【隐写术】F5隐写

原创

Em0s_Er1t 于 2021-05-18 13:10:25 发布 1614 收藏 4
分类专栏： Notes 文章标签： python 算法 java 安全
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/m0_46296905/article/details/116942784
版权

Notes 专栏收录该内容
12 篇文章 1 订阅
订阅专栏

这些天入门MISC，对隐写术产生了兴趣，想 了改 一下，顺便写个博客记录，主要讲解F5隐写的矩阵编码和隐写工具。
建议先阅读计算机图像显示原理与BMP图像文件格式，对计算机的图像显示有初步认识。

一、什么是隐写术

wiki：隐写术是一门关于信息隐藏的技巧与科学，所谓信息隐藏指的是不让除预期的接收者之外的任何人知晓信息的传递事件或者信息的内容。

为了方便理解wiki中关于隐写术的定义，现在举个关最简单的例子：一个24位图中8个bit的数据代表一个像素点，在这样的图片中，人眼是无法识别`11111111`和`11111110`所代表的蓝色的，最低有效位（`LSB`）就可以被用来存储其他我们想保密的信息。

二、F5隐写

1.矩阵编码

矩阵编码的基本思想是用n位LSB表示k位信息（n>k），还是先从一个例子引入。如果要写入的原LSB是$a=a_1a_2a_3$（n==3），要写入的信息$x=x_1x_2$（k == 2），

> （这里的带下标的a和x都是值为0或1的二进制位，代表各个位上的对应值）

则让a的每两位异或得到的结构跟对应要写入的信息比对，不相等则修改LSB，相等则不改变。这个例子会导致下面四种情况：

- $x_1 == a_1 \hat{} a_3$，$x_2 == a_2 \hat{} a_3$，此时不做任何修改
- $x_1 != a_1 \hat{} a_3$ ，$x_2 == a_2 \hat{} a_3$，此时修改a_1
- $x_1 == a_1 \hat{} a_3$，$x_2 != a_2 \hat{} a_3$，此时修改a_2
- $x_1 != a_1 \hat{} a_3$ ，$x_2 != a_2 \hat{} a_3$，此时修改a_3

由于二进制的异或运算的特性可以发现，这个例子里最多只要更改1位就可以达成数据嵌入的效果。

最大更改位数 d_{max} 的不同代表着不同的编码方式，毫无疑问， d_{max}取值不同使n和k的关系不同。每种编码方式都可以用有序数组（d_{max}，n，k）表示，而对于F5隐写，采用的矩阵编码是属于d_{max} == 1，即（1，n，k）的编码方式，此时n和k满足$n ==2^k - 1$。

（1）嵌入

那么对于n位LSB和k位信息，我们也可以根据以上的例子推测出来通用形式了，下面给出具体的F5隐写的矩阵编码。(忽略了一开始的格式校验步骤等等)

根据待嵌入消息`x`的长度就算出`n`和`k`。

将待嵌入消息`x`分组，`k`个消息为一组，每一组写入`n`个LSB。

`n`和`k`满足关系$n=2^k-1$，即`k`位信息嵌入`n`位LSB。

$a=a_1a_2a_3……a_n$是嵌入之前原LSB组成的`n`位二进制数据，计算散列函数`f(a)`，

> **计算散列函数f(a)：**
> 第`i`项表示为$a_i * i$，i从1开始到n每一项异或相加得到散列函数`f(a)`值
>
> $$f(a)=\oplus_{i=1}^{n} a_i \cdot i$$

计算要修改的是`a`的第几位，`y==x ^ f(a)`

如果用`a'`代表信息处理后的待嵌入LSB的码文，那么`a'`只会出现下面两种情况：

1. `a'==a`，此时y==0，无需修改任何位。
2. `a'!=a`，此时y!=0，`a`和`a'`只有从左往右第`y`个二进制位不同（d_{max}==1），则将第`y`个二进制数取反 修改即嵌入成功。

进入下一组`k`位消息的嵌入。

（2）提取

提取的话很容易，关键看下面的推导公式

$$f(a') = \oplus_{i \neq y} a_i i \oplus \bar{a}_y y =$$
$$\oplus_{i \neq y} a_i i \oplus (1 \oplus a_y)(x \oplus f(a)) =$$
$$\oplus_{i \neq y} a_i i \oplus x \oplus f(a) \oplus a_y y = x$$

