信息隐藏技术研究综述

姜志凯

(南开大学 网络空间安全学院, 天津 300071)

摘 要 随着互联网、计算机以及数字技术等新兴技术的不断发展，在某些领域，传统密码学已不能很好地起到保护信息的作用，因此，古老的信息隐藏技术进过现代化改进，重新登上了历史舞台，以其破解难度大、覆盖范围广、安全系数高等特点被应用于知识产权保护、政治、军事、国家安全等众多领域。本文将从信息隐藏技术的概述、特征入手，简单介绍信息隐藏技术的研究背景、研究意义、国内外研究进展、关键技术、分析以及相关的应用领域，并提出自己的总结与展望。

关键词 信息隐藏；特征；嵌入算法；数字水印

中图法分类号 TP309

A review of information hiding technology

JIANG Zhi-Kai

(School of Cyberspace Security, Nankai University, Tianjin 300071,China)

Abstract With the continuous development of Internet, computer and digital technology and other emerging technologies, in some fields, traditional cryptography has been unable to play a good role in protecting information. Therefore, the ancient information hiding technology has been modernized and improved, and re-entered the historical stage. It has been applied in many fields such as intellectual property protection, politics, military, national security, etc, thanks to it's difficulty to crack, wide coverage and high safety factor. This paper will start from the overview and characteristics of information hiding technology, briefly introduce the research background, research significance, research progress at home and abroad, key technologies, analysis and related application fields of information hiding technology, and put forward my own summary and outlook.

Key words Information hiding; Characteristic; Embedding algorithm; Digital watermarking

1 引言

千百年来，为了保证生产生活有序进行乃至国家安全，必须对部分信息进行保护，信息安全强调信息本身的安全属性,主要包含:信息的机密性,信息不泄露给未授权者的特性;信息的完整性,保护信息正确、完整和未被篡改的特性;信息的可用性,信息可被授权用户访问,并按其要求运行的特性。为了对信息进行有效的保护，人们研究出了各种信息安全技术，包括：密码技术、防火墙技术、信息加密技术、身份认证技术、安全协议等。历史证明，密码技术是保护信息机密性的一种最有效的手段。通过密码技术，人们将明文加密成敌人看不懂的密文，使得信息不会泄露。但是，随着互联网、计算机以及数字技术等新兴技术的不断发展，敌人破解密文的能力也越来越高，信息的安全性也被削弱，更加“高明”的信息保护技术亟待研究。密码技术的一个明显的漏洞就是，通过开放的密文间接告诉黑客，我这有重要信息，快来破解，这使得黑客破解密码的技术随着密码技术的发展而发展。因此，某些情况下必须换一种思路，即隐藏信息的存在，重新启

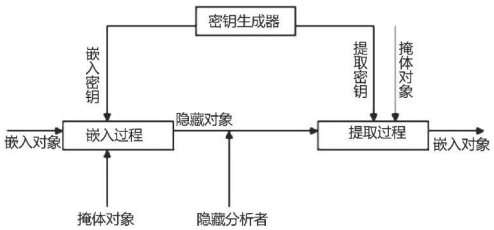
姜志凯，男，2001年出生，本科生，专业信息安全，E-mail：2011937@mail.nankai.edu.cn

用古老的信息隐藏技术，并对其进行现代化改进，从而迷惑、麻痹对手，达到保护信息的作用。本文就从研究背景、意义、历史、国内外进展、主要技术介绍及应用等方面介绍一下信息隐藏技术。

2 信息隐藏技术概述及特征

2.1 信息隐藏技术概述

信息隐藏也称作数据隐藏(Data Hiding)，是集多学科理论与技术于一身的新兴技术领域。信息隐藏技术主要是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，使人难以发现隐藏信息的存在，进而达到保护信息的目的。下图为信息隐藏系统模型，由 4 个主要部分组成：嵌入信息、提取信息、生成密钥和隐藏分析。



