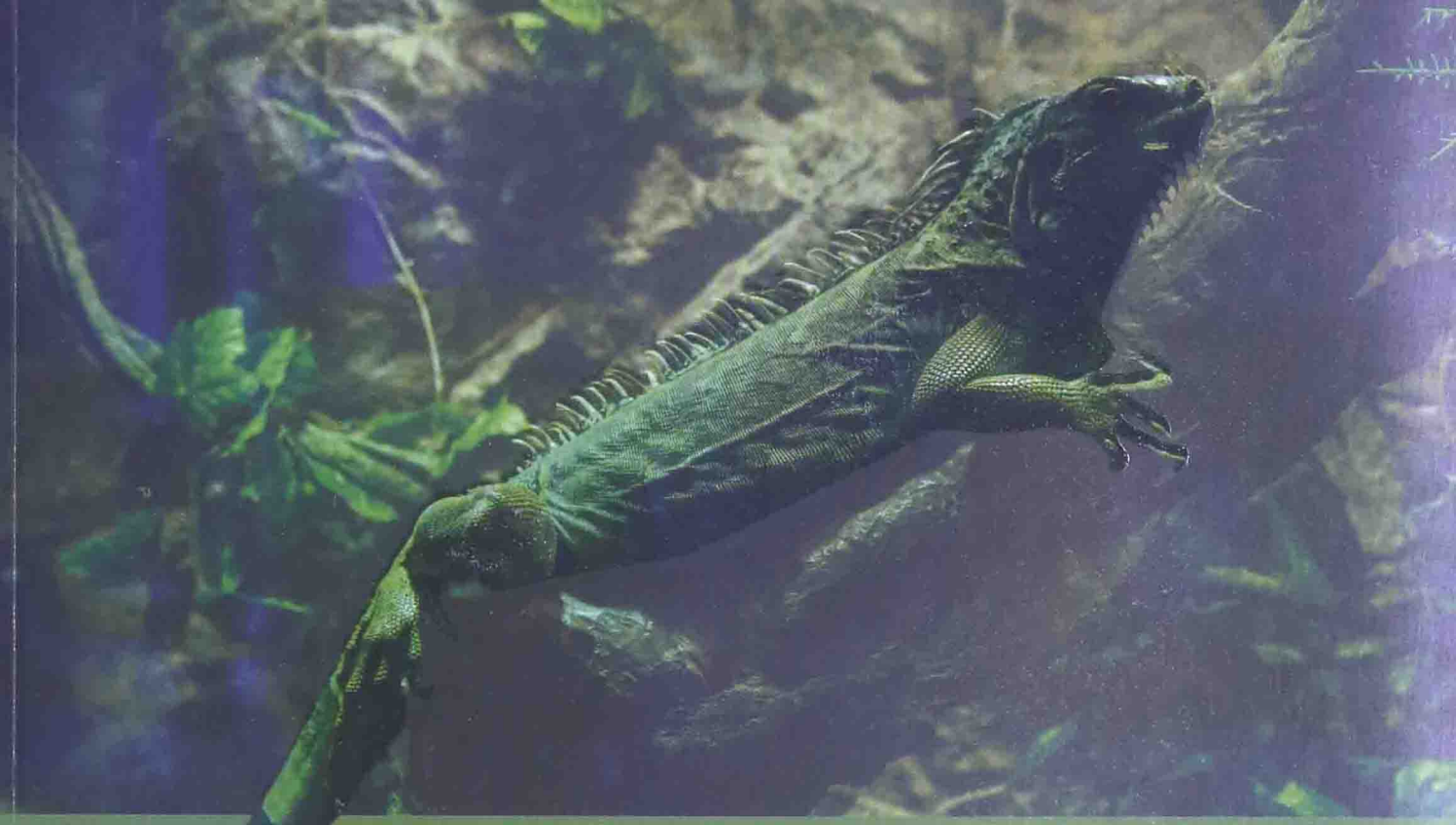

Theory and Application of Steganalysis

隐写分析原理与应用

葛秀慧　田浩　著

清华大学出版社

Theory and Application of Steganalysis

隐写分析原理与应用

葛秀慧　田浩　著

清华大学出版社
北京

内 容 简 介

本书以最新的研究成果为背景，阐述隐写分析这一研究方向，内容涉及隐写分析的基本术语、基本原理与方法以及具体的实践。本书语言通俗易懂，章节清晰，把原本抽象的原理与具体的示例进行结合，使读者能更加深入透彻地学习隐写分析，并且介绍了最新的隐写分析技术，使读者学到最新的技术。本书主要是对隐写分析这一研究领域的总结和升华，并给出可供实现的代码。通过本书的学习，读者不仅能掌握隐写技术的基础知识，还可提高实践经验，实现理论与动手能力的结合。

