信息隐藏技术综述

迟文韬1)

1）南开大学网络空间安全学院 2020级信息安全、法学双学位特色班

摘 要 信息隐藏主要指将特定的信息嵌入数字化宿主信息 （如文本，数字化的声音、图像、视频信号等）中，信息隐藏的目的不在于限制正常的信息存取和访问，而在于保证隐藏的信息不引起监控者的注意和重视，从而减少被攻击的可能性，在此基础上再使用密码术来加强隐藏信息的安全性，因此信息隐藏比信息加密更为安全。

关键词 信息隐藏技术；安全；信息保护；国内外研究现状

A review of information hiding technologies

Chi Wentao1)

1)Nankai University, Cyberspace Security Academy, 2020 double degree class in Information security and Law

**Abstract** Information hiding mainly refers to the specific information embedded in digital host information (such as text, digitized sound, image, video signal, etc.), the purpose of information hiding is not to restrict normal information access and access, but to ensure that hidden information does not attract the attention and attention of the monitor, thereby reducing the possibility of being attacked, on this basis and then use cryptography to strengthen the security of hidden information, so information hiding is more secure than information encryption.

**Key words** Information hiding technology;Safety;Information protection; Research Status at home and abroad

# 引言

漫漫时间长河裹挟着无数的信息延展至今，这些信息参与到人类生活的方方面面，或是农业生产经验，或是时事政策，或是生活琐碎……其实无论是何种信息，它们都帮助着我们将生活的架构串联在一起——在当代的“信息化”特征下，信息扮演的角色无疑更加显得举重若轻。

信息作为如此重要的存在，其安全问题无疑就相应地登上了历史舞台。古代为了特定信息的安全问题，人们创造出了各种信息保护的手段，其中包括了“密写术”、“阴符、阴书”、“藏头诗”等等手段；来到现代，信息保护主要依赖于信息加密技术——通过加密技术把重要的数据变成无规则的乱码，进行本地存储或分享，然而实现‘内容安全’加密后的数据与普通明文数据在形式上会有巨大差异。正因如此，在如今的数据时代，大数据分析技术往往更容易关注到加密后的数据，这些数据进而暴露出使用加密数据的人或组织，在某种程度上数据挖掘或网络攻击更容易不请自来。在这种情形下我们容易明白大数据时代，重要数据隐匿地进行传输流转往往相当重要！而基于信息隐藏技术我们正能实现这种更为安全的信息处理。

# 信息隐藏技术的概念、特征及发展

## 信息隐藏技术的概念

2.1.1信息隐藏技术概念概述

所谓信息隐藏就是将机密信息秘密地隐藏再另一非机密文件内容中。这些非机密文件被称之为载体，载体的形式可以为任何一种数字媒体，例如图像、声音、视频或者一般文件。信息隐藏技术可以保证别有用心的人很难发现或者提取机密信息；而当载体传输到正确的接收器时，接收器则可以使用密钥或者其他方法将机密信息恢复、读取。

## 2.1.2信息隐藏技术和密码技术（概念进一步的阐述）

信息隐藏技术作为一种诞生较晚的信息安全前沿技术，其与传统的密码技术之间无可避免有着明显的区别，这些区别往往能归结于以下几点：

### 2.1.2.1 概念不同

密码技术是一种将明文加密成他人看不懂的密文的技术，是信息保护和网络信息体系建设的基础；而信息隐藏技术则是将机密信息隐藏在另一非机密文件中，提供了一种有别于加密的安全模式，其安全性主要来自于第三方感知上的麻痹性。

### 2.1.2.2 原理不同

密码仅仅隐藏了信息的内容，而信息伪装不但隐藏了信息的内容而且隐藏了信息的存在。信息隐藏技术提供了一种有别于加密的安全模式，其安全性来自于对第三方感知上的麻痹性。在这一过程中载体信息的作用实际上包括两个方面：①提供传递信息的信道；②为隐藏信息的传递提供伪装。随着计算机网络和多媒体技术的发展，信息隐藏技术的应用在不断扩展，载体信息的作用也在发生着变化。应该注意到，密码技术和信息隐藏技术并不是互相矛盾、互相竞争的技术，而是互补的。它们的区别在于应用的场合不同、要求不同，但可能在实际应用中需要互相配合。