嵌入对象：待隐藏的秘密信息；

掩护对象：将用于隐藏嵌入对象的公开信息；

嵌入信息：通过使用特定的嵌入算法，可将嵌入对象添加到可公开的掩护对象中，从而生成隐藏对象；

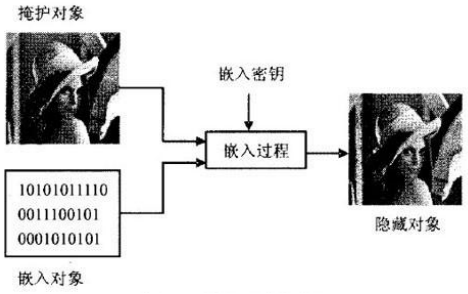
提取信息：使用特定的提取算法从隐藏对象中提取出嵌入对象的过程；

嵌入密钥：在嵌入过程中我们使用嵌入密钥将嵌入对象嵌入掩护对象中，生成隐藏对象；

提取密钥：在提取密钥的参与下从所接收到的隐藏对象中提取出嵌入对象；

隐藏分析：隐藏对象在信道中进行传输，在传输的过程中，有可能会遭到隐藏分析者的攻击，隐藏分析者的目标在于检测出隐藏对象、查明被嵌入对象、向第三方证明消息被嵌入、删除被嵌入对象、阻拦等。

下图为将一个 txt 的文本嵌入到一张 JPEG 的图像中的例子。



2.2 信息隐藏技术的特征

2.2.1 隐蔽性[1]

隐蔽性是信息隐藏的基本要求，有两个方面：一是对人体感觉系统的不可感知性。通过信息隐藏过程之后不会显著更改或降解载体，不会影响人对载体信息的理解或引起视觉、听觉等方面的明显变化，避免通过人类的感觉检测到。二是计算机之类的分析系统的不可预测性。躲过了人，还是存在一定的暴露风险，因为信息被隐藏而未被人类识别，这并不意味着分析系统无法检测到该信息，这要求操作员在嵌入信息之前和之后尽量使载体信息保持相同的特性，在计算分析中不能确认是否有信息隐藏。

2.2.2 安全性[2]

隐藏的信息是被藏在宿主图像或声音的内容之中的，而不是藏在头文件等处，因而不会因格式的改变而遭到破坏。同时隐藏的信息具有很强的对抗非法探测和非法破坏的能力。同时也可以将隐藏信息的内容加密，即时被发现，也无法解密该信息。

2.2.3 鲁棒性[1]

鲁棒性是指经过一系列处理或干扰后，载体中隐藏的信息不会被破坏，可以从中提取出完整的信息。这些处理包括重采样、有损压缩、模数转换、滤波、信道噪声以及其他破坏信息的人为攻击。

2.2.4 自恢复性[1]

即使在销毁数据后，也需要能够独立于原始数据，基于其余数据来还原原始隐藏数据。数据在运输、处理和转换过程中将不可避免地被破坏。

2.2.5 信息容量[1]

信息容量是指载体所能隐藏的信息数量。这与载体本身的特性、信息隐藏的算法有关，并且取决于对隐藏信息的鲁棒性的要求。随着机密信息量的增加，对载体本身的影响和损害不可避免地增加，这增加了暴露的风险，同时降低了隐藏信息的鲁棒性。因此，在实际应用中，应该根据需要合理地选取隐蔽性、鲁棒性和信息容量。

3 研究背景及意义

3.1 研究背景

我们先看几个例子：

第一次世界大战中，英国成功破解德国“齐默尔曼电报”，使美国放弃中立地位而对德宣战，最终以英国为首的协约国赢得了战争胜利。

二战初期，因无线电密码被德国人破译，而使北非战场英军详细作战计划被源源不断送到德军将领隆美尔的案头，使英军陷于被动境地，直至更换密码，才使德军不再“耳聪目明”。波兰沦陷后，其密码机构在数学家、现代计算机科学奠基人——图灵领导下，破解了德军九成以上“恩尼格玛”密电文，使德国许多重大军事行动对盟军不再是秘密。对此，英国首相丘吉尔曾称密码破译者是“下金蛋最多的鹅”。

