图像隐写分析

原创

格物1030 于 2021-08-16 16:18:21 发布 849 收藏 5

文章标签： 机器学习 安全

本文链接：https://blog.csdn.net/qq_41997104/article/details/119730451

由于最近在写毕业论文，需要对图像的隐写分析进行深入的理解，一直对这个概念比较模糊，而且能查到的资料比较少，希望能通过简单易懂的语言帮助到大家！

文章目录

一、什么是隐写分析

在百度百科中，隐写分析是指在已知或未知嵌入算法的情况下，从观察到的数据检测判断其中是否存在秘密信息，分析数据量的大小和数据嵌入的位置，并最终破解嵌入内容的过程。

- 在密码学中，信息隐藏指将某些特殊信息隐藏于正常载体之中，掩盖特殊信息存在的事实。就像在战争电视剧中，信上的重要情报通过火烤才显现出来。
- 隐秘通信：隐藏了特殊信息的载体经由不安全信道传送。不安全的通道就代表有被截获的可能，而实现隐秘通信的技术手段主要是隐写术（Steganography），隐写术主要研究如何将实际存在的信息隐藏在正常载体中。
- 隐写分析是对隐写术的攻击，为了检测秘密信息的存在以至破坏隐秘通信。也就是提前将信上的情报解密出来。

隐写分析理论构建方面把隐写分析简化为检测载体的噪声甚至去噪，如何区分随机噪声和秘密信息是一个有待解决的问题。图像隐写分析是隐写分析的一个应用，由于数字图像具有信息冗余度大的特性，因此在其中隐藏秘密信息是难以被肉眼察觉，是一个理想的秘密信息载体。

二、隐写分析方法

按照采用的技术基础，可将隐写分析分为传统隐写分析模型和基于深度学习的隐写分析模型。

1. 传统隐写分析：需要一定的先验知识和根据数据而定的filters
2. 基于深度学习的隐写分析：利用网络强大的表征学习能力自主提取图像异常特征，大大减少了认为参与。其可分为（1）半学习隐写分析模型和（2）全学习隐写分析模型。

隐写分析可分为一下三个阶段：

1. 判断载密图像（stego）中是否隐藏秘密信息；
2. 判断载密图像中秘密信息的位置和容量（多为纹理复杂度或图像边缘处）；
3. 从载密图像中提取秘密信息，需要具体了解隐写方法、隐写位置、隐写容量等各种信息。

针对LSB和LSBN，修改最低有效位会在一定程度上破坏相邻元素之间的关联性，载体图像的某种统计特性特征会发生改变，这种在已知隐写算法的情况下，设计专用的隐写分析方法。
随着隐写算法的逐渐增强以及各式各样隐写算法的不断涌现，通用型隐写分析模型逐渐壮大，下面注重介绍SRM（steganalysis rich model)空域隐写分析，即通过分析数字图像的统计特性，来检测图像中是否嵌入秘密信息。

三、SRM(富模型隐写分析)

首先介绍一下基于残差图像的统计隐写分析：在早期的隐写分析研究中，研究者提出了对图像的噪声成分（残差图像）建模抽取隐写分析特征的方法。
2010年，Pevny等人设计了SPAM（Subtractive Pixel Adjacency Matrix)隐写分析特征。该方法通过对图像相邻像素的差分来进行建模，以感知隐写引起的图像相邻像素相关性的变化。证实了自然图像的噪声成分存在相邻像素相关性。SRM利用残差图像的统计进行隐写分析：
1、SRM通过建立不同的子模型，首先对训练样本中的图像空域特征信息进行提取，通过使用数十个一阶、二阶甚至高阶滤波器对图像进行处理，获得具有高度多样性的残差图像集合；
2、对得到的残差信息进行截断和量化，计算相应的共生矩阵；
3、利用机器学习的方式训练分类器。
并不仅仅分析图像中是否有秘密信息，并且分析可能的隐写方法、隐写修改的内容，通过隐写方法和隐写位置截取秘密信息。

SRM隐写分析特征针对载体图像和一个由30个隐写分析滤波器组成的阵列卷积后生成的残差图像阵列进行提取。
利用SRM隐写分析的特征，在提取图像噪声时，使用SRM滤波器核提取噪声是很好的方法。

参考文献

[1]陈君夫,付章杰,张卫明,程旭,孙星明.基于深度学习的图像隐写分析综述[J].软件学报,2021,32(02):551-578.

[2]吴贤城,周子凌,李振军,谭舜泉.对抗隐写分析滤波器残差提取的图像隐写算法[J].计算机应用,2019,39(S2):152-155.