

67

国家自然科学基金项目资助
国家重点基础研究规划项目资助

信息隐藏技术及其应用

刘振华 尹 萍 编著

科 学 出 版 社

2 0 0 2

内 容 简 介

信息隐藏是一门新兴的学科,是与密码术、多媒体、计算机网络紧密相关的交叉学科,它通过将秘密消息隐藏在其他消息之中达到隐匿消息存在的目的,其在版权保护、保密通信等领域都具有广泛的应用价值。本书系统地阐述了信息隐藏的基本概念、主要技术、攻击方法和信息隐藏的应用,同时介绍了近年来国内外研究人员在这一领域的主要成果。

全书共分七章。第一章简要介绍了信息隐藏技术的发展、术语、主要原理及存在的局限性,其余各章分别对信息隐藏技术在隐写术、数字水印、数字指纹、计算机系统中的隐通道、密码术中的阈下通道、低截获概率通信、广播加密、匿名服务等方面应用的主要技术和攻击方法做了详尽的说明。

本书可作为信息安全、密码学等相关专业的大学高年级学生或研究生的教学用书,也可供以上领域的研究工作者参考。

图书在版编目(CIP)数据

信息隐藏技术及其应用/刘振华,尹萍编著. —北京:科学出版社,2002
ISBN 7-03-010084-0

I. 信… II. 刘… III. 信息处理-安全技术 IV. G202

中国版本图书馆 CIP 数据核字(2002)第 002646 号

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

<http://www.sciencep.com>

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2002年2月第一版 开本:850×1168 1/32

2002年2月第一次印刷 印张:8

印数:1—4 000 字数:190 000

定价:15.00元

(如有印装质量问题,我社负责调换〈路通〉)

目 录

序

前言

第一章 信息隐藏概论	1
1.1 研究内容	1
1.2 基本概念	4
1.2.1 术语	4
1.2.2 模型	7
1.3 信息隐藏的基本理论	9
1.3.1 早期结论	10
1.3.2 随机性	11
1.3.3 稳健性	12
1.4 理论局限	14
1.4.1 理想压缩	15
1.4.2 熵	16
1.4.3 可选择信道	17
1.4.4 奇偶性	18
1.4.5 等价类	19
1.5 具体应用	20
1.6 发展现状	21
1.7 小结	23
第二章 隐写术	25
2.1 隐写术的发展	25
2.2 隐写术与密码术	30
2.3 隐写系统模型	31
2.4 隐写技术	33

2.4.1	隐匿安全	33
2.4.2	伪装	36
2.4.3	隐蔽被嵌入信息的位置	38
2.4.4	扩散被嵌入信息	40
2.4.5	特殊环境下的技术	42
2.5	隐写算法设计	44
2.5.1	简单隐写系统	45
2.5.2	抗压缩隐写系统	47
2.5.3	回声隐藏系统	52
2.6	隐写术的局限性	57
2.6.1	稳健性攻击	57
2.6.2	马赛克攻击	63
2.7	主动看守者和被动看守者	64
2.8	公钥隐写术	66
2.8.1	被动看守者	66
2.8.2	主动看守者	67
2.9	小结	68
第三章	数字水印	71
3.1	知识产权保护	72
3.1.1	知识产权的定义及其内容	72
3.1.2	数字作品的版权保护	73
3.1.3	法律问题	74
3.1.4	技术考虑	75
3.2	版权标记技术的发展	76
3.2.1	复制保护机制	76
3.2.2	数字水印方案	78
3.3	数字水印的定义和分类	80
3.4	数字水印的主要特征	80
3.5	数字水印的嵌入和检测技术	82
3.5.1	时空域数字水印	83

3.5.2	变换域数字水印	88
3.6	数字水印的攻击	108
3.6.1	StirMark	108
3.6.2	解释攻击	113
3.6.3	拷贝攻击	129
3.6.4	实现考虑	134
3.7	数字水印的评估	136
3.7.1	基准测试程序	136
3.7.2	一般过程	137
3.7.3	攻击手段	139
3.7.4	测试结果	145
3.8	小结	147
第四章	数字指纹	150
4.1	介绍	151
4.1.1	数字指纹技术的发展	151
4.1.2	术语和定义	154
4.1.3	数字指纹的主要特征	155
4.2	数字指纹系统模型	158
4.3	数字指纹的编码	159
4.3.1	指纹编码的码距	160
4.3.2	指纹码字矩阵的秩	161
4.3.3	指纹码字的个数	162
4.3.4	利用指纹码字矩阵分析分发指纹的抗合谋攻击能力	164
4.4	数字指纹的攻击	166
4.4.1	单用户攻击	167
4.4.2	合谋攻击	167
4.5	跟踪算法	168
4.5.1	单用户攻击	169
4.5.2	合谋攻击	170