随着多媒体技术和 Internet 的迅猛发展，互联网上的数字媒体应用正在呈爆炸式的增长，越来越多的知识产品以电子版的方式在网上传播。数字信号处理和网络传输技术可以对数字媒体（数字声音、文本、图像和视频）的原版进行无限制的任意编辑、修改、拷贝和散布，造成数字媒体的知识产权保护和信息安全的问题日益突出，并已成为数字世界的一个非常重要和紧迫的议题。因此，如何防止知识产品被非法复制及传播，也是目前急需解决的问题。

由以上可看出，随着数字化进程的不断推进，在政治、经济、军事等领域，信息保护变得愈发重要，有必要研究传统密码学之外的新技术来保护信息，因此，古老的信息隐藏技术重新登上了历史的舞台并进行了现代化的改造。

3.2 研究意义

信息隐藏，是一门体现人类高度智慧的信息安全斗争技术和艺术。从古至今，几乎所有新的信息隐藏手段和技术一旦出现，就立即会被用于情报作战中，不仅演绎出许多惊心动魄、惊险绝伦的故事，而且在一定程度上决定着战争的胜负乃至国家命运。

因此，国际上开始提出并尝试一种新的关于信息安全的概念，开发设计不同于传统密码学的技术，即将机密资料信息秘密地隐藏于一般的文件中，然后再通过网络传递。由于非法拦截者从网络上拦截下来的伪装后的机密资料，并不像传统加密过的文件一样，看起来是一堆会激发非法拦截者破解机密资料动机的乱码，而是看起来和其他非机密性的一般资料无异，因而十分容易逃过非法拦截者的破解。其道理如同生物学上的保护色，巧妙地将自己伪装隐藏于环境中，免于被天敌发现而遭受攻击。这一点是传统加解密系统所欠缺的，也是信息隐藏的基本思想。

信息隐藏的实现既要保证对载体信息的影响不会被人的感知系统所发现，这就从某种程度上限制了隐藏数据的大小，又要尽可能提高隐藏信息的鲁棒性和免疫性，即经过信息的运输转换等过程免遭破坏的能力，这二者就像鱼和熊掌，往往不可兼得，因此实现信息隐藏十分具有挑战性，需要我们不断深入研究。

3.3 信息隐藏与密码技术的区别

区别在于：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。密码技术让信息“不可懂”，而信息隐藏技术让信息“不可见”。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。

4 信息隐藏技术的历史沿革

其实，信息隐藏的思想并不新奇，早在古代时期，人类就用智慧发明了这种信息保护技术，应用在各个领域，发挥着不可磨灭的作用。现代数字化信息隐藏技术是由古老的隐写术(Steganography)发展而来的，隐写术一词来源于希腊语，其对应的英文意思是“Covered writing”。隐写术的应用实例可以追溯到非常久远的年代。古希腊历史学家希罗多德在书中写到，将信息刻在光头上，待头发长出来进行信息传递；古代的藏头藏尾诗；在第一次世界大战中人们制造出了复杂的化合物做成隐写墨水和显影剂，用这些化学物质书写肉眼看不见，只有用其他适宜的化合物或通过某种光、电、热、汽等物理方法才能显示出书写信息；二战时期，一位女钢琴家将信息编在乐谱里，弹奏出来，达到信

息的隐藏目的；利用微缩原理将秘密文件、资料情报缩小至数十或数百乃至数千分之一，制成显微薄片；卡登格子隐藏法；纸币防伪技术等数不胜数的信息隐藏事例。

这些不仅是当时保护信息的技术，更是体现了人类文明的艺术，现代的数字化信息隐藏技术是对古人文明的继承并应用在生活之中。

5 国内外研究进展

信息隐藏研究虽然可以追溯到古老的隐写术，但在国际上正式提出数字化信息隐藏研究则是在 1992 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。中国台湾国立大学通信和多媒体实验室也做了大量的工作。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。

