隐写术基础

原创

唠嗑！ 已于 2022-04-04 19:47:50 修改 527 收藏 4
文章标签： 网络安全 学习 语音识别 深度学习 系统安全
于 2022-04-04 19:42:04 首次发布

本文链接：https://blog.csdn.net/forest_LL/article/details/123953611

目录

前言

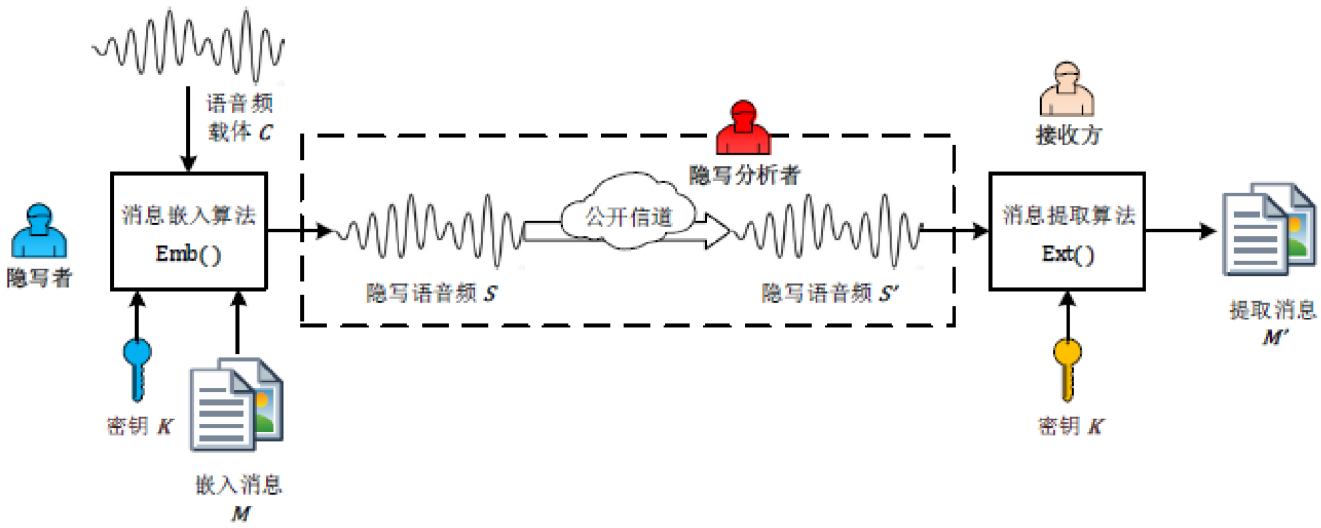
隐写术是一门关于信息隐藏的技巧与科学，所谓信息隐藏指的是不让第三者知晓信息的传递。隐写术的英文名叫做Steganography，起源于德国的一位修道士特里特米乌斯的著作《steganographia》。隐写技术提供对秘密信息存在性的保护，可以看成是一种保密通信技术和安全存储技术。数字隐写的载体包括音频、图像、视频、文本、网络包等等。

一. 隐写系统模型

音频隐写对抗模型包括三个实体和两个系统。

- 三个实体：隐写者、接收方和隐写分析者。隐写者和接收方利用隐写系统来传递信息。隐写分析者利用隐写分析系统来发现和检测隐写通信系统的存在性。
- 两个系统：隐写系统和隐写分析系统