密码技术的原理主要是对原来为明文的文件或数据按照某种算法进行处理，使其成为不可读的一段代码，通常称之为“密文”，使其只能在输入相应的密钥之后才能显示出本来内容，通过这样的途径来达到保护文件、数据不被其他人非法窃取、阅读的目的。而信息隐藏技术的原理则类似于生物学中的保护色，其是将机密文件或数据通过算法或者其他技术上的处理，隐藏到一般的非机密文件中，当其传送到接收器或者传到目的人手中时，其能够通过密钥或者其他算法、方法对目标文件进行处理，使其还原出原机密文件。

### 2.1.2.3 外在形式不同

如上文所说，密码技术实质上是可以被黑客或者计算机检测到的，即便它对明文进行了足量的处理，进而获得不可读懂的“乱码”；而信息隐藏技术则是将机密信息隐藏于一般的非机密数字媒体也即“普通”媒体中，其目的是为了让机密文件不被发现，即机密文件不可见。简而言之，数据加密隐藏了信息的内容，让第三方看不懂；信息隐藏技术则不仅隐藏了信息的内容，而且隐藏了信息的存在。

### 2.1.2.4 二者之间的联系

传统的密码技术与信息隐藏技术并不是互相矛盾、互相竞争的技术，而是有益的相互补充，在实际应用中相互配合。

## **2.2** 信息隐藏技术的特征

### 2.2.1 隐藏性

作为一种信息保护的手段，隐藏性是信息隐藏技术的基本要求。其主要包括两个方面内容：一是信息隐藏技术需保证不容易让人体感官察觉，即在进行信息隐藏以后，载体的性质不会发生明显改变，不会因此而引起人们听觉、视觉或者其他感官的察觉。二是信息隐藏技术需尽量规避被计算机系统检测出来，即要求在进行信息隐藏时，这是因为一个载体即便其外在并未发生任何改变足以引起人的感官识别，但仍旧有可能被计算机监测到其特性的改变，例如载体类型、大小等等。这便要求信息隐藏技术在进行信息嵌入时应该尽量保证载体的特性不变，并尽可能地不被计算机检测出来。

### 2.2.2 安全性

信息隐藏技术的目的就是为了保障信息传递的安全，为此，安全性自然也是信息隐藏技术的一大特征。安全性主要也分为两个方面：一是保证隐藏在载体中的机密信息能够安全传达到目的地，这要求在传输途中不会被他人或电脑检测出来；二是需要保证在传输途中，隐藏在载体中的机密信息不会损坏。

### 2.2.3 鲁棒性

鲁棒性是指控制系统在一定结构、大小的参数摄动下，维持其他某些性能的特性。在信息隐藏技术中，即经过一系列的处理和干扰后，载体中隐藏的机密信息不会被破坏，仍旧可以从中提取出完整信息。

