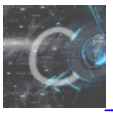
图像隐写发展历史

原创

MarDino 于 2019-10-24 19:26:32 发布 2559 收藏 29

分类专栏： 安全

本文链接：https://blog.csdn.net/weixin_44106928/article/details/102728269



前言

随着技术发展，计算机安全也不仅局限于网络安全，信息本身安全性也引起了人们的关注。一种有别于常规密码学的隐写术正逐渐发展，并常被用于传递隐藏信息。前几天就有俄罗斯黑客将恶意代码隐写进音频wav文件里进行传播，本文将针对图像隐写的发展历史进行一个总结

囚徒模型

博弈论和密码学里面常提到的一个模型就是囚徒模型。在一个监狱里，有两个罪犯和一个狱警。如果罪犯要传递一些信息，就很容易被狱警发现。但如果信息隐藏的过于隐秘，比如一些奇奇怪怪的举动，这也很容易引起狱警的关注。所以最好的办法就是将信息隐藏在常见的东西，这样既能达到传递信息的目的，也难以被人察觉，这也是隐写术的基础思想

数字水印

在讲图像隐写之前，我们先讲数字水印。我们常见的水印有视频水印，纸币水印。水印的目的在于保护载体，比如我们视频水印就是防止别人盗取视频，纸币水印就是保证纸币不被他人所伪造。

实际上，水印也可看作是一种信息的嵌入，视频里面常见的白色水印也就代表我们往里面嵌入了一些白色像素。不同的水印具有不同的性质，比如有些水印比较脆弱，可能图片压缩过后，水印不是特别清楚。有些水印则鲁棒性较高，也就是嵌入信息量大，不会因为一些轻易的改变而导致水印的消失。另外拓展，水印不止在空间域（即我们人眼所直观看到的地方）上进行嵌入，还可以在DCT域，WT域上嵌入。这些域都是经过一些变换得来，我们人眼是很难察觉到这些变换域上的变化。但要是在变换域上观察，就十分明显。

密码学简介

通常我们讲的安全大多数是以密码学里的安全作为基础，什么样的密码算安全的呢？这里密码学有个安全最低要求：已知密文和加密算法条件下，不能完全还原出明文，即正向运算容易，逆运算求解困难， 接触过安全的都知道，我们需要密钥来进行解密。在没有密钥情况下，一定时间内无法通过计算机计算得出来密码，那么这个加密算法就是安全的

所以不同时间段，我们的加密算法安全程度也不一样。比如最近谷歌研制出量子计算机，强大的计算能力足以破解我常见的加密算法，那么此时我们的“”加密算法“”，在量子计算机面前就是不安全的

隐写简介

在隐写里，我们的安全指标与密码学里面的指标不同
一是我们应用场景的不同
二是图像这个东西我们很难以一个计算复杂度来进行衡量
三是我们不考虑柯克霍夫定律
具体可参考
https://baike.baidu.com/item/%E6%9F%AF%E5%85%8B%E9%9C%8D%E5%A4%AB%E5%8E%9F%E5%88%99/2249887?fr=aladdin

在图像隐写里面，我们有三个指标来进行衡量，分别是安全性，鲁棒性，隐写容量

我们可以简单的把图像隐写理解为在图像本身加入一定的噪声，而我们的目的就是让别人看不出我们加入的噪声，所以隐写的数据越多，即噪声越大，越容易被发现

常用的度量方法就是 不可检测性
当我们区别不出隐写图像和原始图像，那么就达到了隐写的目的

总的来说图像隐写和数字水印很相似，这两者都是往图像里面嵌入数据
但是在数字水印这里我们允许失真来保证水印的鲁棒性
而图像隐写里我们是要避免被识别出来，所以在嵌入信息同时，要尽最大可能减小图像失真程度

