网络空间安全专业规划教材

总主编◎杨义先　　执行主编◎李小勇

信息隐藏与数字水印

Information Hiding and Digital Watermarking

杨 榆　雷 敏　编著

北京邮电大学出版社
www.buptpress.com

网络空间安全专业规划教材

总主编　杨义先　　执行主编　李小勇

信息隐藏与数字水印

杨榆　雷敏　编著

北京邮电大学出版社
www.buptpress.com

内 容 简 介

信息隐藏与数字水印是网络空间安全研究的重要内容之一。本书主要介绍了音频信息隐藏与数字水印、图像信息隐藏与数字水印、隐写分析、水印攻击与分析、信息隐藏与数字水印实验。

本书可用作高等院校网络空间安全、信息安全和计算机等相关专业学生教材和参考书，同时可用作科技工作者科研参考资料。

图书在版编目(CIP)数据

信息隐藏与数字水印 / 杨榆，雷敏编著. --北京 ：北京邮电大学出版社，2017.9

ISBN 978-7-5635-4943-6

Ⅰ. ①信… Ⅱ. ①杨…②雷… Ⅲ. ①信息系统—安全技术—高等学校—教材②电子计算机—密码术—高等学校—教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2016)第 241200 号

书　　名：信息隐藏与数字水印
著作责任者：杨　榆　雷　敏　编著
责 任 编 辑：刘　颖
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：
开　　本：787 mm×1 092 mm　1/16
印　　张：12.5
字　　数：302 千字
版　　次：2017 年 9 月第 1 版　2017 年 9 月第 1 次印刷

ISBN 978-7-5635-4943-6　　定价：28.00 元

Prologue 序

Prologue

作为最新的国家一级学科，由于其罕见的特殊性，网络空间安全真可谓是典型的“在游泳中学游泳”。一方面，蜂拥而至的现实人才需求和紧迫的技术挑战，促使我们必须以超常规手段，来启动并建设好该一级学科；另一方面，由于缺乏国内外可资借鉴的经验，也没有足够的时间纠结于众多细节，所以，作为当初“教育部网络空间安全一级学科研究论证工作组”的八位专家之一，我有义务借此机会，向大家介绍一下2014年规划该学科的相关情况；并结合现状，坦诚一些不足，以及改进和完善计划，以使大家有一个宏观了解。

我们所指的网络空间，也就是媒体常说的赛博空间，意指通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间。它已成为继陆、海、空、太空之后的第五空间。网络空间里不仅包括通过网络互联而成的各种计算系统（各种智能终端）、连接端系统的网络、连接网络的互联网和受控系统，也包括其中的硬件、软件乃至产生、处理、传输、存储的各种数据或信息。与其他四个空间不同，网络空间没有明确的、固定的边界，也没有集中的控制权威。

网络空间安全，研究网络空间中的安全威胁和防护问题，即在有敌手对抗的环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施，以及网络和系统本身的威胁和防护机制。网络空间安全不仅包括传统信息安全所涉及的信息保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。

网络空间安全一级学科，下设五个研究方向：网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全。

方向1，网络空间安全基础，为其他方向的研究提供理论、架构和方法学指导；它主要研究网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等内容。

方向2，密码学及应用，为后三个方向（系统安全、网络安全和应用安全）提供密码机制；它主要研究对称密码设计与分析、公钥密码设计与分析、安全协议

设计与分析、侧信道分析与防护、量子密码与新型密码等内容。

方向3，系统安全，保证网络空间中单元计算系统的安全；它主要研究芯片安全、系统软件安全、可信计算、虚拟化计算平台安全、恶意代码分析与防护、系统硬件和物理环境安全等内容。

方向4，网络安全，保证连接计算机的中间网络自身的安全以及在网络上所传输的信息的安全；它主要研究通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御（攻防与对抗）、端到端的安全通信等内容。