**2.3**  信息隐藏技术的发展

虽然数字化的信息隐藏技术是一门全新的技术，但是它的思想其实来自古老的隐写术。现代信息隐藏技术是由古老的隐写术（Steganography）发展而来的。

接下来是一些历史发展进程中的实例

1文头送信：利用将信息文刺在头皮上，再利用长起来的头发予以隐匿

2诗画传达，例如藏头诗、藏尾诗、漏格诗以及绘画等形式，主要方式是将要表达的意思和“密语”隐藏在诗文或画卷中的特定位置实现信息的隐藏

3音乐传达：利用事先规定的密码进行编制乐谱进而传递出信息

4微缩原理，利用显微点膜片实现信息的隐藏

5密写术：利用某些化合物对纸张、布料、塑料等有“潜隐”功能的载体进行书写，只有在特定条件下，信息才会显露出来。

6掩蔽纸张传递法：利用收发信人拥有者的相同掩蔽纸张实现信息的安全传递

7隐匿标记： 利用掩蔽材料的预定位置上某些误差和风格特性来隐藏消息

8现代信息隐藏技术：现代又发明了很多方法用于信息隐藏：高分辨率缩微胶片、扩频通信、流星余迹散射通信、语义编码（Semagram）等。 其中：扩频通信和流星余迹散射通信多用于军事上，使敌手难以检测和干扰通信信号；语义编码是指用非文字的东西来表示文字消息的内容，例如把手表指针拧到不同的位置可表示不同的含义，用图画、乐谱等都可以进行语义编码。

9量子技术隐形传递信息：发送者利用量子特性的独特功能，对所提取的信息通过运用量子技术突破经典信息系统的极限，超水平进行信息传递。

可以看到信息隐藏技术随着技术发展不断焕发着崭新的活力，无疑昭显了信息隐藏技术独特的魅力与重要性。

# 信息隐藏技术实例

## 数字水印技术 [[1]](#footnote-0)

### 3.1.1 数字水印技术的概念和特征

数字水印是信息隐藏常用的技术之一，是一种基于内容而不是密码机制的技术。它是将一些相关标识直接嵌入到数字载体中或者进行间接表示，不影响原载体中的信息，且不容易被识别、提取和修改。

与整体的信息隐藏技术相同，数字水印同样具有隐藏性和安全性的特征，此外，它还具有水印容量的特征。所谓水印容量，是指原始图像在不产生形变的情况下能够嵌入的最大水印数据量。

### 3.1.2 数字水印技术的基本原理和框架

#### 3.1.2.1数字水印技术的生成技术

数字水印技术是通过信号处理，将不可感知、抗检测、具有隐藏性、安全性的数字水印嵌入到数字载体中，同时不影响原载体应用价值的编码技术，通过提取隐藏的信息，能达到保护创作者知识产权的目的。

生成数字水印的主要步骤分为三个部分，即数字水印生成、嵌入和提取三个部分。无论是哪种算法，其首要步骤都是生成水印。水印也分为有意义和无意义两种。前者一般为创作者的个人标签（文字、数字）等，生成水印便是对这些标签进行预处理的过程；后者通常是伪随机实数序列和白噪音等随机序列。

#### 3.1.2.2数字水印的基本框架

生成数字水印的算法完成后，进行数字水印的嵌入和提取，需要选择合适的水印嵌入方法将标识信息嵌入到数字媒体文件中，不影响数字产品的视觉效果，且在需要提取水印时，能够提取出完整的水印信息。水印的提取则是嵌入过程的逆变换，在进行提取时需要原始载体和嵌入水印的标识信息相互协助提取水印信息。

### 3.1.2数字水印的应用[[2]](#footnote-1)

数字水印技术作为一种新兴的信息加密技术，其应用领域设计各个方面，这里提出一些主要应用领域：版权保护，即通过提取信息中的水印来证明版权原创者对其作品的所有权，作为鉴定起诉非法侵权的有力证据；内容认证，入指纹数据库、医学影像、网上交易等；交易跟踪，当信息产品的某个拷贝进行多次交易时，可以利用水印进行记录，一旦发现有未经授权的拷贝出现，就可以据此确定它的来源。

## 可视密码技术[[3]](#footnote-2)

### 3.2.1 可视密码技术的概述

可视密码在秘密共享领域，是一个新的分支，其主要思想是将原始秘密图像通过构造基础矩阵分为n张图像，将这n张图像分发给相应的参与者。从表面上看，参与者所持有图像都是随机分布的黑白像素点图像，仅仅只是观察单一张图像，无法得出原始图像的秘密信息。若要恢复出人眼可识别的原始图像，只需要叠加其中任意等于或多于k 张图像即可，而少于k张图像叠加则不能得到原始图像可视密码技术的加密解密过程，不需要复杂的计算机运算，在恢复加密信息时只需要进行简单的胶片叠加，依靠人眼视觉 系统即可，因而得到了广泛的关注和应用。