早期隐写技术以及隐写检测

第一代隐写检测技术

早期隐写技术是在低维特征下，以图像统计特性进行隐写
于是一种隐写术产生，就有专门的一种隐写检测技术去检测，分析其特征
下面我们简单介绍早期隐写技术的代表LSB

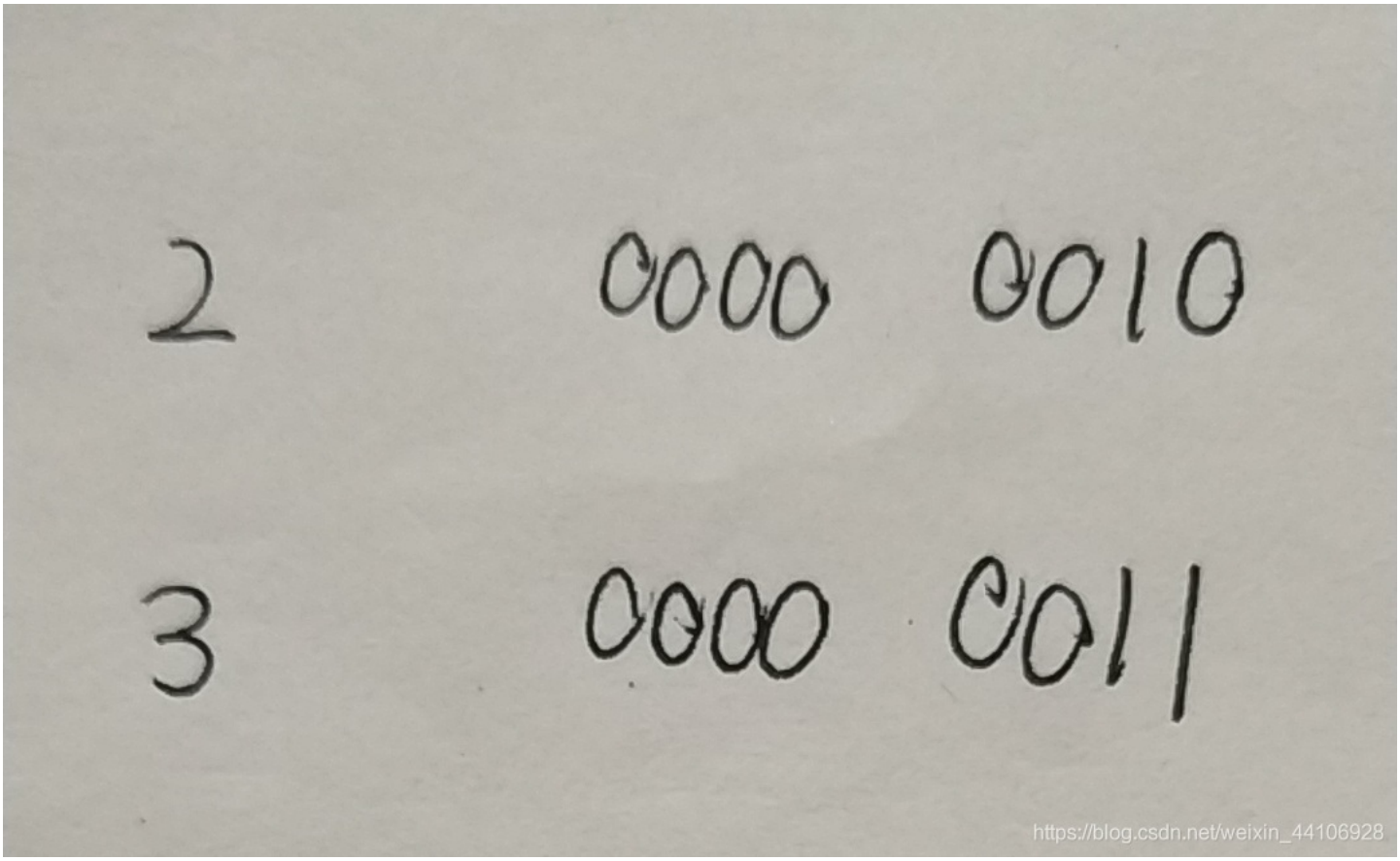
我们知道图像是由一个个像素组成
而每个像素都有对应不同的灰度值(亮度)构成
数字图像处理上引入了统计概念