方向5，应用安全，保证网络空间中大型应用系统的安全，也是安全机制在互联网应用或服务领域中的综合应用；它主要研究关键应用系统安全、社会网络安全（包括内容安全）、隐私保护、工控系统与物联网安全、先进计算安全等内容。

从基础知识体系角度看，网络空间安全一级学科主要由五个模块组成：网络空间安全基础、密码学基础、系统安全技术、网络安全技术和应用安全技术。

模块1，网络空间安全基础知识模块，包括：数论、信息论、计算复杂性、操作系统、数据库、计算机组成、计算机网络、程序设计语言、网络空间安全导论、网络空间安全法律法规、网络空间安全管理基础。

模块2，密码学基础理论知识模块，包括：对称密码、公钥密码、量子密码、密码分析技术、安全协议。

模块3，系统安全理论与技术知识模块，包括：芯片安全、物理安全、可靠性技术、访问控制技术、操作系统安全、数据库安全、代码安全与软件漏洞挖掘、恶意代码分析与防御。

模块4，网络安全理论与技术知识模块，包括：通信网络安全、无线通信安全、IPv6安全、防火墙技术、入侵检测与防御、VPN、网络安全协议、网络漏洞检测与防护、网络攻击与防护。

模块5，应用安全理论与技术知识模块，包括：Web安全、数据存储与恢复、垃圾信息识别与过滤、舆情分析及预警、计算机数字取证、信息隐藏、电子政务安全、电子商务安全、云计算安全、物联网安全、大数据安全、隐私保护技术、数字版权保护技术。

其实，从纯学术角度看，网络空间安全一级学科的支撑专业，至少应该平等地包含信息安全专业、信息对抗专业、保密管理专业、网络空间安全专业、网络安全与执法专业等本科专业。但是，由于管理渠道等诸多原因，我们当初只重点考虑了信息安全专业，所以，就留下了一些遗憾，甚至空白，比如，信息安全心

理学、安全控制论、安全系统论等。不过幸好，学界现在已经开始着手，填补这些空白。

北京邮电大学在网络空间安全相关学科和专业等方面，在全国高校中一直处于领先水平；从20世纪80年代初至今，已有30余年的全方位积累，而且，一直就特别重视教学规范、课程建设、教材出版、实验培训等基本功。本套系列教材，主要是由北京邮电大学的骨干教师们，结合自身特长和教学科研方面的成果，撰写而成。本系列教材暂由《信息安全数学基础》《网络安全》《汇编语言与逆向工程》《软件安全》《网络空间安全导论》《可信计算理论与技术》《网络空间安全治理》《大数据服务与安全隐私技术》《数字内容安全》《量子计算与后量子密码》《移动终端安全》《漏洞分析技术实验教程》《网络安全实验》《网络空间安全基础》《信息安全管理(第3版)》《网络安全法学》《信息隐藏与数字水印》等20余本本科生教材组成。这些教材主要涵盖信息安全专业和网络空间安全专业，今后，一旦时机成熟，我们将组织国内外更多的专家，针对信息对抗专业、保密管理专业、网络安全与执法专业等，出版更多、更好的教材，为网络空间安全一级学科，提供更有力的支撑。

杨义先

教授、长江学者、杰青

北京邮电大学信息安全中心主任

灾备技术国家工程实验室主任

公共大数据国家重点实验室主任

2017年4月，于花溪

前言

Foreword

Foreword

没有网络安全，就没有国家安全；没有网络安全人才，就没有网络安全。

为了更多、更快、更好地培养网络安全人才，国务院学位委员会正式批准增设“网络空间安全”一级学科。并且首批授予了北京邮电大学等29所大学“网络空间安全一级学科博士点”。如今，许多大学都在努力培养网络安全人才，都在下大功夫、下大本钱，聘请优秀老师，招收优秀学生，建设一流的网络空间安全学院。