### 3.2.2 可视密码技术的优点与研究

#### 可视密码技术的优点

1普遍性

可视密码技术是针对图像进行的加解密的技术，解密过程只需要叠加共享图像，适用于绝大多数人；

2隐蔽性

每一张共享图像都是随机分布的黑白像素，隐藏的信息不会被攻击者察觉；

3安全性

从可视密码技术的原理可知，由于原始图像被随机分为n张图像，攻击者采用任何方法或手段都无法对单张分享图像进行分析都不会得到任何和原始图像有关的加密信息。

#### 可视密码的研究

近几年来，对可视密码的研究主要分为以下几个方面：方案参数优化；彩色可视密码方案；放欺骗的可视密码方案。

可视密码是专门针对图像的加解密技术，在如今数字化信息高速发展的时代，有着广泛的应用空间，它可以有效地解决秘密图像信息隐藏的问题。可视密码技术主要应用在对安全性要求较高的领域，比如密钥分发、存取控制、数字签名、数字水印、身份验证等方面；同时，在军事领域方面，可视密码技术可以有效地利用在卫星拍摄图的加密与传输过程中，更大限度地提升了作战的保密性和安全性。因此，可视密码技术具有极大的研究价值和应用前景

## 潜信道

1978年，Gustavus J Simmons提出了潜信道的概念，随后进行了许多研究，其中潜信道是用于实现在公开信道中建立的秘密通信的信道。大多数数字签名方案包括潜信道通信，最大特征是潜信道包含在数字签名中，但是不影响数字签名过程。

## 隐匿协议

隐匿协议的原理是通过分析一方的业务量来识别另一方，可以确保通信信道不被他人窃听。隐秘通信通过在路由中使用多个加密层，保证路由的每一层处理不同的数据，可以使数据传输的路径很难被察觉到。隐秘通信的应用领域比较广泛，例如可以用于电子选举和电子现金的解决方案，防止选民或者购买者的身份暴露。

# 信息隐藏关键技术[[4]](#footnote-3)

近年来，信息隐藏技术蓬勃发展，取得了长足进展，但在其中有这样一些技术扮演着关键角色

## 替换技术

所谓替换技术，就是试图用秘密信息替换载体中不重要的部分，以达到对机密信息进行编码的目的。替换技术是在空间域进行的一种操作，通过选择合适的伪装载体和适当的嵌入区域，能够有效地嵌入机密信息，同时又可以保证数据的失真度在人的视觉允许范围内。替换技术算法简单，容易实现，但是鲁棒性很差，不能抵抗图像尺寸变化、压缩等一些基本的攻击，因此在数字水印领域中一般很少使用。

## 变换技术

大部分信息隐藏算法都是在变换域进行的，其变换技术包括离散傅里叶变换（DFT）、离散小波变换（DWT）等，这些变换技术都有各自的特点。

## 扩频技术

当对伪装对象进行过滤操作时，可能会消除机密信息，解决的方法就是重复编码，即拓展隐藏信息。在整个伪装载体中多次嵌入一个比特，使得隐藏的信息在过滤之后仍能保留下来。这种方法会导致传输效率降低，但会使载体和隐藏信息这一整体更加安全，提升整体的安全性。

扩频技术一般是使用比发送的信息数据速率高许多倍的伪随机码，将载有信息数据的基带信号频谱进行扩展，形成宽带低功率谱密度信号。最典型的扩频技术，为直序扩频和跳频拓频。直序扩频是在发端直接用具有高频率的拓频编码去扩展信号的频谱，而在接收端用相同的扩频编码解扩，将扩频信号还原为原始信号。跳频扩频是在发端将信息码序列于扩频码序列组合，然后按照不同的码字去控制频率合成器，使输出频率根据码字的改变而改变，形成频率的跳变；在接收端为了解跳频信号，要用与发端完全相同的本地扩频码发生器去控制本地频率合成器，从中恢复出原始信息。

