信息隐藏隐写系统框架

原创

Fasthand_ 于 2020-01-29 21:34:13 发布 1594 收藏 3
分类专栏： 隐写 文章标签： 数据安全 信息安全 安全 其他 算法

本文链接：https://blog.csdn.net/qq_43390703/article/details/104105419

信息隐藏中隐写是其中很重要的一部分。本文通过一段时间的CTF的学习结合个人CTF比赛杂项选手的刷题经历总结。对一部分自己所学过的隐写进行系统的概括。

隐写

隐写相关概念

定义

隐写分析（steganalysis）技术是对表面正常的图像、音频、视频等媒体信号进行检测，判断其中是否嵌有秘密信息，甚至是指出媒体中存在秘密信息的可能性，这样就可以找到敌对隐蔽通信的信源，从而阻断隐蔽通信的信通。

分类

从攻击的角度，我们用阐述隐写术的“囚犯”问题对隐写术进行分类。

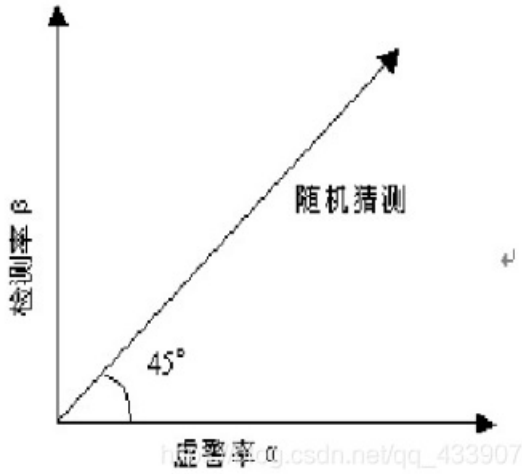
1、被动攻击
看守人员持有囚犯传递的信件。简单来讲就是不对信息内容进行破坏、修改仅是对文件进行分析，与原始媒体进行对比分析，在已知敌方所使用的隐写工具和隐写内容的情况下对待检测载体进行检测或者仅持有隐写载体对象而对隐写算法完全不知的盲分析（难）。

2、主动攻击
又称积极攻击。看守不经过判断分析就对信息进行修改。对媒体信息进行某种处理，使得媒体的使用不受影响但是干扰其中的秘密信息或造成尽可能的损伤。

3、其他
除了被动攻击与主动攻击，隐写分析还包括估计嵌入信息量的多少，秘密信息的存在性，提取秘密信息以及在位置隐写算法和密钥的情况下如何解决隐写分析处理等。

隐写分析评价指标

1、准确性
隐写分析最重要的一个评价指标。一般采用虚警率（把非隐藏信息误判位隐藏信息的概率）和检测率（把隐藏信息正确判为隐藏信息）表示，两个指标可以描绘成一个二维平面。检测率相关还有一个漏报率，即把隐藏信息判为非隐藏信息的概率。



隐写分析要求在尽量减少虚警率和漏报率的前提下取得最佳检测率，在几个指标无法兼顾的时候首先减少漏报率。

$$P_e = (1-\beta)P(\text{隐藏信息}) + \alpha P(\text{非隐藏信息}) = \eta P(\text{隐藏信息}) + \alpha P(\text{隐藏信息})$$

平均错误概率：
全局检测率=1-平均错误率

B为检测率，a为虚警率。n为漏报率。（希腊文字母。。形似代替吧。。）
如果a=B，即（a,B）在上图的对角线上，全局检测率为50%属于随机猜测（瞎猜/。/）。当全局检测率高于85%看作检测性能良好。