优秀教材是培养网络空间安全专业人才的关键。但是，这却是一项十分艰巨的任务。原因有二：其一，网络空间安全的涉及面非常广，至少包括密码学、数学、计算机、操作系统、通信工程、信息工程、数据库等多门学科，因此，其知识体系庞杂、难以梳理；其二，网络空间安全的实践性很强，技术发展更新非常快，对环境和师资要求也很高。

信息隐藏与数字水印是网络空间安全研究的重要内容之一，近几年得到很大的发展，各种新技术和新方法层出不穷。目前国内信息隐藏与数字水印教材较少，同时缺乏理论与实践相结合的教材。本书作者在北京邮电大学教授本科生和研究生的“信息隐藏与数字水印”课程，深知一本优秀的教材对于课程授课教授和学生的重要性。

本教材结合作者多年的教学和科研成果，同时重点参考北京邮电大学钮心忻教授主编的“普通高等教育‘十五’国家级规划教材”《信息隐藏与数字水印》和作者本人获得2015年中国通信学会年科学技术三等奖的《信息隐藏与数字水印实验教程》两本教材。

本教材除理论知识外，还提供丰富的实验，所有的实验提供源代码，本教材已经形成一套独具特色的立体化教学资源，所有的实验将通过最新的MOOE(Massive Open Online Experiments)形式提供；本教材兼顾实用性与专业性，本教材中所介绍的既有基础经典算法，也有最新的科研成果，读者可在此基础上举一反三，掌握信息隐藏与数字水印的各种工具和算法；本教材也是国内目前唯一一本能提供复习题及参考答案的信息隐藏与数字水印教材。

本书共分为10章，本书的第1～5章由杨榆编写，第6～10章由雷敏编写。

在本书的编写过程中，参考并实现了信息隐藏与数字水印领域大量经典算法和参考书籍，在此对这些算法的提出者和图书作者表示感谢。在教材编写过程中，廊坊师范学院的访问学者李维仙副教授为本图书的整理做了大量工作；教材编写组成员周椿入、杨明珠、梅晨曦、王勉、邓诗琪、艾心、钱劼等硕士研究生收集图书所需大量素材，绘制大量图片，并编程实现教材中所有实验；教材编写组成员罗群教授、邹仕洪副教授也多次审阅书稿，为书稿提出宝贵修改建议；教材编写组成员还就教材实验内容的难易程度、教材实验内容的覆盖面、教

材授课配套课件内容等教材立体化建设内容到绵阳、南京、杭州和其他开设地区不同层次开设信息安全专业的高校调研，听取其他高校授课教师关于教材的建议，并与其他高校授课教师进行深入交。在此对他们一一表示感谢！

由于作者水平有限，书中难免出现各种疏漏和不当之处，欢迎大家批评指正。

编者

Contents 目录

Contents

第 1 章　概论 …… 1

1.1　什么是信息隐藏 …… 1
1.2　信息隐藏的历史回顾 …… 2
1.2.1　技术性的隐写术 …… 2
1.2.2　语言学中的隐写术 …… 3
1.3　分类和发展现状 …… 4
1.3.1　伪装式保密通信 …… 4
1.3.2　数字水印 …… 5
1.4　信息隐藏算法性能指标 …… 7

第 2 章　基础知识 …… 9

2.1　人类听觉特点 …… 9
2.1.1　语音产生的过程及其声学特性 …… 9
2.1.2　语音信号产生的数字模型 …… 10
2.1.3　听觉系统和语音感知 …… 12
2.1.4　语音信号的统计特性 …… 14
2.1.5　语音的质量评价 …… 15
2.2　人类视觉特点与图像质量评价 …… 18
2.2.1　人类视觉特点 …… 18
2.2.2　图像的质量评价 …… 19
2.3　图像信号处理基础 …… 20
2.3.1　图像的基本表示 …… 20
2.3.2　常用图像处理方法 …… 21
2.3.3　图像类型的相互转换 …… 24
本章小结 …… 28