图书在版编目(CIP)数据

隐写分析原理与应用/葛秀慧，田浩著. --北京：清华大学出版社，2014
ISBN 978-7-302-35553-3

Ⅰ. ①隐…　Ⅱ. ①葛… ②田…　Ⅲ. ①密码术　Ⅳ. ①TN918.3

中国版本图书馆 CIP 数据核字(2014)第038591号

责任编辑：龙启铭
封面设计：傅瑞学
责任校对：李建庄
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954
印 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市吉祥印务有限公司
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：14　　**字　　数**：306 千字
版　　次：2014 年 10 月第 1 版　　**印　　次**：2014 年 10 月第1次印刷
印　　数：1～2000
定　　价：29.00 元

产品编号：057783-01

前言

隐写术是将秘密信息嵌入伪装载体的一门科学，其主要目标是使嵌入的秘密信息不可检测。但在这个世界上，事物总是两两对立，相互作用，彼增我长，就像矛与盾的关系一样，是对立统一的。既然存在着隐写术，就会存在敌手对其进行隐写分析，隐写分析者判断载体中是否存在隐藏的信息，如存在，则会想方设法地进行破译与提取。当某些隐写算法被破解后，就会有新的隐写算法问世，之后又会进行新一轮的破译，这个过程循环往复，像大海的波浪一样，推动着信息隐藏领域的研究不断发展前进。隐写术与隐写分析的关系就与大家所熟悉的加密解密的关系一样。

隐写分析是与数学、密码学、信息论、计算机视觉、模式识别、统计分析及机器学习等多学科交叉的学科，是各国研究者所关注和研究的热点。在隐写分析中，可以分为专用隐写分析和盲隐写分析。专用隐写分析就是针对某一专用隐写工具和算法进行分析，判定可疑载体是否含密，如果含密则根据需要破坏或提取秘密信息。盲隐写借助机器学习方法以蛮力的方法分析数据，进行特征选择。使用强有力的机器学习技术，并用成千幅的图像对分类器进行训练，就能察觉特性的很小偏差。隐写分析实质属于模式识别或机器学习的分类问题；其估计秘密信息长度，破译秘密信息，则属于量化分析和解密的范畴。

本书以最前沿的研究领域为基础，对隐写分析这一活跃的研究领域进行分析，既包括基本的攻击原理，也包括经典的示例。同时，将隐写分析领域最前沿的分析技术加以总结、实验，使读者通过具体的示例来理解抽象的隐写算法和特征。

本书共分5章，第1章主要探讨隐写分析的定义、隐写分析的目标、隐写分析方法、隐写分析的攻击类型、隐写分析分类、隐写分析的信息论基础和隐写系统评价。第2章主要针对空域的LSB算法进行分析与攻击。先介绍针对LSB的著名攻击，如Chi-Square(X^2)测试、RS攻击、SPA分析；接着分析基于一阶直方图和二阶直方图的特征：HCF-COM(HARD3)、ALE-10、AC-4，还分析了空域的BSM特征与IQM特征。第3章主要分析频域(DCT和

DWT)的JSteg隐写分析、F5隐写分析、OutGuess隐写分析及相应的频域特征，如FRI-23特征、FARID特征和共生矩阵。第4章探讨载体模型、MB模型、隐式马尔可夫模型、SPA模型、Rich模型及假设测试、量化分析与回归分析。因为隐写分析本质是分类问题，所以在第5章，我们集中分析各种分类方法，并加以比较，找到适合相应特征数据的最准确的分类方法，达到隐写分析的终极目标，即盲检测。第5章主要探讨的问题为模式识别、判别函数、线性判别、非线性判别、决策树、特征选择、特征提取、分类器、盲隐写分析与机器学习方法。