# 国内外研究现状

### 5.1 国际信息隐藏研究会

信息隐藏研究可以追溯到古老的隐写术，但在国际上正式提出信息隐藏研究则是在1922年。

国际上的第一届信息隐藏研究会于1996年在剑桥大学举行，这次会议推动了信息隐藏的理论和技术研究。1998年在美国俄勒冈州召开了第二届信息隐藏研究会，1999年9月29日～10月1日在德国Dresden召开了第三届信息隐藏研讨会。最近IEEE ICIP，EUSIPCO的会议中也都研讨了信息隐藏。如今，信息隐藏已经成为当前国际上的研究热点。

### 5.2 国内信息隐藏研究会

《全国信息隐藏暨多媒体信息安全学术大会》（CIHW），开始于1999年，到目前为止已经举行了15届。研讨会的交流内容涵盖了隐藏理论与模型，隐密术与隐密分析，数字水印与数字版权管理，数字水印技术与防伪，非常规载体信息隐藏，数字取证，软件保护等问题，研讨会所收录的论文代表了国内信息隐藏技术学术研究的较高水平。同时，研讨会的召开，为致力于信息隐藏技术研究的专家学者提供了广泛的交流学习机会，在一定程度上促进了我国信息隐藏技术的研究和应用。

### 5.3国外信息伪装学术机构

目前国外研究信息伪装的学术机构又麻省理工学院的媒体实验室、IBM等一些机构和大学，研究的重点在于如何将信息隐藏到图像、声音和文字等载体中。目前对于信息隐藏技术多应用在数字产品的著作权保护方面（即数字水印）。瑞士洛桑联邦工技院信号处理实验室和通信研究所、美国的NEC研究所，中国的台湾国立交通大学等都去了不少的成就。除了学术界的研究以外，一些公司也开发出了不饶软件用以提供数字产品著作权保护的服务，例如：Fraunhofers SYSCOP，HIGHWATER FBI， Digimarc Corporation， DICE's Argent Digital watermark等等。

### 5.4国内信息伪装学术机构

当前国内研究信息伪装的科研院所有：北京邮电大学信息安全中心，中国科学院自动化研究所模式识别国家重点实验室，北方工业大学，清华大学，北京理工大学，北京电子技术应用研究所，国家信息安全测评认证中心等单位。

# 总结

与加密技术相比，信息隐藏技术的优势在于我们不仅可以应用公用信道，而且可以将明文隐藏到普通的媒体中，使攻击者难以发现秘密信息的存在，从而真正达到秘密通信的目的——信息隐藏技术作为信息安全技术的新生主力，在保障信息安全的潜力方面无疑不可估量。

对于信息隐藏技术：一方面其能够帮助完善国家信息安全体系，提高国家信息安全水平；另一方面又能提高网络信息检测能力，维护国家安全。更不用提其应用领域遍及军事、政治、经济、文化等。信息隐藏技术无疑将会在现代信息安全事业中发挥着重要作用。

参 考 文 献

[1] 王贤敏《机密空间信息隐藏与遥感影像授权使用》2005

[2] 娄振华 《信息隐藏的安全性研究》2008

[3] 李晓璐 《基于内容的生物图像秘密隐藏方法研究》2009

[4] 陈凌云《图像信息隐藏技术的应用研究》2008

[5]“信息隐藏”MBA智库

[6]中国声谷先进制造业集群企业专访 第二十二期 “创新信息隐藏技术 做数据安全的守护者”

[7]程明《关于网络信息技术安全的探究》 2014

1. [↑](#footnote-ref-0)
2. [↑](#footnote-ref-1)
3. [↑](#footnote-ref-2)
4. [↑](#footnote-ref-3)