4.6	一个数字指纹方案的实例	174
4.6.1	编码方案	175
4.6.2	抗合谋攻击能力的分析	176
4.6.3	跟踪算法	178
4.7	小结	179
第五章	计算机系统中的隐通道技术	181
5.1	介绍	181
5.2	隐通道的发展	182
5.3	隐通道的分类	184
5.4	隐通道分析方法	185
5.5	基于上下文的隐通道	186
5.5.1	定义	187
5.5.2	隐通道类型	187
5.5.3	高性能网络分析	188
5.5.4	L与H之间的隐通道	189
5.6	小结	190
第六章	密码协议中的阙下信道	192
6.1	介绍	192
6.2	阙下信道的发展	193
6.3	阙下信道的分类	194
6.4	数字签名方案中的阙下信道	195
6.4.1	DSA 数字签名方案的阙下信道	195
6.4.2	ElGamal 数字签名方案中的“牛顿通道”(Newton channel)	197
6.5	阙下信道的监测与防范	198
6.5.1	定义	199
6.5.2	一次无阙下“硬币抛掷”密码协议	201
6.6	小结	202
第七章	信息隐藏的其他重要应用	204
7.1	广播加密	204

7.1.1 介绍	205
7.1.2 可跟踪方案	206
7.2 低截获概率通信	209
7.2.1 扩展频谱通信	209
7.2.2 流星猝发通信	210
7.3 匿名服务	211
7.3.1 匿名电子邮件	211
7.3.2 匿名电子选举	213
7.4 小结	215
附录	217
A. 信息隐藏相关研究团体	217
B. 国外部分从事信息隐藏技术研究的人员	219
C. 目前国际上流行的信息隐藏软件	223
D. 从事水印和信息隐藏技术开发的公司及其产品	227
E. 我国数字水印和信息隐藏研究	232
F. 国际信息隐藏研讨会论文集目录	234

第一章 信息隐藏概论

在现实生活中，人们对于信息的保密往往是求助于密码术，而计算机软硬件技术的发展使得密码破译能力越来越强，这迫使人们对加密算法的强度提出越来越高的要求。在许多领域，密码术的应用已经越来越显现出它的局限性。由于密码术是利用随机性来对抗密码攻击的，而密文的随机性同时也暴露了消息的重要性，即使密码的强度足以使得攻击者无法破解出明文，但攻击者有足够的手段来对其进行破坏，从而使得消息无法被接收。密文容易引起攻击者注意是密码术的一个显著弱点。因此，对于某些应用来说，仅仅对信息的内容加以保密是不够的，本书将介绍信息的另一种保密方式，即对信息存在本身或信息存在位置的保密——信息隐藏。

1.1 研究内容

在许多应用领域中，人们常常希望将秘密信息隐藏在某些对象中，或者防止别人通过这种方式秘密传递信息。其中比较有代表性的例子有出于某种利益的隐蔽通信，保护作者合法权益的版权标记，以及军事上所需的低截获概率通信等。对隐写术、数字水印、操作系统中隐通道、密码协议中隐通道以及低截获概率通信等技术手段的研究能够在一定程度上从理论上和工程上满足人们的需求，这些都是信息隐藏所研究的内容。

隐写术 (Steganography) 是信息隐藏技术的一个重要分支，它的历史非常悠久，并且可以在很多领域得到应用。情报人员利用隐写墨水在报纸上写信或在磁带的特定位置加入次声波回声等方法来传递秘密信息，这就是隐写术应用的一个典型实例。在计

计算机领域应用隐写术的基本原理是利用信息中普遍存在的冗余性向其中嵌入秘密信息，从而达到隐蔽重要信息存在的目的。举例来说，由于人眼的分辨率是有限的，对于一幅 8 比特/像素 (Bit/Pixel) 的灰度图像，最低两位的随机变化并不会在视觉上造成差异，这样，就可以利用隐写术将秘密消息隐藏在图像之中。同样，视频、音频等媒体中也都含有大量信息冗余，可以为隐写术的使用提供条件。利用隐写技术将加密后的信息隐藏在无关紧要的信息中保存起来或发送出去，可以避免引起其他人的注意，是一种更为安全有效的信息保密方式。