隐写者可以看成信源，接收方可以看成信宿，密钥K可有可无，在传递时的公开信道可能是有损信道。系统模型图如下：



一个隐写系统S_0是由隐写者的消息嵌入算法和接收方的消息提取算法两部分组成。ϵ代表嵌入算法集合，D代表提取算法集合，如下：

$$S_0 = (\epsilon, D)$$

对任意的消息嵌入算法都一定有对应的消息提取算法，K代表隐写密钥，如下表达式：

$$\forall Emb_K \in \epsilon, \exists Ext_K \in D, s.t Emt_K = Emb_K^{-1}$$

利用M代表信息，C代表原始载体，s代表携带信息的隐秘载体，可得如下表达式：

$$\begin{cases} Emb(C, K, M) = S \\ Ext(S, K) = M \end{cases}$$

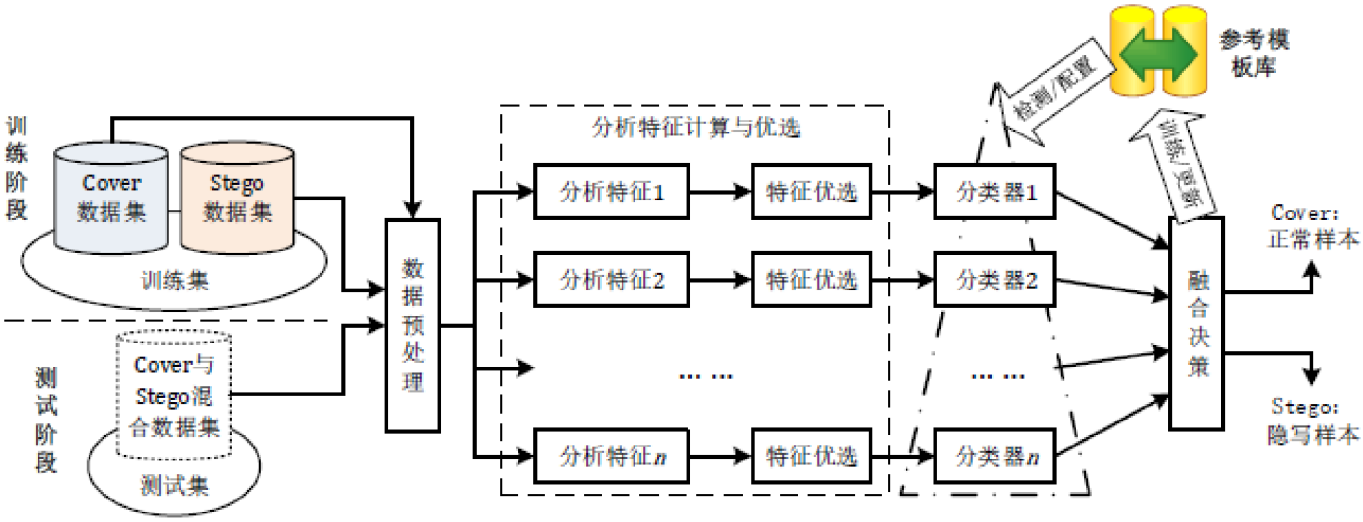
在有损信道下，如果$Ext(S', K) = M$依旧成立，则称S_0是鲁棒的。

二. 隐写分析系统模型

隐写分析系统S_a可利用统计分析特征来正确区分隐写样本S和正常样本C，本质上是一个分类检测器，如下表达式：

$$S_a(X) = \begin{cases} 0, & \text{if X is normal} \\ 1, & \text{if X is steganography} \end{cases}$$

目前隐写分析系统正从传统的机器学习方法往深度学习技术发展，即便如此，一个可投入应用的隐写分析系统少之又少，此领域有待发掘。当前隐写分析系统主要还停留在评测隐写算法的安全性上。隐写分析系统的主要流程如下：

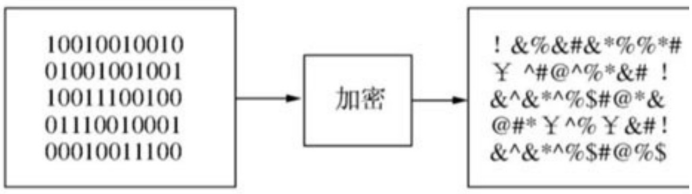


三. 对比隐写技术与密码技术

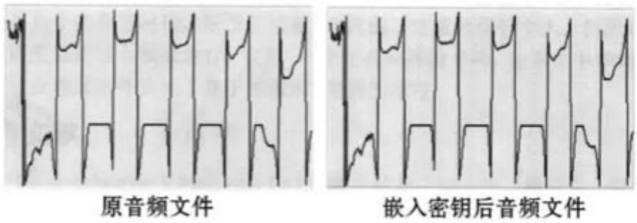
隐写技术总体上来看比密码系统更安全，但是由于密码技术的通信效率更高，所以目前生活中的加密主要还是使用密码技术。关于两者的对比可形成如下表格：

	隐写技术	密码技术
本质区别	保护通信双方进行秘密信息交换行为的事实，即保证通信的隐蔽性。安全层级更高	保护内容机密性、完整性和非否认性。攻击者无法获知数据的真实内容但能够知道其为加密数据或者通信双方采用了加密通信。
安全性评估	分析者使用充分多的检测器对载密样本和自然样本进行检测的结果等效于**随机猜测**，或者分析者的检测器无法区分是载密样本还是自然样本。其安全性的本质上是关于分类检测器的可靠性问题。基于隐写技术的数据保护需要数字媒体来提供隐蔽信道，因此隐写的安全等价于检测器对于**数字媒体统计特征改变的不可区分性。**	密码系统基于，到目前为止，不能够设计出比暴力搜索密钥更快的攻击方法，其应用通信的效率更高。
数学基础	隐写系统设计的安全性模型是基于数字信号的统计学理论。	密码系统设计的安全性模型是基于密钥或者某些公开的数学难题。

