。

-V 显示软件版本号。

如果检测结果显示该文件可能包含隐藏信息，那么Stegdetect会在检测结果后面使用1～3颗星来标识隐藏信息存在的可能性大小，3颗星表示隐藏信息存在的可能性最大。

从下图可以看出很可能是Jphide的信息隐藏方式：

10.在知道隐藏方式之后可以开始进行信息提取，和使用JPHS进行信息隐藏过程类似，打开需要提取隐藏信息的图片C4n-u-find-f14g.jpg，输入对应密码（在不知道密码的情况不可以尝试Stegdetect工具里的Stegbreak程序进行基于字典的暴力攻击）flag，密码验证通过JPHS会自动提取隐藏信息，之后便可以另存提取出的信息。

11.打开提取得到的find.txt便可以得到我们想要的隐藏信息。

0x03 参考资料

Jphide原理剖析及检测

基于二次加密的JPhide隐写检测方法