撰写本书，是作者长期的一个愿望，希望能写一本关于隐写分析研究方向的全面而翔实的书籍，经过几年资料的搜索整理和一年多的实验整理，最终呈现给读者这本图书。

本书的出版得到了河北省科技厅科技攻关项目(题目：隐写分析关键技术研究，批号：N011213507D)，河北省优秀专家出国培训项目和河北经贸大学出版基金的资助。

虽然作者精心地构思与书写，但会存在着局限性，因为书是作者思想的体现。对隐写分析这一研究领域，作者的研究只是冰山一角，不能概全，以管窥豹，仅见一斑。所以，肯定存在不足与错误，恳请广大读者和专家给予批评、指正。

作　者

2014年9月

目录

第1章 简　介

隐写术(steganography)是将秘密信息嵌入伪装载体的一门科学,其主要目标是使嵌入的秘密信息不可检测。但在这个世界上,事物总是两两对立,相互作用,彼增我长,就像矛与盾的关系一样,是对立统一的。既然存在着隐写术,就会存在着敌手对其进行**隐写分析**(steganalysis)。隐写分析者判断载体中是否存在隐藏的信息,如存在,则会想方设法地进行破译与提取。当某些隐写算法被破解后,就会有新的隐写算法问世,之后又会进行新一轮的破译,这个过程循环往复,像大海的波浪一样,推动着信息隐藏领域的研究不断发展前进。隐写术与隐写分析的关系就与大家所熟悉的加密解密的关系一样。

在本章中,主要探讨的问题如下:

- 隐写分析的定义。
- 隐写分析的目标。
- 隐写分析方法。
- 隐写分析的攻击类型。
- 隐写分析分类。
- 隐写分析的信息论基础。
- 隐写系统评价。

1.1 什么是隐写分析

隐写分析是检测隐藏数据的一门科学,其对貌似正常的传输媒体(如图像、音频、视频等)信号进行检测,判断其中是否存在秘密信息,如存在,则找到隐蔽通信的信源,阻断隐蔽通信的信道,如有需要,还会进一步提取隐藏的信息。有时,不能提取隐藏的秘密信息,但由于隐写算法在嵌入秘密数据时,必定会修改原数据,则载体数据的某些统计特性不可避免地会产生变化。只要分析者能分析出数据的统计特性的异常,就能判断出秘密信息的存在,即使不能提取秘密信息,但仍能有效地阻断隐蔽通信,并找到秘密信息的接收双方。

在隐写分析中，存在着各种攻击方法，但最具挑战的隐写分析是未知隐藏媒体、密钥、统计、隐藏媒体分布和嵌入算法的情况下所执行的盲隐写分析。此外，隐写分析的检测概率与隐藏信息的长度成正比，在载体中嵌入的信息越短，在嵌入过程中引入的可检测的特征越少。同时，还要使漏报率和误报率最低。在隐写分析中，一般都是判断载体是否存在秘密信息，但有时，在检测判定存在秘密信息之后，还要进一步提取秘密信息，如果秘密信息经强加密算法加密，则会加大提取信息的难度，因为还要运用解密知识。除此之外，为了提取秘密信息，还要研究信息嵌入方式、载体分布与容量等相关内容。

1.2 为什么需要隐写分析

互联网已成为人们生活中不可分割的一部分。通过互联网，通信双方不一定要直接相见或沟通。攻击者使用隐写术就可以隐藏秘密消息，并通过互联网进行传输。目前，在网上有150[14]多种开源的隐写工具可供使用。任何事情都有两面性，隐写术的广泛应用，使人们能更安全地进行隐蔽通信，但一些政府认为在互联网时代，隐写术已成为一种严重威胁，美国空军实验室与宾汉姆顿大学(Binghamton University)合作开发算法和技术来检测计算机和电子传输中各类媒体是否隐藏了秘密信息。其研究的重点是开发针对各类隐写算法的盲检测方法。在今日美国(USA Today)报道中，称9·11事件恐怖分子使用了隐写术，将秘密的计划信息隐藏于公共网站的图像之中。