目前，包括麻省理工的媒体实验室、IBM、美国 NEC 研究所、中国科学院自动化研究所模式识别国家重点实验室、清华大学、北京理工大学等在内的多所国内外实验室、研究机构及重点大学致力于研究信息伪装等技术。

目前信息隐藏技术主要包括以下几种：数字水印技术、可视密码技术、潜信道、隐匿协议等。

5.1 信息隐藏的方法

在数字媒体中嵌入隐藏信息的方法主要包括在时间域、空间域和变换域的隐藏。又可以载体的不同分类信息隐藏方法，在文本中隐藏信息、利用阈下信道隐藏信息、利用操作系统中的隐蔽信道来隐藏信息、在可执行文件中隐藏数据、在视频通信系统中隐藏信息，目前研究得最多和最深入的是在静止图像中的隐藏，下面简单介绍几种不同的信息隐藏实现方法。

5.1.1 LSB 算法[3]

LSB 算法在 1994 年由 Schyndel 等人提出，该算法利用载体图像中每个像素的最低位来进行秘密信息的嵌入，如果最低位和秘密信息一致就不发生变化，否则就将 1bit 的秘密信息嵌入该最低位.在恢复时，只要直接从掩体图像的每个像素的最低位提取并组合即可得到秘密信息.LSB 算法隐藏容量大、实现简单但稳定性较差，容易受到攻击.特别是在秘密信息量增大时，掩体图像的直方图分布会发生改变，增大了被攻击的几率.因此，研究者提出了 LSB 匹配算法，在秘密信息嵌入过程中随机选取嵌入位置，并根据待嵌入秘密信息的比特值，让载体图像的最低位随机加 1 或者减 1.本文用来做比较和分析的 LSB 算法都是指 LSB 匹配算法。

5.1.2 Patchwork 算法[3]

Patchwork 算法是由 Bander 等人提出来的，该算法利用图像特征的统计来进行信息的隐藏.在载体图像中随机选择 P 对像素点（ai，bi），并将它们的灰度值按公式（1）进行变换:

$$\begin{cases} a_i = a_i + 1 \\ b_i = b_i - 1 \end{cases} \quad i = 1,2,\cdots,p \tag{1}$$

该算法利用了整幅图像的灰度均值偏移的性质，在不改变整幅图像的灰度均值的情况下提高了整幅图像的对比度.从而针对图像的裁剪、有限冲击相应滤波器和 JPEG 压缩的攻击都有一定的抵抗力，具有较好的鲁棒性.但它不能抵抗串谋攻击，隐藏容量比 LSB 小。

5.1.3 DCT 算法[4-5]

这种算法是,将图像分割成为 8x8 的不重迭的像块,经 DCT 变换后,对其部分交流系数进行调整并嵌入隐蔽信息。较早的算法嵌入点选择的是中频系数,并考虑到了要减少嵌入信息对图像主观质量的影响和尽量避免有损压缩可能造成的损害。由 Cox 等人提出的基于扩频通信技术的频率域水印嵌入算法应该说是对这一技术的重大改进。这一算法旨在兼顾了嵌入信息的不可察觉性和鲁棒性,提出了应将水印信息嵌入图像信息中被感知的重要部分。因为这些部分在有损压缩时还会重点保留,因此可以提高水印的鲁棒性。该算法利用一个平均能量很低的正态分布的随机数字序列作为水印信息,并选取 DCT 系数中除 DC 系数外的部分较低的频率系数进行调制及作为水印信息的嵌入点,所以可抗拒有损编码和对一些会引起失真的信号进行处理。

5.1.4 图像分存[6]

