音频隐写术：分析剑桥大学提出的MP3Stego算法

原创

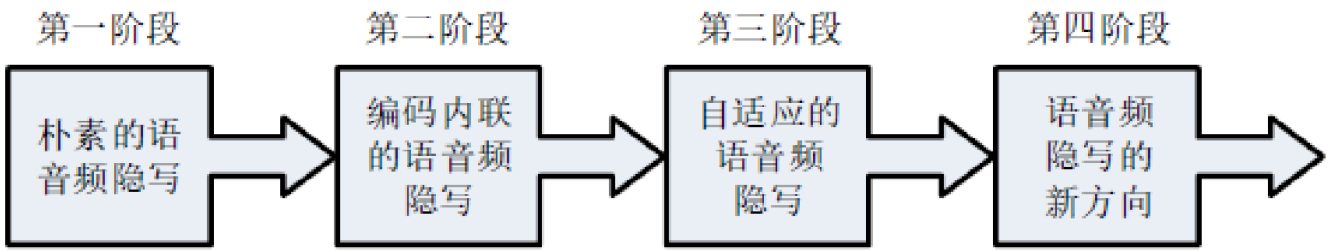
唠嗑！ 于 2022-04-05 16:22:41 发布 5010 收藏 2
文章标签： 算法 安全 语音识别 音视频 视频编解码

本文链接：https://blog.csdn.net/forest_LL/article/details/123960992

目录

前言

从信号处理的角度来看，隐写思想的本质就是将载密的噪声信号叠加到载体信号上，并且使得处理后的载体信号仍然保持**感知透明性**和**统计不可检测性**。音频隐写技术的发展经历了五个阶段：朴素的语音频隐写、编码内联的语音频隐写、自适应的语音频隐写和语音频隐写的新方向。如下图：



1. 朴素的语音频隐写阶段。第一阶段主要是解决语音频的听觉不可感知和隐藏容量等问题，使用的方法包括**时域的低有效位隐写**、**回声隐藏**、**相位编码隐藏**、**扩频隐写**，以及**变换域隐写**。
2. 编码内联的语音频隐写阶段。为了节省网络传输和存储的带宽，语音频数据一般会被压缩，所以需要保证隐藏的信息在语音频压缩后仍能被正确提取。此阶段主要解决基于编码内联的语音频隐写方法中**可行嵌入域**和**基本嵌入方式**等问题。
3. 自适应的语音频隐写阶段。此阶段主要解决自适应隐写框架、失真函数构造和隐写码等最优嵌入问题，从而提高隐写方

法的抗隐写分析能力。

4. 语音频隐写的新阶段。列举几个近些年来研究的新方向，比如适配有损信道的鲁棒隐写技术、针对网络语音频流的低时延快速隐写技术、基于人工智能的隐写技术、以及隐写协议设计和容错的隐写存储技术等。所有的这些研究新领域都将会促进完善隐写技术的体系和结构。