隐写术的目标是使隐藏数据不可检测，如果隐写系统达到了这一要求，则隐藏的数据会同其他数据一样在网络中安全传输。而隐写分析所面临的挑战在于要在海量的位流中分析出隐藏的数据。

因为任何隐写系统都需要选择嵌入算法、提取算法、秘密消息和载体。根据加密学的原则，算法公开，密钥保密。因此，隐写系统的安全需要关注秘密信息的长度和欲嵌入的载体。嵌入的消息长度与检测率成反比，消息越短，检测率越低，消息越长，检测率越高。因为任何嵌入算法都会对载体造成影响，所以秘密消息长度是受限的。同时，载体有文本、音频、视频与图像。目前在隐写分析中以图像为载体的研究非常多。图像分为模拟图像(照片、光学图像等)和数字图像(将模拟图像离散化后的点阵图像)，图像的实质就是被量化的二维采样数组。在计算机中，用数字矩阵表示图像，矩阵中的每个元素称为像素。计算机存储有两种方式：位映射和向量处理。位映射是将图像的每个像素转换为数据，并存放在以字节为单位的矩阵中。向量处理存储图像内容的轮廓而不存储图像数据的每个点。在信息隐藏中，一般认为灰度图像是最佳的伪装载体。图像有许多种格式，如原始的未压缩格式的BMP，是最早被作为隐写载体的。然后，无损压缩的GIF等格式图像也被作为隐写载体。目前，因为相机、扫描仪等生成的图像均为JPEG格式，所以目前这种

格式的图像正在作为隐写载体的主体。此外，检测的难度也与秘密信息嵌入的方式相关。嵌入方式分为三种：顺序嵌入、随机嵌入和自适应嵌入。顺序嵌入顾名思义就是按顺序嵌入秘密信息。如按从左到右或按从低位到高位。顺序方式的实现最简单，所以安全性最低，隐写分析能检测出像素具有相同的统计特性。随机方式是随机地选择载体的子集，一般用密钥初始化伪随机发生器，从而产生随机位置，秘密信息位会嵌入这些随机位置，与顺序嵌入相比，随机嵌入安全性更高。自适应嵌入是根据载体的内容确定秘密信息嵌入的位置，与顺序嵌入和随机嵌入相比，安全性更高，因其统计特性取决于载体的统计特性。

自适应嵌入既不依赖于掩体的格式，也与嵌入函数不关联。但对嵌入而言，自适应嵌入的准则是不变的，一般是根据 Kerckhoffs 原则。该原则的主要思想是除密钥之外，敌手知道算法的一切内容，具体的原则如下：

- 即使非数学上不可破解，系统也应在实质(实用)程度上无法破解。
- 系统内不应含任何机密物，即使落入敌人手中也不会造成困扰。
- 密匙必须易于沟通和记忆，无须写下，且双方可以容易改变密匙。
- 系统应可以用于电信。
- 系统应可以携带，不应需要两个人或以上才能使用(应只要一个人就能使用)。
- 系统应容易使用，不至于让使用者的脑力过分操劳，也无需记得长串的规则。

根据这一原则，意味着敌手能更集中地重新识别嵌入改变的区域。在最坏情况下，敌手甚至可以比较掩体样本和隐体之间的样本子集。

在对隐写算法和秘密信息完全不知的情况下，进行盲隐写分析的难度最大，也是隐写分析的终极目标。隐写分析的发展是一个循序渐进的过程：先是视觉分析，提出了人类视觉模型；然后是结构分析，针对特定的某些隐写算法和特定载体进行分析，如对图像位平面的分析；接下来，研究人员发现，某些已有的隐写工具在隐写嵌入过程中会产生某些特征，通过这些特征，隐写分析工具能对其进行检测，这是隐写分析史上一个重要突破，这意味着自动隐写分析的可行性，人们将这种方法称为**统计隐写分析**(statistics steganalysis)。但是，针对特征统计方法，已出现了抗统计分析的算法，即在嵌入秘密消息时仍保持载体的统计特征不变，所以，对统计分析方法而言，又有了新的挑战。从目前分类而言，前三种分析方法都称为**专用隐写分析**(special steganalysis)，也称为**目标隐写分析**(targeted steganalysis)。因此，在一定时期，专用隐写分析具有重要的实际意义和应用价值。但是，随着隐写分析技术的积累与发展，由于专用隐写的局限性，目前的隐写分析主要聚焦于**通用隐写分析**(universal steganalysis)，也称为**盲隐写分析**(blind steganalysis)，它主要应用了机器学习和模式识别。