近年来，由于计算机网络和多媒体技术的迅速发展，越来越多的文学和艺术工作者使用计算机进行创作，同时，大批网络创作者也应运而生，他们的共同特点是将作品以数字形式进行存储和传输。然而，数字作品的便利性与不安全性是并存的，它可以低成本、高速度地被复制和传播，为创作者和使用都提供了有利条件，但这些特性也容易被盗版者所利用，因而，采取多种手段对数字作品进行保护、对侵权者进行惩罚已经成为迫在眉睫的工作。除了与传统作品版权保护相类似的法律和管理手段外，还应该针对数字作品的特点为其提供技术上的保护。向数字作品中加入不易察觉但可以鉴别的版权标记是进行数字作品版权保护的一种有效技术手段，这种技术被称为版权标记技术。

版权标记技术中的标记可以是一个商标、一个序列号、或是一种防止未授权用户直接拷贝的方法等。根据标记内容和所采用技术的不同可以将版权标记技术分为数字水印技术和数字指纹技术。数字水印技术是向数字作品中嵌入版权信息，从而达到确定所有者身份，识别侵权者的目的；数字指纹则是向为不同用户分发的数字拷贝中分别嵌入不同的序列号，使得版权所有者在发现非法再分发时能够确定是哪些用户违背了许可协议。版权标记能够保护几乎所有的数字产品，包括音频、视频、图像、图形、文本、软件等。因此，版权标记技术引起了音乐、电影、书籍出版者的广泛关注，成为目前信息隐藏研究的热点问题之一。

在长期的使用过程中人们发现，计算机系统中存在的安全漏洞也可以被用来秘密传输信息，这一技术被称为计算机系统上的隐通道技术，也是信息隐藏研究人员所关注的问题之一。计算机系统的进程通信中有大量的数据流存在，在对可信计算机平台的评估中，无论是存储隐通道还是时域隐通道，人们发现隐通道是不可能完全阻断的。现代计算机系统带宽越来越大，遗憾的是，要保证安全，就不可避免地要降低系统的带宽，人们必须折中考虑降低带宽对系统性能的影响。现在，人们通过使用特定的分析工具检测出系统中存在的隐通道，从而可以减少系统的安全漏洞。

在信息安全领域内，数学家创造性地利用各种数学结构来进行各种编码体制、密码协议的设计，但是这些数学结构也会被高手用来攻击密码算法和发现密码协议的缺陷，其中阙下通道就是攻击者研究的重点所在。自1978年人们发现苏美SALT II条约监督协议中存在着阙下通道以来，阙下通道就成为密码协议研究的一个重要选题，人们发现，数字签名协议在使用随机数来增强抗攻击能力的同时，也恰恰造出了可以被用来传输秘密消息的阙下通道。这样，阙下通道也可以成为进行信息隐藏的工具之一。

现代战争中，截获与反截获是机要通信战线上的重要斗争之一，低截获概率通信的研究已经越来越引起各国政府和军队的重视，成为现代通信的重大课题。20世纪50年代中期开始研究的扩频通信技术就是一种无线低截获概率通信。它将待传送的信息数据进行伪随机编码调制，实现频谱扩展后再传输，接收端则采用同样的编码进行解调获取信息。扩频通信把原本集中于较窄频段的待传送信息展宽到较宽频带，并可以在很低的信噪比下传送信息。因此，在不知道伪随机编码的情况下，截获低功率谱密度的扩频通信信息将是一件很困难的事情。流星猝发通信则是利用微流星体电离轨迹进入地球的大气层会反射无线电波这一现象来建立远程通信连接。由于流星轨迹会迅速散射，因而信号强度也会快速衰减，流星猝发通信的这一间歇特性以及每一条轨迹相对

较小的覆盖区域，使得它们本质上难于被监视，可以用于低截获概率通信。

另外，在广播加密和匿名服务等领域也有信息隐藏技术的重要应用，本书的第二章到第七章将分别对信息隐藏各个应用分支的研究做更加详细的介绍。

1.2 基本概念

20世纪90年代前期，信息隐藏的各种应用引起不同研究团体的关注和重视。最初，这些研究团体各自进行着他们的研究工作，也各自使用不同的术语。1996年5月信息隐藏第一次国际学术研讨会的召开使这些独立的研究团体走到了一起，在这次会议上，人们对信息隐藏应用中的一些共同术语达成共识，本书借鉴了其中的大部分模型和术语。