本章习题 …… 28

第 3 章　信息隐藏基本原理 …… 29

3.1　信息隐藏的概念 …… 29
3.2　信息隐藏的分类 …… 30
3.2.1　无密钥信息隐藏 …… 30
3.2.2　私钥信息隐藏 …… 31
3.2.3　公钥信息隐藏 …… 32
3.3　信息隐藏的安全性 …… 34
3.3.1　绝对安全性 …… 35
3.3.2　秘密消息的检测 …… 35
3.4　信息隐藏的鲁棒性 …… 36
3.5　信息隐藏的通信模型 …… 38
3.5.1　隐藏系统与通信系统的比较 …… 38
3.5.2　信息隐藏通信模型分类 …… 39
3.6　信息隐藏的应用 …… 40
本章小结 …… 41
本章习题 …… 41

第 4 章　音频信息隐藏 …… 42

4.1　基本原理 …… 42
4.2　音频信息隐藏 …… 44
4.2.1　LSB 音频隐藏算法 …… 44
4.2.2　回声隐藏算法 …… 44
4.3　简单扩频音频隐藏算法 …… 45
4.3.1　扩展频谱技术 …… 45
4.3.2　扩频信息隐藏模型 …… 45
4.3.3　扩频信息隐藏应用 …… 46
4.4　基于 MP3 的音频信息隐藏算法 …… 47
4.4.1　MP3 编码算法 …… 47
4.4.2　MP3 解码算法 …… 48
4.5　基于 MIDI 信息隐藏 …… 49
4.5.1　MIDI 文件简介 …… 49
4.5.2　MIDI 数字水印算法原理 …… 49
本章习题 …… 50

第 5 章　图像信息隐藏 …… 51

5.1　时域替换技术 …… 51
5.1.1　流载体的 LSB 方法 …… 54
5.1.2　伪随机置换 …… 55
5.1.3　利用奇偶校验位 …… 56
5.1.4　基于调色板的图像 …… 56
5.1.5　基于量化编码的隐藏信息 …… 57
5.1.6　在二值图像中隐藏信息 …… 57
5.2　变换域技术 …… 59
5.2.1　DCT 域的信息隐藏 …… 59
5.2.2　小波变换域的信息隐藏 …… 61
本章习题 …… 63

第 6 章　数字水印与版权保护 …… 64

6.1　数字水印提出的背景 …… 64
6.2　数字水印的定义 …… 65
6.3　数字水印的分类 …… 67
6.3.1　从水印的载体上分类 …… 67
6.3.2　从外观上分类 …… 68
6.3.3　从水印的加载方法上分类 …… 68
6.3.4　从水印的检测方法上分类 …… 70
6.4　数字水印的性能评价 …… 71
6.5　数字水印的应用现状和研究方向 …… 73
6.5.1　数字水印的应用 …… 73
6.5.2　数字水印的研究方向 …… 75
本章小结 …… 76
本章习题 …… 76

第 7 章　数字水印技术 …… 77

7.1　数字水印的形式和产生 …… 77
7.2　数字水印框架 …… 78
7.3　图像数字水印技术 …… 80
7.3.1　水印嵌入位置的选择 …… 80
7.3.2　工作域的选择 …… 81

7.3.3 脆弱性数字水印技术 …… 85
7.4 软件数字水印技术 …… 87
7.4.1 软件水印的特征和分类 …… 87
7.4.2 软件水印简介 …… 88
7.4.3 软件水印发展方向 …… 89
7.5 音频数字水印技术 …… 89
7.5.1 时间域音频数字水印 …… 90
7.5.2 变换域音频数字水印 …… 90
7.5.3 压缩域数字水印 …… 93
7.5.4 音频数字水印的评价指标 …… 93
7.5.5 音频水印发展方向 …… 95
7.6 视频数字水印技术 …… 96
7.6.1 视频水印的特点 …… 96
7.6.2 视频水印的分类 …… 97
本章小结 …… 98
本章习题 …… 98