一. 语音频隐写分析

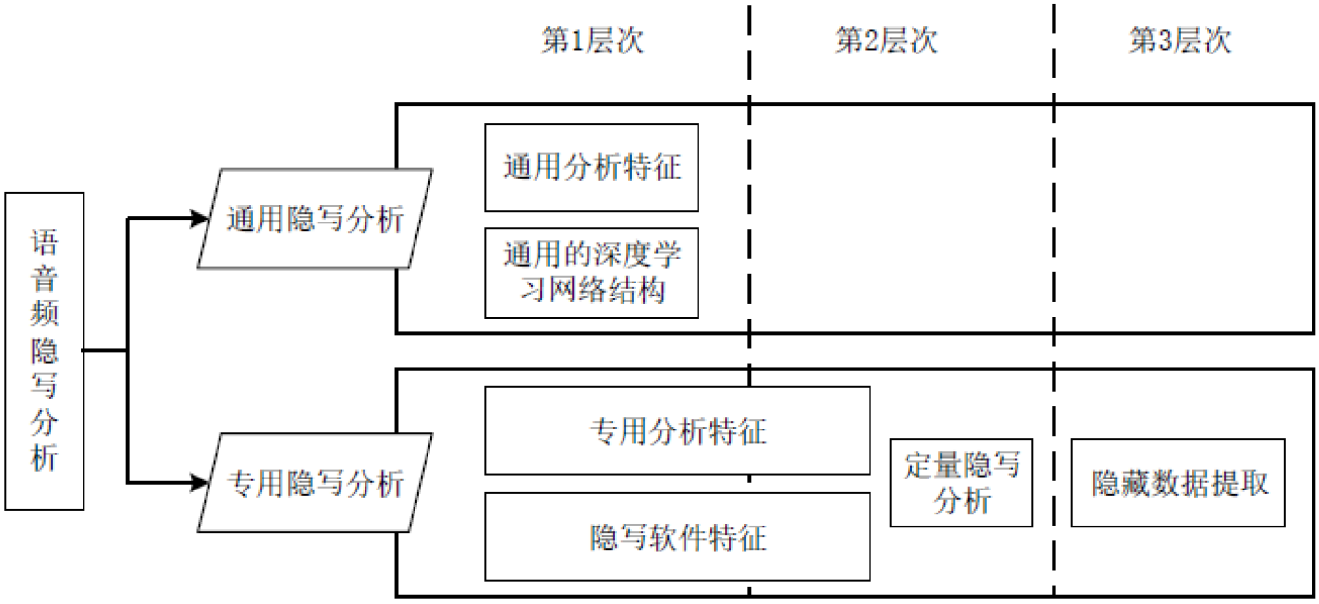
第三方截获者的分析系统有不同的分类方法，包含：两类和三层次。

两类包含：通用隐写分析和专用隐写分析。

三层次包含：

1. 第一层次：分析方法能正确判定隐写样本和正常样本
2. 第二层次：分析方法能够识别所采用的隐写算法或者估计隐写负载量
3. 第三层次：分析方法能够提取出隐藏数据，实现对隐写算法的完全破解

三个层次主要使用的技巧与方法可见下图：



二. 修改量化步长

量化和**熵编码**是音频编码的核心组件，基于量化步长修改方法本质是一种**内置式隐写**方法，通过调整量化步长大小或奇偶性来实现秘密信息的嵌入。

（1）普通的MP3Stego算法

最经典的基于量化步长修改的嵌入方法就是MP3Stego算法。此算法是剑桥大学计算机实验室安全组开发的针对MP3编码的隐写软件。简洁来看，就是在MP3编码的**内层循环**中实现秘密信息的嵌入，通过调节量化误差的大小，将量化编码后**Part23 块长度**part2_3_length的奇偶性作为隐秘消息嵌入的依据。

MP3Stego算法的嵌入过程类似编码的过程，具体步骤如下：

步骤1：使用量化步长q_s对MDCT系数量化后进行哈夫曼编码，计算哈夫曼码流中Part23块长度为part2_3__length。

步骤2：计算embedRule=(part2_3_length%2)□m，m代表当前待嵌入的消息比特。

步骤3：利用B_{max}代表最大可用比特数，如果embedRule=0且part2_3_length$\leq B_{max}$，则消息嵌入成功；否则，令$q_s = q_s + 1$并跳转执行步骤1。

优点：MP3Stego算法引入的隐写失真需要通过编码器的失真控制，所以该算法的不可感知性较好。

缺点：该算法隐写容量偏低，平均每帧只能隐藏2比特的消息；而且，如果在较低编码码率情况下（例如96Kbps以下），很容易导致编码器陷入死循环。

（2）改进后的MP3Stego算法

解决的主要思想为：将隐写的对象由块长度调整为量化步长，通过修改量化步长使得量化步长的**奇偶性**与**消息比特**相同。

改进后的MP3Stego算法的具体嵌入步骤如下：

步骤1：在嵌入操作之前，对原始秘密信息进行压缩去除冗余，并通过密钥对压缩后的秘密信息进行加密，获得压缩加密信息M(结合密码学）。

步骤2：令L_M代表M的长度，将L_M和M连接在一起，形成最终待嵌入的秘密信息S，即$S = L_M||M$。

步骤3：利用密钥产生伪随机序列产生器的种子，由伪随机序列产生器产生L_s个比特来选择需要进行隐藏的颗粒，其中L_s表示信息S的长度。

步骤4：输入一帧音频数据，其包含两个颗粒，对每个颗粒进行MDCT变换，得到576个MDCT系数。

步骤5：对MDCT系数进行量化。如果当前颗粒为不需要隐藏的颗粒，则使用常规的内循环结束条件；否则，在内循环中增加量化步长q_s，直到满足$embedRule = (q_s\%2) \bigoplus m = 0$且part2_3_length≤$B_{max}$，其中m代表S中一个待嵌入的比特。

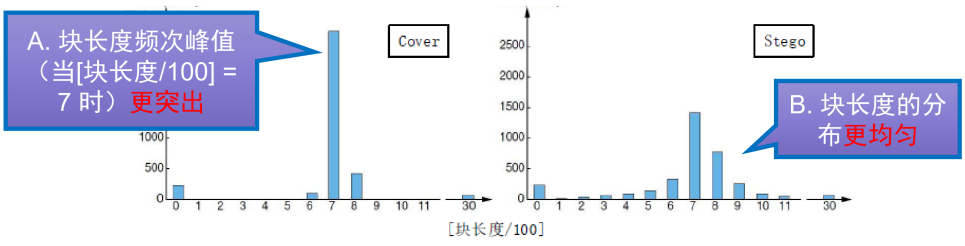
步骤6：不断重复操作步骤4和5，直到所有的颗粒均处理完毕。

三. MP3Stego算法分析

隐写算法的分析本质上就是寻找一些统计量或者统计分析特征，使得尽可能的区分正常样本和隐写样本。在MP3Stego算法分析中，主要关注四个方面：块长度part2_3_length的方差统计量、量化步长差分的方差统计量、边信息中main_data_begin值的均值统计量和大值区系数的方差统计量。