2、适用性
指检测算法能进行多少种检测，多少类隐写算法或嵌入算法。

3、实用性
指由现实条件是否允许其稳定产生检测结果、自动化程度、实时性（分析用时）等衡量。

4.复杂度
针对隐写分析算法本身，可以由隐写分析实现需要的资源开销，软硬件条件等来衡量。

以上指标并没有十分科学的定量，只能根据实际效果等进行得到一个相对结论。

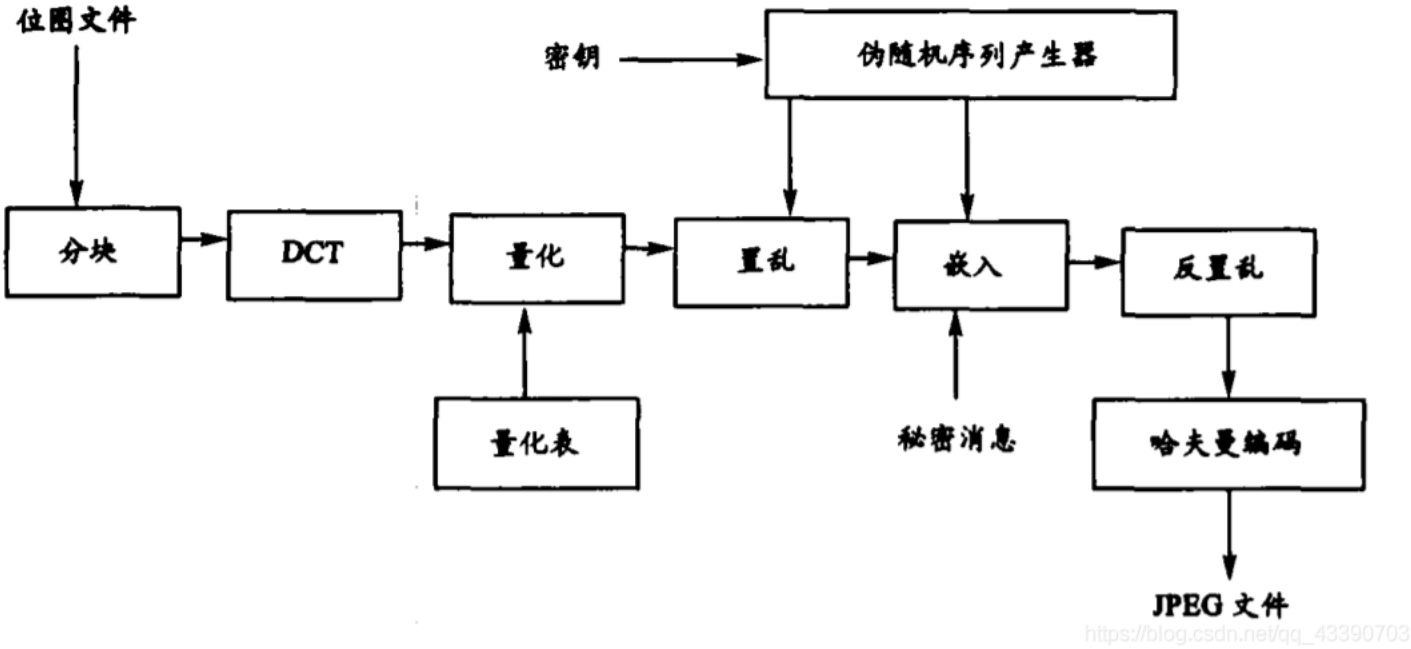
F5隐写算法

F5算法隐写

F5是由德国著名学者Pfitzmann和Westfeld在2001年提出的一种隐写分析方法，是一种只针对JPEG图像，可以提供较大的嵌入容量、抗卡方分析检测的隐写算法。

F5算法论文详细介绍
F5算法源码
DCT变换

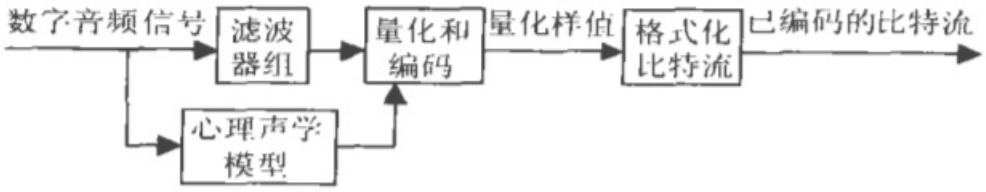
不想看论文没关系，我简要的描述一下F5算法的原理：
为什么F5隐写算法只对jpeg图像可行呢？