1.2.1 术语

顾名思义，信息隐藏就是将保密信息隐藏于另一非保密载体中，以不引起检查者的注意。我们通常将希望被秘密保存的信息称为**嵌入对象**，将用于隐蔽嵌入对象的非保密载体称为**掩体对象**。嵌入对象通过嵌入过程被隐藏在称为掩体对象的非保密信息中，从而生成**隐藏对象**。掩体对象可以是掩体文本、掩体图像或掩体音频等，对应的隐藏对象也可以是隐藏文本、隐藏图像或隐藏音频等。将嵌入对象添加到掩体对象中得到隐藏对象的过程被称为**信息的嵌入**，嵌入过程中所使用的算法称为**嵌入算法**。信息嵌入的逆过程，即从隐藏对象中重新获得嵌入对象的过程称为**信息的提取**，也可称为信息的恢复。在提取过程中所使用的算法称为**提取算法**。执行嵌入过程和提取过程的组织或个人分别被称为**嵌入者**和**提取者**。

在嵌入和提取过程中通常会使用一个秘密信息来对其进行控制，使得只有它的持有者才能对其进行操作，这个秘密信息被称

为**隐藏密钥**，隐藏密钥在嵌入过程中被称为**嵌入密钥**，在提取过程中被称为**提取密钥**。通常情况下，嵌入密钥和提取密钥是相同的，这样的信息隐藏技术被称为**对称信息隐藏技术**；反之，若嵌入密钥与提取密钥不相同，则被称为**非对称信息隐藏技术**。

与密码术类似，我们可以将信息隐藏的研究分为**隐藏技术**和**隐藏分析技术**两部分。隐藏技术研究的主要内容是寻求向掩体对象中秘密添加嵌入信息的方法，而隐藏分析技术研究的主要内容则是考虑如何从隐藏对象中破解出嵌入信息，或通过对隐藏对象的处理达到破坏嵌入信息和阻止信息检测的目的。我们将隐藏技术的研究者称为**隐藏者**，将隐藏分析技术的研究者称为**隐藏分析者**。

1.2.1.1 隐写术

“**隐写术**”一词源于希腊词语“**στεγανω**”，其字面意思是“**掩饰性地写**”，通常被解释为将秘密信息隐藏在其他信息中。信息隐藏的基本概念可以直接引入隐写系统中，即将嵌入对象隐藏在掩体对象中，生成隐写对象，相应的密钥称为隐写密钥。不难看出，隐写术的主要目的在于将重要的信息隐蔽起来，以便不引人注意地传输或存储。因此，在一个隐写系统中，嵌入对象是主体，而掩体对象则可以是任何能够达到隐蔽传输目的的载体数据。通常情况下，选择掩体对象时需要考虑隐写容量的大小和隐写结果的不引人注意性这两方面因素。在实际应用中，通常可以精心设计一个掩体对象来隐藏嵌入对象，甚至还可以根据嵌入对象直接构造隐写对象，这样可以提高隐写容量，达到高效隐写的目的，但同时还应该考虑所生成的隐写对象应不引人注意这一原则。

在隐写信道中存在的隐藏分析者常常被称为“**看守者**”，这是因为人们一般将 Simmons 提出的“**囚犯问题**”作为隐写系统的通用模型。根据看守者能否对流经他的信息流进行改动和处理，还可以将隐写系统中的看守者分为“**被动看守者**”和“**主动**

看守者”。

1.2.1.2 版权标记系统

所谓版权标记系统，是指作者可以用来向其创作出的数字作品中添加不易察觉但可以鉴别的版权标记，以达到版权保护目的的系统。对应的嵌入对象被称为**版权标记信息**，掩体对象为作者的原始作品，通过系统的嵌入过程生成水印作品。版权标记系统中的标记信息可以是一个商标、一个序列号、或是一种防止未经授权用户直接拷贝的方法。根据标记内容和目的的不同可以将版权标记系统分为数字水印系统和数字指纹系统两大类。在数字水印系统中，水印所代表的是作者的身份，这一信息必须经过注册获得管理机构的认可，因此多个作品可以被嵌入相同的水印；而在数字指纹系统中，指纹所代表的则是购买者的身份，同一作品的每一份被出售版本都被嵌入不同的指纹以对购买者进行区分。