目前，国内外研究人员都在进行大量相关的实验，但是，隐写分析还需要研究隐写分析算法的评价、隐写分析理论构建与实用隐写系统的实现。目前隐写分析方法的评价还

未形成评价标准体系，需要建立用于检测的测试图像库以及评价度量手段。对于隐写分析的理论构建，一般将隐写分析简化为检测载体的噪声，所以区分随机噪声和秘密消息是一个需要解决的问题。鉴于隐写分析的准确性、实用性和适用性等各方面的综合要求，还需要将统计分析和归类判断等方法相结合，实现全自动检测，这也是构建实用隐写检测系统的终极研究方向。

在当前的互联网环境中，隐写分析在安全通信中起着举足轻重的作用。

1.3 隐写分析方法

随着隐写分析技术的发展，所使用的技术也分为如下 4 个阶段。

- 视觉隐写分析(Visual steganalysis)。
- 结构隐写分析(Structural steganalysis)。
- 统计隐写分析(Statistical steganalysis)。
- 学习隐写分析(Learning steganalysis)。

1.3.1 视觉隐写分析

在隐写分析初期，使用人类的感观来分辨载体是否含有秘密信息。如图 1.1 和图 1.2 分别是未含密载体图像和含密伪装图像。只凭人类的感知，很难察觉原图像与伪装图像之间的区别。

图 1.1 原始图像

图 1.2 伪装图像

为了能区分图像，隐写分析者想出了许多分析方法，也建立了相应的人类视觉感知模型。

不可感知性是隐写术的重要衡量指标。目前，根据人类听觉和视觉系统，已经提出了许多感知模型[15]，在此，先对人类感知进行分析，然后利用人类视觉感知特点和矩阵理论来描述 Watson 的感知模型。

人眼对在波长范围从 400nm～770nm 的电磁辐射非常敏感。彩色图像可以用函数 $C(x,y,t,\lambda)$表示。这个函数能表示位置(x,y)，反射光的波长 λ 和动态图像情况下的时间。对于颜色视觉，有三个基础可用的光谱敏感度函数 $V_R(\lambda)$、$V_G(\lambda)$和 $V_B(\lambda)$。通过人眼或照相机系统对场景中对象进行感知主要是通过它的辐射 $R(\lambda,x,y,t)$。照明与主观人类感知之间，以及与人类响应之间都存在着直接关系。在 Weber 定律中，第一次公式化地给出了这种关系，公式表示为

$$\frac{W_L}{L}=k \tag{1-1}$$

实验调查表明，Weber 定律只适用于中间照明值，对于很高和很低的照明值都不适用。可感知的亮度 B 与照明 L 间的关系是对数关系，即 $B\alpha\log L$。

根据 Thomas Young 的三原色理论，视觉系统所能感知的所有颜色都是基本颜色的线性组合。如果两种颜色之间存在**最小可觉差**(just noticeable difference，JND)，实际最小可觉差值不是常数，这主要是因为存在人类视觉的非线性和 RGB 空间的不均匀性。如果人眼颜色感知能力还未饱和，在较强照明时，人眼颜色感知能力更好。在 Buchsbaum 非线性等式中的常数考虑了眼睛的适应条件和照明条件。Buchsbaum 在 Weber 研究的基础上开始了他的研究，分析获得了对数形式的视觉非线性。

感知模型实际上是函数 $D(C_0,C_S)$，这个函数是计算原图像和隐写后图像之间的感知距离，传统使用的 MSE 均方差就是一个最简单的距离函数。感知模型的基本指标是灵敏度、掩蔽及合并。

(1) 灵敏度：对于视觉的感知，都与输入信号的频率相关。频率响应主要指空间频率、光谱频率和时间频率。空间频率通常指亮度敏感度，光谱频率以颜色形式感知，一般为低频响应，时间频率响应以运动的形式感知。