也就是说只要提取出`a'`，然后进行`f(a')`运算就可以得到信息了

2.隐写工具

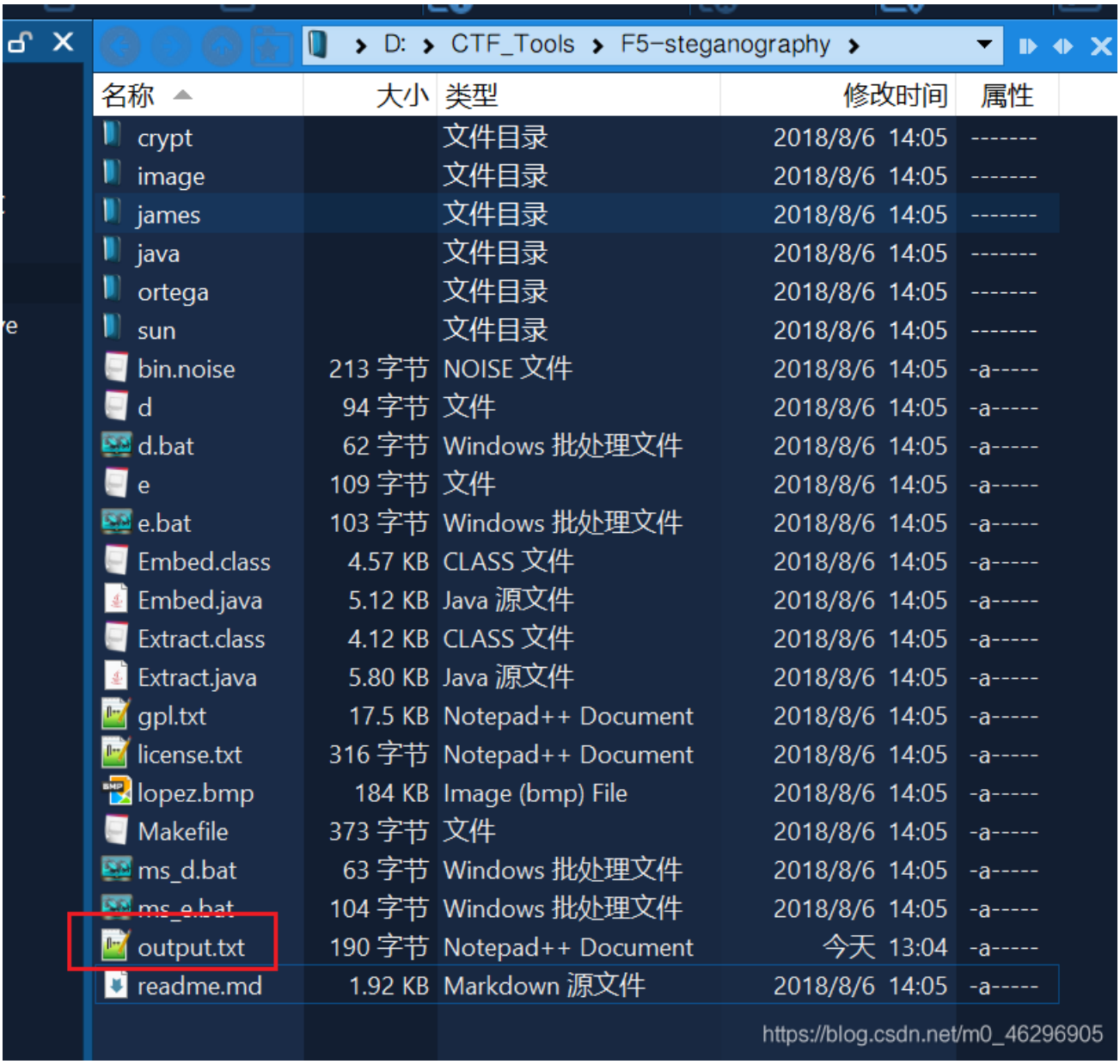
安利一下，https://github.com/matthewgao/F5-steganography

（1）使用

cd到安装目录下命令行输入

```
java Extract “待提取的图片路径”
```

最后在安装目录下会生成一个output文件，这就是提取出的文件，举例如下。



【参考：

- https://xueshu.baidu.com/usercenter/paper/show?paperid=b15b8bd5deef65cfa827b9a9a254458c&site=xueshu_se】