在版权标记系统中，隐藏分析者通常被称为“**盗版者**”，指他们的行为与海盗掠夺他人财物毫无二致。此外，在数字指纹系统中，可能有多个用户联合起来对添加有指纹的数据拷贝进行处理和伪造，这样的攻击被称为“**合谋攻击**”，参与合谋攻击的用户被称为“**合谋盗版者**”。

1.2.1.3 计算机系统中的隐通道

计算机系统**中的隐通道**是指可以用来传输信息的系统安全漏洞。隐通道中的概念与隐写术中的类似，但掩体对象是一个系统的整个运行过程。根据隐通道存在位置的不同可将其分为**存储隐通道**和**时间隐通道**。计算机系统的进程通信中有大量的数据流存在，在可信计算机平台的评估中，人们发现隐通道是不可能完全阻断的，无论是存储隐通道还是时域隐通道。

1.2.1.4 密码协议中的阙下通道

密码协议中的阙下通道是指被用来传输秘密消息的各种编码

体制和密码协议设计中所采用的数学结构。密码协议中的阙下通道主要存在于签名和认证协议中，例如许多数字签名协议在使用随机数来增强抗攻击能力的同时，也恰恰造出了可利用数字签名传输秘密消息的阙下通道。在阙下通道中，如果隐写分析者完全知道将被认证的消息，或者隐写分析者可以阻塞错误消息，那么唯一可被发送者利用的掩体对象就是被认证数据。这里隐写分析者对有效认证有一个精确的标准，并且只要能够维持有效认证就可以改变隐写数据。

1.2.1.5 低截获概率通信

低截获概率通信，顾名思义就是使信号被截获的概率降低的通信技术。其中的掩体对象是整个通信频带。例如扩频通信把集中于较窄频段的待传送信息展宽到较宽频带，并在很低的信噪比下传送信息，以增加截获的困难性。

1.2.2 模型

一个信息隐藏系统的一般化模型可以用图 1-1 来表示。系统主要包括一个嵌入过程和一个提取过程，其中嵌入过程是指信息隐藏者利用嵌入密钥，将嵌入对象添加到掩体对象中，从而生成隐藏对象这一过程。隐藏对象在传输过程中有可能被隐藏分析者截获并进行处理。提取过程是指利用提取密钥从接收到的、可能经过修改的隐藏对象中恢复嵌入对象，在提取过程中有可能需要

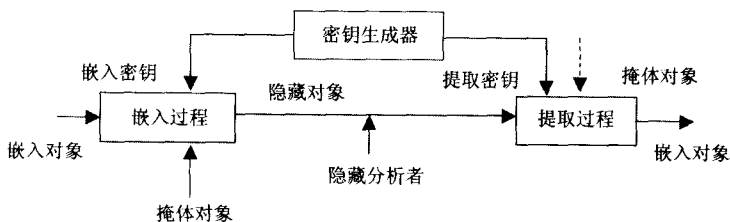


图 1-1 信息隐藏系统的一般模型

掩体对象，也可能不需要。该模型中没有包括对待隐藏信息的预处理和提取后的后处理，在有些情况下，为了提高保密性需要预先对待隐藏信息进行预处理（例如加密），相应地在提取过程后要得到对嵌入对象进行后处理（例如解密），恢复原始信息。

图 1-1 中的“对象”可以是“消息”、“图像”、“文本”等，下面对图中的各部分内容做详细的说明：

1. **嵌入对象**：信息隐藏嵌入过程的输入之一，指需要被隐藏在其他载体之中的对象。嵌入对象将在提取过程中被恢复出来，但是由于隐藏对象在传输过程中有可能受到隐藏分析者的攻击，提取过程通常只能正确恢复出原始嵌入对象的一部分。
2. **掩体对象**：用于隐蔽被嵌入信息的载体，在一些信息隐藏系统的提取过程中也需要掩体信息的参与。在同一个掩体对象分别用于隐藏多个嵌入对象时（如数字指纹系统）必须考虑合谋攻击。
3. **隐藏对象**：嵌入过程的输出，指将被嵌入对象隐藏在掩体对象中之后得出的结果。隐藏对象应该与掩体对象具有相同的形式，并且为了达到不引人注意的效果，通常要求二者之间的差别是不可感知的。
4. **密钥**：在隐藏过程中可能需要的附加秘密数据。通常需要在提取过程中使用与嵌入过程中相同或相关的密钥才能重新提取出被嵌入消息。