(2) 掩蔽：在视觉中有两种掩蔽，频率掩蔽和亮度掩蔽，前者是一段频率对另一段频率的感知掩蔽，后者是局部亮度将掩蔽对比度变化。

(3) 合并：在感知距离模型中，对多个不同失真的感知性综合归一为对伪装载体的评价，称为合并，公式为

$$D(C_0,C_S)=\left(\sum_i |d[i]^p|\right)^{\frac{1}{p}} \tag{1-2}$$

Watson 提出了一个测量视觉保真度模型，用于估计原图像和伪装图像之间的 JND 值。对于噪声加入图像后产生的影响估计，此模型比 MSE 效果要好。

模型的基本原理是根据图像的块离散 DCT 估计变化的感知性，然后将这些估计合并成对感知距离的单个估计。此模型基于 DCT 域，经过分块量化处理后，图像能量集中在每一块的低频部分，这样就能估计量化噪声的感知度，从而可以根据每幅图像的具体特性来改变量化步长。

在信息隐藏中需要用此模型评价和控制信息隐藏的算法。

Watson 模型由一个敏感度函数、两个基于亮度和对比度掩蔽和合并部分组成。

(1) 模型定义了频率敏感度表，表中每个元素表示在每块中不存在任何掩蔽噪声时，可感知 DCT 系数的最小幅度值。DCT 频率敏感度表如表 1.1 所示。

表 1.1 DCT 频率敏感度表

1.40	1.01	1.16	1.66	2.4	4.43	4.79	6.56
1.01	1.45	1.32	1.52	2.0	2.71	4.67	4.93
1.16	1.32	2.24	2.59	2.98	4.64	4.6	5.88
1.66	1.52	2.59	4.77	4.55	5.3	4.6	7.6
2.4	2.00	2.98	4.55	6.15	7.46	6.28	10.17
4.43	2.71	4.64	5.3	7.46	9.62	8.71	14.51
4.79	4.67	4.6	6.28	8.17	11.58	11.58	17.29
6.56	4.93	5.88	7.6	10.17	14.51	14.5	21.15

(2) 亮度掩蔽，如果 DCT 块的平均亮度值较高，DCT 系数较大的修改也不易察觉，Watson 模型对每个像素块，根据敏感度表的值进行调整，亮度的掩蔽阈值 $t_L[i,j,k]$ 为

$$t_L[i,j,k] = t[i,j](C_0[0,0,k]/C_{0,0})^{\alpha T} \tag{1-3}$$

(3) 上述亮度掩蔽值也受到对比度掩蔽的影响，对比度掩蔽阈值 $s[i,j,k]$ 为

$$s[i,j,k] = \max\{t_L[i,j,k], |C_0[i,j,k]|^{\omega[i,j]} t_L[i,j,k]^{1-\omega[i,j]}\} \tag{1-4}$$

(4) 合并，对原始图像与伪装图像比较，计算对应 DCT 系数的差值，然后除以对比度掩蔽，得到每项的可感知距离 $d[i,j,k]$，然后合并成一个总的感知距离为

$$D_{\text{Wat}}(C_0, C_S) = \left(\sum_i |d[i,j,k]^p|\right)^{\frac{1}{p}} \tag{1-5}$$

因为此模型是基于 DCT 变换的，主要用于 JPEG，经过变换之后，可以将能量集中在少量的低频系数之上，然后通过此模型来估计量化后的感知度。

在视觉分析研究中，其中最典型的视觉分析方法就是将原图像与伪装图像进行二值化处理，这样就能明显分辨两幅图像是否有区别。对图 1.1 和图 1.2 进行二值化处理，处理后的结果如图 1.3 和图 1.4 所示。

此时，通过人类视觉就能明显感知到后者隐藏了秘密信息。但由于每种图像呈现的结果不同，所以视觉分析具有很强的载体依赖性。

图 1.3　原图像的二值化图像

图 1.4　伪装图像的二值化图像

1.3.2　结构隐写分析

在视觉隐写分析之后，因为特定的隐写软件会留下标识特征，所以分析者会在媒体表示或文件格式中搜索这类标识或特征，从而出现了结构检测（也称为特征检测）。在任何隐写系统中，当嵌入秘密信息时，都会改变载体的某些性质或模式，这些引入的可检测的变化就称为特征。任何隐写工具都会引入某种特征。如对于 LSB 嵌入，嵌入秘密信息的像素值会产生改变，Westfeld 和 Pfitzman[16]观察到了 LSB 位平面的 PoV 现象，也提出了针对此的 Chi-Square 检测。