举例音频隐写与密码技术最直观的区别如下：

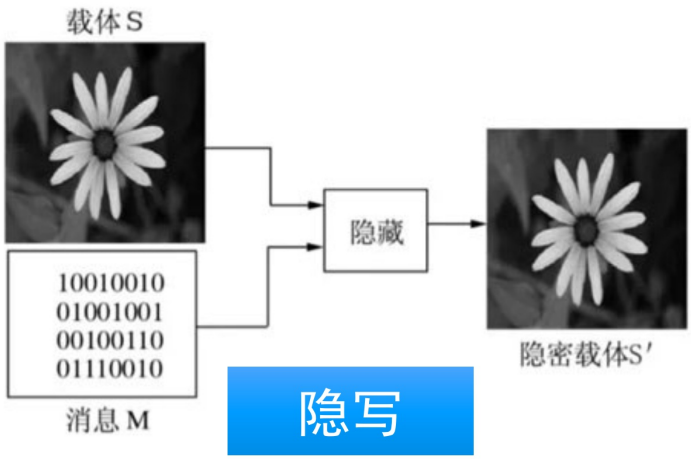


密码

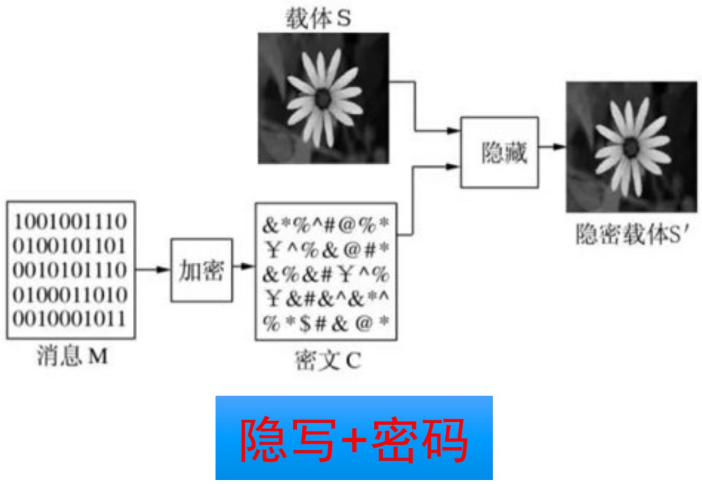


音频隐写

基于图片的隐写如下：



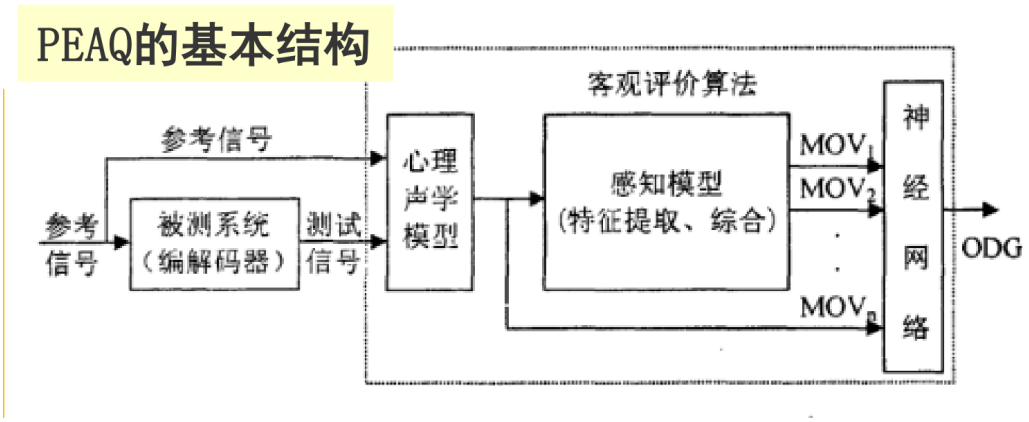
隐写也可以和密码系统结合起来进行使用，如下：



四. 隐写术的基本术语与概念

4.1 不可感知性

不可感知性又称之为感知透明性，指的是隐写后的载体在感知上与原始载体不存在差异。更专业一点就是，嵌入失真是不可感知的。也有一套客观度量的评价指标PEAQ，其基本结构可见下图：



PEAQ算法对参考信号和测试信号进行对比分析得出语音频质量的客观差异等级（ODG），ODG越大则嵌入失真越小，不可感知性越好。另一方面，主观上也有平均主观意见MOS。两者的质量等级图如下：

质量等级	Excellent（优）	Good（良）	Fair（中）	Poor（差）	Bad（劣）
ODG值	0	-1	-2	-3	-4
MOS值	5	4	3	2	1