上图是F5算法实现的流程，对于jpeg的存储过程中，首先要对jpeg图像进行分块，在对每块内容进行DCT变换，之后进行一个量化过程再此之后将隐写的秘密嵌入量化后的非零的DCT系数当中。这就解释了整个F5算法的逻辑以及为什么只是用与jpeg图像当中。

MP3信息隐写

MP3隐写简单介绍



一般的音频文件如果能以有损的形式进行4：1压缩便很不错了，但是MP3格式却可以在保持相当不错的音质效果的前提下达到12：1的压缩效果。其过程为上图。
首先MP3音频通过滤波器组和MDCT变化完成时域信号转换为频域信号，同时经过心理声学模型，根据人耳的特性产生掩蔽阈值用于压缩声音信号，最后用量化和编码模块来根据掩蔽值来对声音频域信号进行量化和编码，最后量化后的低比特率数据被格式化为MP3比特流。
其中编码实现MP3一个重要部分是两个嵌套的循环。
内循环：量化编码循环。哈夫曼编码使得结果比特数达到足够小。
外循环：噪声控制循环。根据屏蔽阈值对量化噪声进行控制。
数字音频的频域信号在量化和编码时，存在量化误差，这是一个不确定的值（采用不同的心理声学模型也会导致不同的量化误差），**并且这个量化误差如何取值可以在量化编码程序中进行调整设定**
MP3stego通过调节量化误差的大小，将量化和编码后的长度作为信息隐藏的方法（内循环中实现）：
1、长度为偶数代表信息0
2、长度为技术代码信息1
从而实现MP3比特流中隐藏信息。如果编码时不符合编码要求，重新进行调节量化误差再进行量化编码。

MDCT：改进离散余弦变换(Modified Discrete Cosine Transform)一种线性正交交叠变换。它使用了一种时域混叠抵消技术(TDAC)，包含50%的时域交叠窗，在不降低编码性能的情况下有效地克服加窗离散余弦变换(DCT)块处理运算中的边缘效应，从而有效地去除由边缘效应产生的周期化噪声，在相同编码率的情况下，MDCT性能优于DCT，广泛应用于语音、宽带音频和图像信号的变换编码中。MDCT本身计算量庞大，对于实时编解码系统，直接计算复杂度很难接受，其快速算法一类是基于FFT，另一类是基于DCT。
比特率：比特率是指每秒传送的比特(bit)数。单位为 bps(Bit Per Second)，比特率越高，每秒传送数据就越多，画质就越清晰。声音中的比特率是指将模拟声音信号转换成数字声音信号后，单位时间内的二进制数据量，是间接衡量音频质量的一个指标。 视频中的比特率（码率）原理与声音中的相同，都是指由模拟信号转换为数字信号后，单位时间内的二进制数据量

DCT算法

基于DCT域水印技术的图像信息隐藏方法研究。
改进目前许多图像隐形水印算法在嵌入强度和含水印图像的质量评价等方面存在的问题，设计了一个较完整的基于DCT域的图像隐形水印算法，使该算法较好地兼顾不可感知性、稳健性和安全性。
图像隐藏原理：先把原图像各8×8块按Hilbert扫描顺序排列, 然后在原图像分块的Hilbert序列中选取一块图像的DCT域的三个中频分量之间嵌入水印。嵌入水印具有很好的透明性，水印嵌入强度是与原图像特征相自适应的。同时，水印的提取无须求助于原图像。

MIDI信息隐藏

MIDI信息隐藏
MIDI文件结构：

类型	长度	数据
4个字节	4个字节	4个字节

每个Midi文件的开头都有如下内容，它们的十六进制代码为:“4d 54 68 64 00 00 00 06 ff ff nn nn dd dd”。
前四个是ASCII字符“MThd”是用来鉴别是否Midi文件，而随后的四个字节是指明文件头描述部分的字节数，它总是6，所以一定是“00 00 00 06”，以下是剩余部分的含义:

ff ff	指定Midi的格式	00 00单音轨 00 01多音轨，且同步。这是最常见的 00 02多音轨，但不同步
nn nn	指定轨道数	实际音轨数加上一个全局的音轨
dd dd	指定基本时间格式类型	类型1：定义一个四分音符的tick数，tick是MIDI中的最小时间单位 类型2：定义每秒中SMTPE帧的数量及每个SMTPE帧的tick