第 8 章 信息隐藏分析 …… 99

8.1 隐写分析分类 …… 99
8.1.1 根据适用性 …… 99
8.1.2 根据已知消息 …… 100
8.1.3 根据采用的分析方法 …… 100
8.1.4 根据最终的效果 …… 100
8.2 信息隐藏分析的层次 …… 101
8.2.1 发现隐藏信息 …… 101
8.2.2 提取隐藏信息 …… 103
8.2.3 破坏隐藏信息 …… 103
8.3 隐写分析评价指标 …… 105
8.4 信息隐藏分析示例 …… 107
8.4.1 LSB 信息隐藏的卡方分析 …… 107
8.4.2 基于 SPA 的音频隐写分析 …… 108
本章小结 …… 110
本章习题 …… 110

第 9 章 数字水印的攻击 …… 111

9.1 数字水印攻击的分类 …… 111

9.1.1　去除攻击 …… 112
9.1.2　表达攻击 …… 112
9.1.3　解释攻击 …… 113
9.1.4　法律攻击 …… 114
9.2　水印攻击软件 …… 114
本章小结 …… 116
本章习题 …… 116

第 10 章　信息隐藏与数字水印实验 …… 117

10.1　信号处理基础 …… 117
【实验目的】 …… 117
【实验环境】 …… 117
【原理简介】 …… 117
【实验步骤】 …… 118
10.2　BMP 图像信息隐藏 …… 126
【实验目的】 …… 126
【实验环境】 …… 127
【原理简介】 …… 127
【实验步骤】 …… 127
10.3　LSB 图像信息隐藏 …… 130
【实验目的】 …… 130
【实验环境】 …… 130
【原理简介】 …… 130
10.4　DCT 域图像水印 …… 136
【实验目的】 …… 136
【实验环境】 …… 136
【原理简介】 …… 136
【实验步骤】 …… 136
10.5　回声信息隐藏 …… 138
【实验目的】 …… 138
【实验环境】 …… 138
【原理简介】 …… 139
【实验步骤】 …… 139
10.6　LSB 信息隐藏的卡方分析 …… 141
【实验目的】 …… 141

信息隐藏与数字水印

【实验环境】…… 142
【原理简介】…… 142
【实验步骤】…… 143
10.7　简单扩频语音水印算法…… 145
【实验目的】…… 145
【实验环境】…… 145
【原理简介】…… 145
【实验步骤】…… 145
综合复习题一…… 150
综合复习题二…… 161
综合复习题一参考答案…… 167
综合复习题二参考答案…… 177
参考文献…… 179

第 1 章

概　论

1.1　什么是信息隐藏

随着计算机技术和网络技术的发展，越来越多的数字化多媒体内容信息（图像、视频、音频等）纷纷以各种形式在网络上快速交流和传播。在开放的网络环境下，如何对数字化多媒体内容进行有效地管理和保护，成为信息安全领域的研究热点。对于上述问题，人们最初的想法是求助于传统的密码学。但是传统的加密手段在对数字内容管理和保护上存在着一定的缺陷。为此，人们开始寻找新的解决办法来作为对传统密码系统的补充。多媒体数字内容在网络上的传递、发布和扩散带来了一系列问题和应用需求，从总体上来说可以分为两大部分：多媒体数字内容的版权保护问题和伪装式保密通信，这两个研究问题都属于信息隐藏研究的范畴。

在很多参考文献中，对信息隐藏、数字水印、隐写术和隐写分析的描述经常混淆，为了更好地对本书的内容进行介绍，本书采用以下约定：

（1）信息隐藏（Information Hiding）。信息隐藏通过对载体进行难以被感知的改动，从而嵌入信息。

（2）隐写术（Steganography）。隐写术是通过对载体进行难以被感知的改动，从而嵌入秘密信息的技术。Steganography 一词来自于希腊词根：steganos 和 graphie。steganos 指有遮盖物的；graphie 指写。因此，Steganography 的字面意思即为隐写。