4.2 安全性

安全性关注于统计不可检测性，是指隐写算法能够抵抗隐写分析攻击。从数学的角度，其度量指标可使用混沌矩阵来定义，包含检测正确率P_{ACC}和错误率P_e。利用P_{FA}代表虚警率，即假阳性率（False Positive Rate,FPR)；利用P_{MD}代表漏警率，即假阴性率（False Negative Rate,FNR)。数学关系式如下：

$$P_{ACC} = 1 - P_e = 1 - \frac{P_{FA} + P_{MD}}{2} = 1 - \frac{FPR + FNR}{2}$$

如果以坐标$(P_{FA}, 1 - P_{MD})$为点绘制接收者操作特征曲线（Receiver Operating Characteristic curve,ROC曲线），该曲线下的面积AUC(Area Under the Curve of ROC)值可展示其检测性能。具体来看AUC值越大表示分类检测器的正确率越高，检测性能越好。具体的规定指标如下：

> **从AUC 判断分类器（预测模型）优劣的标准：**
>
> - AUC = 1，是完美分类器。
> - AUC = [0.85, 0.95], 效果很好
> - AUC = [0.7, 0.85], 效果一般
> - AUC = [0.5, 0.7],效果较低，但用于预测股票已经很不错了
> - AUC = 0.5，跟随机猜测一样（例：丢铜板），模型没有预测价值。
> - AUC < 0.5，比随机猜测还差；但只要总是反预测而行，就优于随机猜测。

4.3 隐蔽性

隐蔽性包含了不可感知性和安全性，也是隐写系统的基本要求。从这个要求不难看出，隐写系统比密码系统的安全需要层级更高，密码是保护数据的机密性，而隐写系统需要保护数据的隐蔽性，通俗上讲就是保护通信行为不被检测。

4.4 鲁棒性

鲁棒性指的是载体在经过信息处理的操作后仍然能够正确提取隐藏信息，这里提到的信号处理操作就包含：**二次压缩**和**码率转码**。

利用M'代表提取信息，M代表嵌入信息，则隐写算法的鲁棒性可以用信息的比特误码率（BER)来度量，计算式子如下：

$$BER = \frac{\text{difference number bits between M and M'}}{\text{total number bits of M}}$$

如果BER=0，则表明隐写算法对操作是完全鲁棒的。

4.5 隐藏容量

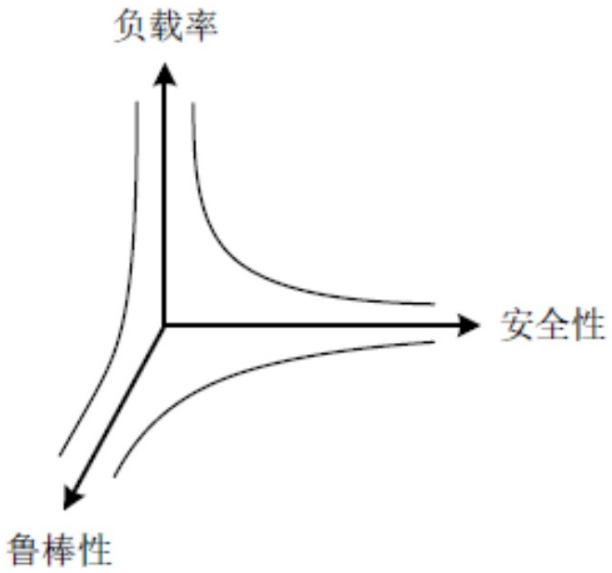
隐藏容量即负载，指的是隐藏消息的长度，通常用相对负载率来度量。严格意义上来讲，相对负载率（RPR)会受到不同嵌入域和嵌入方式的影响，为了统一表达形式，|M|代表隐藏消息的大小，|S|代表隐秘载体的大小，可以直观的用如下表达式：

$$RPR = \frac{|M|}{|S|} \times 100\%$$

性质：

> - 当增加隐写算法的嵌入负载率时，算法的安全性和鲁棒性会同时降低
> - 隐写算法的鲁棒性和安全性也是相对独立的，若增强算法的鲁棒性，即增强嵌入强度也会引入大量的噪声，继而降低算法的安全性

所以，当把负载率、安全性和鲁棒性之间的关系形成图像，如下：



4.6 嵌入效率

嵌入效率指的是每单位期望的嵌入失真条件下，隐藏的期望比特数。由于嵌入失真的计算形式较为复杂，此定义也可以简化为平均每次嵌入修改可隐藏的消息比特数，计算的公式如下：

$$e = \frac{\text{消息的总比特数}}{\text{嵌入修改的平均次数}} \quad (\text{比特/次})$$

嵌入效率通常由隐写算法的**基本嵌入编码**和**隐写码**等因素决定。

4.7 检测粒度

检测粒度是衡量隐写分析系统的性能指标。由于语音频文件是一种流式数据，时间可以很长，因此检测器需要按音频片段来进行检测，音频片段的长度就可以看成隐写分析器的检测粒度。

易得，若检测粒度过小，则统计特征不显著；若检测粒度过大，对检测器的计算性能要求更高，也会引入更多的噪声特征。种种这些因素都会直接地影响隐写分析器的性能。

总结

音频隐写的方法可分类为如下：