3.1 块长度part2_3_length的方法统计量

MP3Stego算法在隐写前后，part2_3_length的统计量是有很大差异的，如下图：



利用n代表统计块长度的总个数，x代表每个块长度的值。由此，块长度方差s^2的计算公式可得如下：

$$s^2 = \frac{\sum x^2 - \frac{1}{n}(\sum x)^2}{n-1}$$

分母处因为要表示无偏估计，所以使用n-1。

3.2 量化步长差分的方法统计量

量化步长是嵌入操作中被直接修改的一个重要参数，考察量化步长的差分统计量一共有三个步骤：

①利用q_i代表第i个颗粒的量化步长，N代表颗粒总数。由此可计算量化步长的一阶差分q_i'和二阶差分q_i''，如下：

$$q_i' = q_{i+1} - q_i \quad (i = 1, 2, \ldots, N-1)$$

$$q_i'' = q_{i+1}' - q_i' \quad (i = 1, 2, \ldots, N-2)$$

②利用$\bar{q_i'}$代表一阶差分序列的均值，$\bar{q_i''}$代表二阶差分序列的均值，可计算两者对应的标准差σ'和σ''，如下：

$$\sigma' = \sqrt{\frac{\sum_{i=1}^{N-1}(q_i' - \bar{q_i'})^2}{N-2}}$$

$$\sigma'' = \sqrt{\frac{\sum_{i=1}^{N-2}(q_i'' - \bar{q_i''})^2}{N-3}}$$

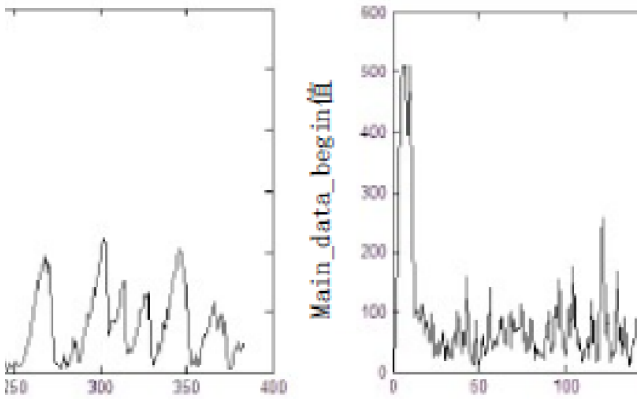
③将(σ', σ'')作为分析检测算法的特征向量。

3.3 边信息中main_data_begin值的均值统计量

MP3使用9比特的变量来记录每帧主数据的开始位置，音频桢长度改变同时将改变main_data_begin的值。由此，利用N代表待测MP3音频的总帧数，m_i对应第i帧的main_data_begin的值，可设计检测特征为main_data_begin值的均值函数，如下计算公式：

$$f = \frac{1}{N}\sum_{i=1}^{N} m_i$$

在给定编码率的情况下，编码器分配给每帧的比特数是恒定的，而MP3Stego算法嵌入将会产生更多的比特数剩余，进而导致下一帧的main_data_begin值比未隐写的音频要大，如下图所示：



左图为未隐写，有图为隐写之后

2.4 大值区系数的方法统计

隐写后，大值区系数的频次变化更加剧烈。利用N代表音频的总颗粒数，g_i代表对应第i个颗粒的大值区系数的个数，$\bar{g}$代表颗粒序列大值区系数的均值，结合隐写后QMDCT大值区系数的稀疏性，可以计算重压缩前后大值区系数方差的差值，如下：

$$\sigma^2 = \frac{1}{N-1}\sum_{i=1}^{N}(g_i - \bar{g})^2$$

此值也可以作为隐写分析特征。采用重压缩矫正的方法也可以进行载体估计，如下计算公式：

$$\Delta\sigma^2 = |\sigma_1^2 - \sigma_2^2|$$

总结

MP3Stego算法主要集中于编码参数域的隐写，此教程还对算法进行了分析。后续教程会进行实际的实验操作。

系列文章

隐写术基础_唠嗑！的博客-CSDN博客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。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https://blog.csdn.net/forest_LL/article/details/123953611?spm=1001.2014.3001.5501