（3）数字水印（Digital Watermarking）。数字水印是通过对载体进行难以被感知的改动，从而嵌入与载体有关的信息，嵌入的信息不一定是秘密的，也有可能是可见。

（4）隐写分析（Steganalysis）。隐写分析是检测、提取、破坏隐写对象中秘密信息的技术。

信息隐藏的载体可以是图像、音频、视频、网络协议、文本和各类数据等。在不同的载体中，信息隐藏的方法有所不同，需要根据载体的特征选择合适的信息隐藏算法。例如，图像、视频、音频中的信息隐藏，大部分是利用了人类感观对于这些载体信号的冗余来隐藏信息。而文本、网络协议和各类数据等就无法利用冗余度来隐藏信息，因此在这些没有冗余度或者冗余度很小的载体中隐藏信息，就需要采用其他方法。

隐写术与数字水印是信息隐藏的两个重要研究分支，采用的原理都是将一定量的信息嵌入到载体数据中，但由于应用环境和应用场合的不同，对具体的性能要求不同。隐写术主要用在相互信任的点对点之间进行通信，隐写主要是保护嵌入到载体中的秘密信息。隐写

术注重的是信息的不可觉察性和不可检测性，同时要求具有相当的隐藏容量以提高通信的效率，隐写术一般不考虑鲁棒性。而数字水印要保护的对象是隐藏信息的载体，数字水印要求的主要性能指标是鲁棒性（脆弱水印除外），对容量要求不高，数字水印有一些是可见的，有一些是不可见的。

信息隐藏不同于传统的数据加密，数据加密隐藏信息的内容，让第三方看不懂；信息隐藏不但隐藏了信息的内容，而且隐藏了信息的存在性，让第三方看不见。传统的密码技术与信息隐藏技术并不矛盾，也不互相竞争，而是有益的相互补充。它们可用在不同场合，而且这两种技术对算法要求不同，在实际应用中还可以相互配合。

1.2 信息隐藏的历史回顾

类似于古典密码术，伪装式信息安全也是自古就有了。本节将讨论古典隐写术以及现代隐写术的发展。

本节将介绍一些参考文献上记载的重要的历史事件，以此来了解历史上人们是如何利用隐写术的。古代的隐写术从应用上可以分为这样几个方面：技术性的隐写术、语言学中的隐写术以及应用于版权保护的隐写术。

1.2.1 技术性的隐写术

最早的隐写术的例子可以追溯到远古时代。

- 用头发掩盖信息。在大约公元前 440 年，为了鼓动奴隶们起来反抗，Histiaus 给他最信任的奴隶剃头，并将消息刺在头上，等到头发长出来后，消息被遮盖，这样消息可以在各个部落中传递。
- 使用书记板隐藏信息。在波斯朝廷的一个希腊人 Demeratus，他要警告斯巴达将有一场由波斯国王薛西斯一世发动的入侵，他首先去掉书记板上的腊，然后将消息写在木板上，再用腊覆盖，这样处理后的书记板看起来是一个完全空白的。
- 将信函隐藏在信使的鞋底、衣服的皱褶中，妇女的头饰和首饰中等。
- 在一篇信函中，通过改变其中某些字母笔画的高度，或者在某些字母上面或下面挖出非常小的孔，以标识某些特殊的字母，这些特殊的字母组成秘密信息。
- Wilkins(1614—1672)对上述方法进行了改进，采用无形的墨水在特定字母上制作非常小的斑点。这种方法在两次世界大战中又被德国间谍重新使用起来。
- 在 1857 年，Brewster 提出将秘密消息隐藏“在大小不超过一个句号或小墨水点的空间里”的设想。到 1860 年，制作微小图像的难题被一个叫 Dragon 的法国摄影师解决了，很多消息就可以放在微缩胶片中。在 1870—1871 年弗朗格-普鲁士战争期间，巴黎被围困时，印制在微缩胶片中的消息通过信鸽进行传递。
- Brewster 的设想在第一次世界大战期间终于付诸实现，其做法是：先将间谍之间要传送的消息经过若干照相缩影后缩小到微粒状，然后粘贴在无关紧要的杂志等文字材料中的句号或逗号上。
- 使用化学方法的隐写术。例如，中国的魔术中采用的一些隐写方法，用笔蘸淀粉水