图像直方图
也就是统计各个灰度的像素数目

这也是我们的一维统计特征
早期的隐写技术就建立在一维统计特征上，即单一的修改像素灰度值

而LSB是一种只对最低有效位修改，嵌入信息的隐写方式

我们使用8位二进制来表示我们的灰度值



这里我们将
2 表示为 0000 0010
3 表示为 0000 0011

最低有效位就是针对修改最低位
比如我要将2最低位嵌入1
那么0000 0010 就被修改为0000 0011
所以它就对应变成十进制的3

而3 最低位嵌入0的话
对应修改为十进制的2

所以我们将2和3称为一个pair
他们两者因为最低有效位修改的关系，称为一个值对
同理0和1是一对，4和5是一对，6和7是一对。

这仅仅只是从我们的一维特征上进行修改。
而我们如果以概率论的角度来看待这种直方图

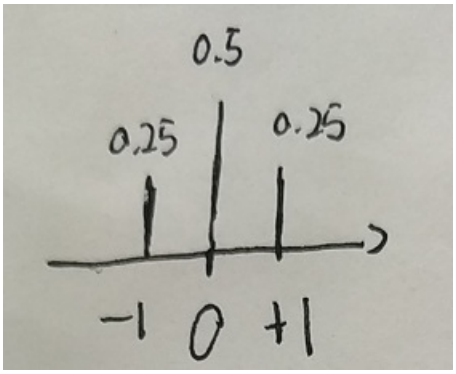
那么直方图就相当于一种灰度值的分布
而最低有效位改变了直方图的分布

在假设隐写嵌入概率为0.5，根据值对的对应关系，我们可以将LSB技术理解为一种值对的平滑

比如
灰度值为2的像素有100个
灰度值为3的像素有200个
我有一半概率将2修改为3，3修改为2
那么最后2的像素就有150个，3的像素也就有150个
就是在分布上，每一对值对的数量都被平滑过
我们便可以基于这种特征，来进行LSB隐写检测的设计

LSB技术很简单，但这是隐写术的基础，在第一代隐写技术里，后续的隐写技术都是基于LSB改进而来

于是研究人员就想，要是打破这种唯一的值对关系，那是不是能进一步改进LSB技术？
就出现了LSB MATCHING 这种隐写技术
传统LSB都是在最低有效位不变或者+1
而LSB Matching引入了一定的随机性，改为不变，加1，减1
但这种方法也很好应对，它无非就是改变了对应关系
我们假设-1 +1的概率分别为0.25 ，不变的概率为0.5



它也是相当于以这一种分布来对原始图像进行滤波，同样我们也能从统计角度上进行检测

第二代隐写技术

研究人员就在第二代隐写技术引入新的内容
我们要是要减小图像的失真，那就得让数据隐藏在细节丰富，人们难以察觉到变化的地方。
这就抛弃了第一代隐写技术对全局统计特性的思想

比如一副图像有天空，草坪。我们要是想进行隐写，就不会在天空那里添加数据(噪声),因为天空部分是很平滑的，如果加上几个噪点很容易被人发现。我们首选是在草地这里去进行隐写，因为草地纹理丰富，我们增添几个噪点让人们难以察觉得到

因此第二代隐写技术产生
并引入了一个失真函数
在上面一个例子我们可以得知，在不同局部嵌入信息，失真量是不一样的。而失真函数正是来评估这种失真量，并对隐写进行优化。
它在统计上并没有唯一的规律，只是按照失真函数进行优化
所以第二代隐写里面，谁的失真函数设计的合理，谁的隐写效果就好