例如，在早期文本的隐写中，常常利用网页的内容。

- 文本：通过使用文本颜色与背景相同来隐藏文本，通过视觉的检测很难发现词和行间的很小移动。为了检测文本是否被破坏，按下 Ctrl＋A 对整个网页进行全选，把整个网页复制粘贴到字处理器中。当然，秘密信息也可以隐藏到网页的上下文中。检测这种嵌入秘密信息的方法就是分析最难的语法结构。
- 非文本元素：任何图片或媒体链接都可能隐藏链接或信息。
- 链接：链接的建立可以不使用下划线或者当鼠标指针经过这些链接时，链接不改变颜色。最简单的发现链接的方式是搜索“HREF＝”。另一种选择是用户可以使用 Tab 键来逐一移动到网页中所有链接之上。
- 注释：注释只有在网页的源代码中才能看到。
- 结构：许多浏览器都忽略没有经过说明的源代码信息，例如，在可选的标签中通常就可能有隐藏的线索。

- 框架：浏览在网页上每个框架的源代码。有时网站不能使用右击，或者使用菜单功能时看不到源代码。在这些情况下，试着在地址栏使用如下命令：

```
view-source:http://(site url)
```

此外，在基于特征的隐写分析中，需要根据大量隐写算法的载体对象集和掩体对象集来设计分类器，此时的分类是基于典型的自然图像本质特征。这些特征会随着图像的改变而改变。通过找到并计算图像嵌入前后特征改变量，就能确定是否嵌入了秘密信息。然后，使用强分类算法使这些特征差最大化，从而使分类更为准确。这些图像特征应该是准确的、单调的、一致的。隐写分析的准确性是指能以平均最小误差检测隐藏信息是否存在的能力。特征的单调性是指特征与嵌入信息大小之间的单调性。检测的一致性是指针对大量隐写算法与图像类型，隐写分析仍能提供准确的、一致性的检测。所以，在特征隐写分析中，所有特征是独立于图像类型的，这也是结构隐写分析优于视隐写分析之处。

在隐写分析初期，一般会利用特征隐写分析来确定载体是否存在隐藏信息；特征隐写分析比较简单，当顺序嵌入隐藏的秘密信息时，使用特征隐写能检测到是否存在隐藏信息，即能得到所希望的结果；当随机嵌入隐藏的秘密信息时，特征隐写分析的可靠性不高，存在很大问题。所以，出现了后来的基于统计的隐写分析方法，即识别原载体与伪装载体的一些统计特性的差异。但特征隐写分析是基础。在后续章节，我们将详细地介绍空域、频域的特征和分类器。

1.3.3 统计隐写分析

统计分析使用统计的方法来检测隐写术，统计隐写分析是利用各种统计分析对可疑的数字媒体进行分析，它借助于数学与统计技术，比特征隐写分析功能更强大。统计隐写需要统计模型，用于描述隐写系统或载体的概率分布，通常需要对相关载体和模型进行解析分析来开发统计隐写模型。一旦定义了模型，分析实际图像所必需的计算都已确定，并能进行自动测试。

统计分析也会使用简单的频谱分析，对于有损压缩算法的压缩文件，一般分析已压缩数据的不一致性。例如，利用 JPEG 压缩中常见的环形伪影，因为其高频部分会使相邻像素失真，且这种失真是可预测的，而简单的隐写编码算法不可能产生这种可检测的边环。

另外，还可以在原载体和伪装载体均可获取的情况下，比较二者异同，以提取隐藏的有效负载。此外，在只有伪装载体的情况下，隐写算法一般是替代载体的噪声部分，使嵌入的信息与白噪声非常接近，但这仍会使未调制的采样信号与调制后的采样信号的噪声分布差异很大。

基本的统计隐写分析会使用统计假设测试来确定载体是否为伪装载体。量化统计分析会使用参数估计来估算嵌入秘密信息的长度。