

图像隐写技术简介（理论版）

原创

稻城亚丁比目鱼  已于 2022-04-08 14:18:13 修改  5842  收藏 1

分类专栏：[图像处理](#) 文章标签：[图像处理](#) [安全](#)

于 2022-03-26 16:06:23 首次发布

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/qq_48951688/article/details/123756464

版权



[图像处理](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

[目录](#)

1. 加密与隐写
2. 隐写术的分类
3. 图像隐写术中常见术语
4. 已有的隐写方案
5. 常见的隐写技术（手段）
6. 评价指标

加密技术与隐写术：

加密与隐写是信息保护最常用的手段之一。

加密中被保留的是加密文件，而隐写术中被保留的是秘密的存在载体，因此有学者认为隐写术比密码学更加安全。

隐写术的分类：

根据隐写操作载体的不同分为：

文本隐写术、

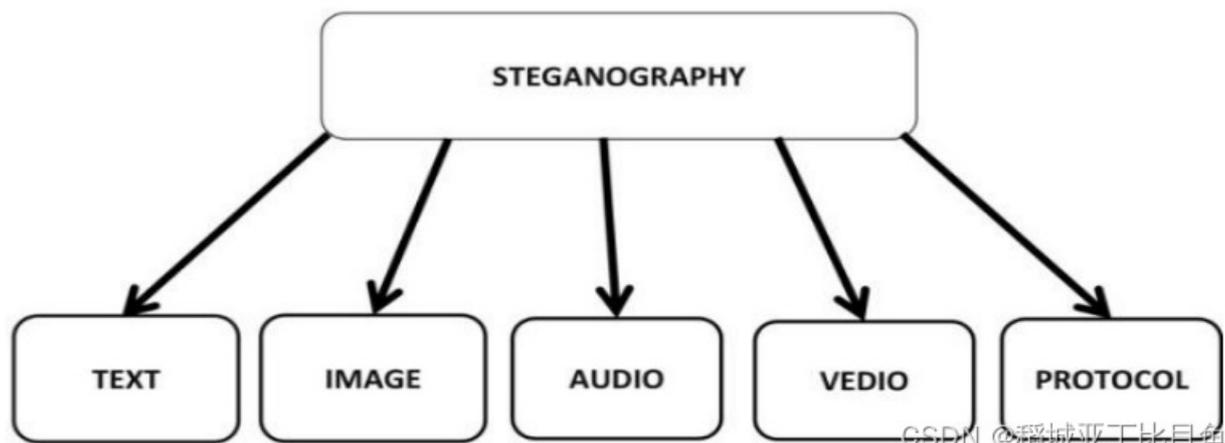
图像隐写术(最常见的技术：空间域、变换域、扩频、拼合等。图像域或者变换域内工作)、

音频隐写术（LSB编码，奇偶校验码、相位编码、扩频、回声隐藏）、

视频隐写术、

协议隐写术（TCP/IP网络协议被作为信息隐藏载体，秘密信息被隐藏在TCP/IP数据包头中）。

下图是隐写术分类图：



常见术语：

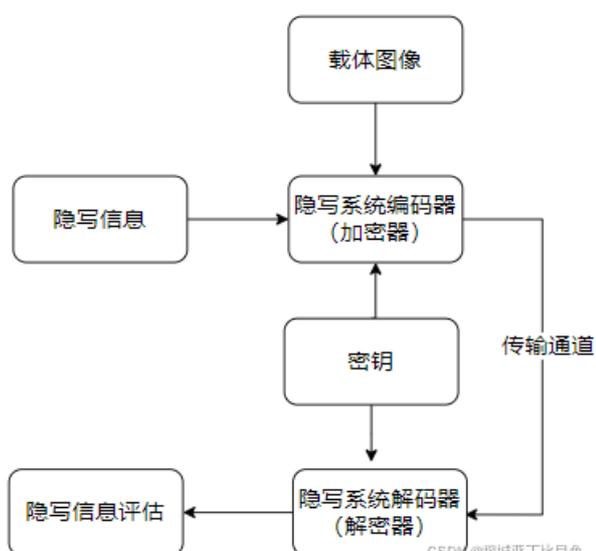
封面图像（载体图像）；

隐藏图像（嵌入原始信息之后产生的图像）；

信息（需要嵌入的文本，或者图像，密码等）；

隐藏密钥（起着嵌入与提取封面信息的密钥）。

下图是图像隐写示意图（其中载体是图像，隐写信息可以是文本、图像、视频、音频等）



已有的隐写思路：

LSB隐写算法：

LSB全称为 Least Significant Bit（最低有效位），是一种常被用做图片隐写的算法（在CTF中经常见到她的身影）。LSB属于空域算法中的一种，是将信息嵌入到图像点中像素位的最低位，以保证嵌入的信息是不可见的，但是由于使用了图像不重要的像素位，算法的鲁棒性差，水印信息很容易为滤波、图像量化、几何变形的操作破坏。

常见组合方案：

RSA算法对数据加密，LSB算法进行数据嵌入。

BlowFish算法加密，LSB算法进行数据嵌入。

MAES（修改后的AES算法）+LSB算法。

Huffman加密+LSB（分成4个片段）。

Hash+Canny边缘检测（文本数据隐藏在图像中）。

RSA加密解密+DiffieHellman算法（选定像素位置嵌入）。

RSA+增强LSB算法（增强LSB算法更好）。

AES+二维Harr离散小波变换（2-D HDWT）

阿诺德猫图（ACM）+倒置LSB。

AES+LSB+DCT（离散余弦变换）。

双异或（XOR）+LSB。

常见的隐写技术（手段）：

空间域：LSB，最小有效位变换。

安全性不高，隐写信息容易被压缩而丢失，信息直接隐写在像素强度中；

频域：离散余弦变换DCT、离散小波变换DWT、离散傅里叶变换DFT。

安全性好，隐蔽性强，信息无损失）：信息不是直接以像素强度隐藏在图像中，而是隐藏在像素系数中，常见图像格式是JPEG。

操作方法：扩频、拼凑、扭曲、屏蔽、过滤。

扩频：将秘密信息均匀分布在图像载体上（为了抵抗统计攻击）。

拼凑：利用冗余模式编码的统计方法（秘密信息通过冗余嵌入增加鲁棒性）。

扭曲（失真）：用来在信号失真中存储嵌入式信息。

屏蔽与过滤：通过标记图像来隐藏信息，与水印技术相似。

常见隐写术：

空间域中隐写术

最小有效位LSB

位图（BMP文件）中的LSB

图形交换格式（GIF文件）中的LSB

变换域（频域）中的图像隐写术

离散余弦变换DCT。

离散小波变换DWT。

离散傅里叶变换DFT。

隐写术的评价指标：

隐蔽性：至少因不被人眼发现。

有效隐写量：能隐藏多少数据。

统计攻击健壮性：要能抵抗统计分析攻击。

图像处理的稳定性：如裁剪图像/旋转图像情况下能否稳定。

独立的文件格式：最强大的隐写算法可在任何格式图像文件中隐写信息。

结束语：隐写术的隐写量、隐蔽性与鲁棒性不可兼得，此消彼长。此所谓，天之道，损有余而补不足。追求了A，定要失去B，与病毒的致死率、传染性、变异性一样，是一个不可兼得的三角法则。

所以中国一定能走出新型冠状病毒的影响，世界终究归于祥和。