在白纸上写字，然后喷上碘水，则淀粉和碘起化学反应后显出棕色字体。化学的进步促使人们开发更加先进的墨水和显影剂。最终，人们发明了“万用显影剂”，结果不可见墨水的隐写方法就此被瓦解了。“万用显影剂”的原理是，根据纸张纤维的变化情况，来确定纸张的哪些部位被水打湿过，这样，所有采用墨水的隐写方法，在“万用显影剂”下都无效了。

- 在艺术作品中的隐写术。在一些变形夸张的绘画作品中，从正面看是一种景象，从侧面看是另一种景象，这其中就可以隐含作者的一些政治主张或异教思想。

1.2.2 语言学中的隐写术

语言学中的隐写术，最广泛使用的是藏头诗。

国外最著名的例子可能要算 Giovanni Boccaccio(1313—1375)的诗作 *Amorosa visione*，据说是“世界上最宏伟的藏头诗”作品。他先创作了三首十四行诗，总共包含大约 1 500 个字母，然后创作另一首诗，使连续三行押韵诗句的第一个字母恰好对应十四行诗的各字母。

16 世纪和 17 世纪已经出现了大量的关于伪装术的参考文献，并且其中许多方法依赖于一些信息编码手段。Gaspar Schott(1608—1666)在他的 400 页的著作 *Schola Steganographica* 中，扩展了 Trithemius 在 Polygraphia 一书中提出的“福哉马利亚(Ave Maria)”编码方法，其中 *Polygraphia* 和 *Steganographia* 是密码学和隐藏学领域最早出现的专著中的两本。扩展的编码使用 40 个表，其中每个表包含 24 个用四种语言(拉丁语、德语、意大利语和法语)表示的条目，每个条目对应于字母表中的一个字母。每个字母用出现在对应表的条目中的词或短语替代，得到的密文看起来像一段祷告、一封简单的信函、一段有魔力的咒语。

Gaspar Schott 还提出了可以在音乐乐谱中隐藏消息。用每一个音符对应一个字母，可以得到一个乐谱。当然，这种乐谱演奏出来就可能被怀疑。

中国古代也有很多藏头诗(也称嵌字诗)，并且这种诗词格式也流传到现在。例如，绍兴才子徐文长中秋节在杭州西湖赏月时，做了一首七言绝句：

平湖一色万顷秋，
湖光渺渺水长流。
秋月圆圆世间少，
月好四时最宜秋。

其中前面四个字连起来读，正是“平湖秋月”。

中国古代设计的信息隐藏方法中，发送者和接收者各持一张完全相同的、带有许多小孔的纸，这些孔的位置是被随机选定的。发送者将这张带有孔的纸覆盖在一张纸上，将秘密信息写在小孔的位置上，然后移去上面的纸，根据下面的纸上留下的字和空余位置，编写一段普通的文章。接收者只要把带孔的纸覆盖在这段普通文字上，就可以读出留在小孔中的秘密信息。在 16 世纪早期，意大利数学家 Cardan(1501—1576)也发明了这种方法，这种方法现在被称作卡登格子法。

下面介绍用于版权保护的隐写术。

版权保护和侵权的斗争从古至今一直在持续着。根据 Samuelson 的记载，第一部版权法是圣安妮的法令，由英国国会于 1710 年制定。隐写术又是如何被用于版权保护的呢？