在这个信息隐藏系统模型还存在一个**隐藏分析者**，他通常位于隐藏对象传输的信道上。隐藏分析者的目标主要有以下几点：

1. 检测出隐藏对象；
2. 查明被嵌入对象；
3. 向第三方证明消息被嵌入，甚至指出是什么消息；
4. 在不对隐藏对象作大的改动的前提下，从隐写对象中删

除被嵌入对象；

5. 阻塞，即删除所有可能被嵌入对象而不考虑掩体对象。

其中前三个目标通常可由被动观察实现，后两个目标通常由主动干扰实现。我们称前者为**被动攻击**，后者为**主动攻击**。相应的攻击者分别被称为被动攻击者和主动攻击者。对面向不同应用的信息隐藏系统，其攻击者的目的也不尽相同。通常，在隐写系统中攻击者并不知道在某个数据对象中是否隐藏有秘密信息，因此隐写系统攻击者的目的往往在于正确检测出被嵌入目标的位置；而对版权标记系统来说，攻击者明确了解作品中含有版权标记，他们的目的就是使得标记不可用，因此版权标记系统的攻击者都是主动攻击者。

信息隐藏系统中的各对象会因研究的具体内容和所使用的技术不同而有所不同，我们将在对信息隐藏各应用分支进行具体描述的后续章节中详细介绍该应用环境下的对应模型。

1.3 信息隐藏的基本理论

信息隐藏产生后很自然地引出了一个问题，即我们是否可以在 Shannon 密码系统理论以及 Simmons 认证系统理论的基础上再建立起一个信息隐藏系统理论。许多领域的实践经验表明，仅仅从思想上加以改进而没有理论支持的技术是难以为使用者提供安全性保障的，因而也难以获得大规模应用。同时，信息隐藏应用的广泛性以及实践中的具体情况也要求我们建立起一个其安全性能被数学证明的信息隐藏理论体系来为信息隐藏技术的可行性和安全性做出保障。举例来说，版权保护机制可能在很长的一段时间内成为攻击者的目标。一般情况下，版权随国家和媒介的不同，在艺术家有生之年及死后 50~70 年都受到保护。这就意味着我们现在所采取的版权保护机制很可能会受到 100 年内各种可利用资源和技术的攻击。在密码系统中，需要提供这样的保证时，一般是采用一次一密技术，因为我们可以证明这个系统的强

度与攻击者所能提供的计算能力无关。那么，在一个信息隐藏系统中是否也能提供这样的保证呢？

目前在隐写术和版权标记技术的研究中人们提出了一些理论雏形，但尚未构成一个完整的理论体系。本节和下一节将分别介绍在信息隐藏领域已有的一些理论基础以及其中存在的局限性。

1.3.1 早期结论

发展一个学科理论的重要步骤之一就是对概念进行澄清。直观上来说，隐写术的目的就是在通信双方之间建立起一条秘密通信路径，使得其间的任何人不能发觉它的存在，而攻击者也无法仅仅通过观察隐藏对象获得嵌入数据的任何信息。1983年，Simmons将其形式化为“囚犯问题”^①，具体描述如下：Alice和Bob在监狱中准备策划一次越狱行动，问题在于他们的通信要被看守者Willie监督。如果Willie在他们的消息中发现任何密文，就会将Alice和Bob单独禁闭起来，使得他们的计划失败。因此Alice和Bob必须找到交换秘密信息的方法。

一般情况下，在隐写系统中，如果Willie可以修改Alice和Bob间的信息流，则称Willie为主动看守者，如果他只能对信息进行观察却不能修改，则Willie被称为被动看守者。对囚犯问题进一步的研究表明，尽管在一个主动看守者存在的条件下，使用公钥隐写术是非常困难的，但仍然存在公钥隐写术的可能。前提是，在这个模型中，Alice和Bob入狱前虽然未曾交换信息，但是彼此知道对方的公钥。

公钥隐写术的困难性导致了阙下通道的引出。阙下通道是指一个具有非常低带宽的通道，它使用掩体对象感知重要的部分来作为传递秘密信息的通道，因而Willie不能对其进行修改。例如，Alice可以编写一个短故事，然后用故事中出现的城市名称

^① Simmons G J. 1984. The Prisoner's Problem and the Subliminal Channel. *Advances in Cryptology: Proceedings of CRYPTO'83*. Plenum Press. 51—67