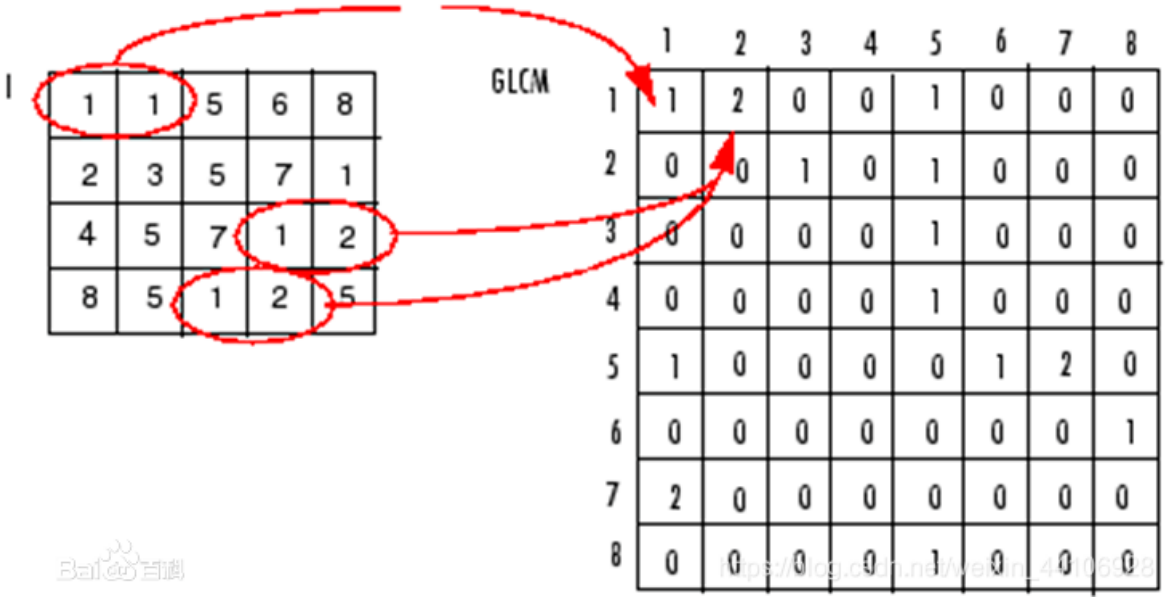
这个概念就很像机器学习里面的损失函数和优化器，机器学习里面为了寻得最优解也是从梯度方向不断去缩小损失函数的值

因此，第二代隐写检测技术除了常规的特征工程，我们还引入了机器学习的方法，如SVM，神经网络。特别是卷积神经网络，卷积层可以提取出不同维度空间的相关特性，进而达到检测的效果。

高维度特征

这里我们提一下不同维度空间的特性，一维的空间特性很简单，就是我们的图像灰度直方图
而高维度特征，我们引入一个共生矩阵的概念

灰度共生矩阵是对图像上保持某距离的两象素分别具有某灰度的状况进行统计得到的。



比如在二维情况下
我们的灰度值有从1-8
我们可以将一个新的统计矩阵写成8x8的形式
我们计算相邻两个像素之间的特性

我们拿个1x2的方框框住整个图像， 发现左右相邻均为1的个数只有1个，所以我们在对应的统计矩阵（1，1）里面填入个数1
对应的我们发现左为1，右为2的个数为2，我们在对应的统计矩阵（1， 2）里面填入2
以此类推，我们得到了一个二维的统计矩阵
他表征的是左右相邻两个像素灰度值的相关性

共生矩阵还有很多种形式，除了左右相邻，我们也可以以竖直方向上找各像素之间的相关性。总而言之就是以任意形状的方框像素相关性我们都能统计到，对应的也就提高了维数特征

因此在高维度下，做传统的特征工程是比较难的，我们便引入卷积神经网络来学习不同维度的相关性

后续隐写技术发展

目前机器学习风头正盛，也有人在尝试使用GAN生成对抗网络去自适应的学习隐写，这也会导致隐写检测难度不断提高，不再像第一代隐写技术与隐写检测技术是一种一一对应的关系

图像预处理

在隐写检测方面，适当的图像预处理能提高隐写检测的准确性
常用的方法有以下三种
calibration
re-embedding
filter

calibration

假设原始图像是x，隐写图像是y
其添加的噪声就是y - x，而这个值会很小难以区分

如果我们以一个新的函数映射将x和y分别映射成f(x) f(y)
那么f(x) - f(y) 这个值就可能会很大，有利于区分，这是一种值得尝试的变换思想

re-embedding

就是我们以同一种隐写方法
在原始图像和隐写图像进行相同的嵌入
这样也可能增大两者的差异，便于后续检测

filter

在早期图像隐写检测神经网络
最具代表性的就是Xu-net
它将图像输入进神经网络之前
做了一次高通滤波，而这也是其提高准确率的一大关键操作

原因是我们隐写嵌入数据相当于引入噪声。
这种其实是高频分量
而原始图像大部分平滑部分属于低频分量
我们使用高通滤波滤去大部分低频分量

留下的高频分量里面隐含隐写嵌入数据
所以我们只需要分析高频分量里是否有嵌入数据
这种思想也在后续隐写检测网络里面经常用到

总结

图像隐写术是一种新兴的安全技术，它更关注的是信息本身的安全。同时隐写术也是一把双刃剑，我们需要好好利用它