>头块之后剩下的文件部分是一个或多个音轨块，每一个音轨块如表所示：标识符串（4字节）：“MTrk”音轨块数据区长度（4字节）：单位为字节音轨块数据区：由多个MIDI事件构成表 MIDI音轨块格式每一个MIDI事件的构成：MIDI事件＝<MIDI消息>采用可变长编码，它决定了其后的MIDI消息被执行的时间。一个MIDI消息是由一个状态字节及多个数据字节构成。MIDI消息根据性质可分为通道消息（Channel Message）和系统消息（System Message）两大类。

通道消息是对单一的MIDI Channel起作用，其Channel是利用状态字节的低4位来表示，可从0到15共有16个channel。通道消息又分为声音消息和模式消息。声音消息用于控制合成器的声音产生。模式消息则为最多达16条通道分配声音关系，包括设定单音模式或复音模式等。
MIDI文件的声音消息有7种。

声音消息	功能描述	数字字节描述
80-8F	声音关闭	1字节：音符号； 2字节：音速

声音消息	功能描述	数字字节描述
90-9F	声音开启	1字节：音符号； 2字节：音速
A0-AF	音键压力	1字节：音符号； 2字节：键压力
B0-BF	控制变化	1字节：控制器号(0-121)；2字节：控制值
C0-CF	改变乐器	1字节：乐器编号
D0-DF	通道触动压力	1字节：压力
E0-EF	音调轮变化	1字节：弯音轮变换值的低字节 2字节：弯音轮变换值的高字节表

MIDI文件声音消息改变MIDI音乐文件的部分声音消息并不影响MIDI文件的听觉效果，通过实验，改变声音开启的最低位比特、乐器编号的最低位比特和通道触动压力的低4比特位，都不会引起听觉差异，因此可在这三种声音消息中嵌入水印信息。

HTML隐写

如{with,height}标记，是html做信息隐藏的关键。class标记和style标记谁放前放后对html页面是没有影响的，但是可以定义当class在前为0，class在后否为1，这样就定义了1 bit信息。本实验通过修改标记对的前后位置关系，对html文件做信息插入，达到隐藏的目的。一般会结合摩斯电码或者经过其他处理，再将处理后的内容在html中表达隐藏。

LSB低位隐写

对于LSB算法的研究十分丰富也存在很多很多改进的算法。
LSB算法运用广泛既可以在图像中使用可以适用于音频文件。
但是，LSB最本质的逻辑是很好理解的。
无论是图像还是音频原理都是相同的，都是将表达存储信息的低位部分进行篡改，达到隐藏自己想要隐藏的信息的目的，同时对原本文件的修改也不会产生很大的影响（人眼无法识别）。
分析LSB隐写工具：
图片工具（Stegsolve.jar）
音频工具 （S-tools）

图像信号处理信息隐藏

二维离散傅立叶、离散余弦和离散小波变换是图像信号常用基础操作，时域信号转换到不同变换域以后，会导致不同程度的能量集中，信息隐藏利用这个原理在变换域选择适当位置系数进行修改，嵌入信息，并确保图像信号经处理后感官质量无明显变化。
这个很复杂，后续慢慢补充。

结语

对于隐写这块的知识，只知道如何使用工具是很简单的，但是要真正理解每一个隐写算法的过程，能够系统的描述每个隐写算法的原理却是需要花费很多的时间和经历的，文章内容还没写完，后续的内容随着论文的阅读和实验的实操完善后再补充总结。越发的去窥看这个宽广的知识领域，越发的对这些算法的发现者油然而起一种敬佩感。
所以，虽然现在很菜，就更要不断向大佬们看起，新手一枚，水文一篇经不起推敲，有理解失误之处，欢迎各位大佬一起交流讨论。