图像分存的含义是,将图像信息分为具有一定可视效果的 n 幅图像,这些图像称为子图像,这些子图像之间没有互相包含关系。如果知道图像信息中的 m(m<n)幅子图像,则该图像可以得到恢复,如果图像信息少于 m 幅,则图像无法得到恢复。其优点在于可以避免由于少数几份图像信息的失窃而造成严重的事故,个别图像信息的泄露不会引起整个

图像信息的泄露,而个别图像信息的丢失也不会引起整个图像信息的损失（与可视密码的思想类似）。下面举一个算法例子。

基于 Shamire(t,n)-阈方案的算法有拉格朗日插值法及采用动直线生成的有理隐式曲线法。当曲线的次数增加时，两种算法呈现出不同的特征，前者由于高次拉格朗日插值法会产生龙格现象，难于满足图像分存的需要，因而应用受限;而动直线生成的曲线推广到高次时，依然稳定可靠，有着较好的应用前景，其原理可推广到采用动曲线和动曲面来进行图像的分存[7]

5.2 数字水印技术[8]

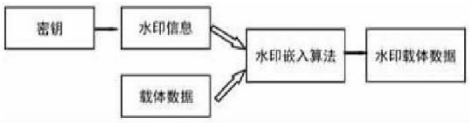
数字水印就是向多媒体数据中添加某些数字信息以达到数字产品真伪鉴别、版权保护等功能。它是一种隐藏于原始图像中的不可见数据，既保护版权又不伤害图像的主观质量和完整性。数字水印是信息隐藏技术的一个重要研究方向。

数字水印技术除了应具有信息隐藏技术的一般特点外，还有其固有的特点和研究方法。它通过一定的算法在被保护的数字多媒体对象（如静止图像、音频、视频等）中嵌入某些秘密信息——水印（watermark）来证明版权归属或跟踪侵权行为。水印这一秘密信息的嵌入，不影响原内容的价值和使用，不能被人的感知系统察觉，并且数字水印必须难以被清除和破坏。这表明，对版权保护应用领域来说，数字水印技术必须具有较强的透明性、安全性和鲁棒性[9]

从图象处理的角度来看，嵌入水印信号就是在强背景下迭加一个弱信号，当迭加的水印信号强度低于 HVS 的对比度门限时，HVS 就无法感到信号的存在。对比度门限受视觉系统的时间、空间和频率特性的影响，因此可以在不改变视觉效果的情况下，对原始图象作一定的调整，如嵌入信息。从数字通信的角度看，水印嵌入就是在一个宽带信道（载体图象）上用扩频通信技术传输一个窄带信号（水印信号）。虽然水印信号具有一定的能量，但分布到信道中任一频率上的能量是难以检测到的。水印的译码（检测）则是一个有噪信道中弱信号的检测问题。设载体图象为 I，水印信号为 W，密钥为 K，则水印嵌入可用如下公式描述:

$$I_W = F(I, W, K)$$

上式中 F 表示水印嵌入策略(算法)。下图为水印信号嵌入模型,其功能是将水印信号加入原始数据中。



数字水印的嵌入算法与基于图像的信息隐藏算法大体相同。

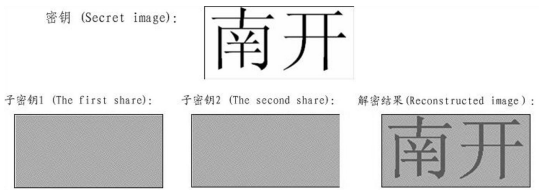
5.3 可视密码技术[10]

可视密码技术(Visual Cryptography):可视密码技术是 Naor 和 Shamir 于 1994 年首次提出的，其主要特点是恢复秘密图像时不需要任何复杂的密码学计算,而是以人的视觉即可将秘密图像辨别出来。 其做法是产生 n 张不具有任何意义的胶片，任取其中 t 张胶片叠合在一起即可还原出隐藏在其中的秘密信息。

可视密码方案实际上是一种秘密共享方案，即使是一个具有无穷计算能力的攻击者，也不能在拥有的子秘密数量少于一个给定值时获得关于秘密图像的任何信息。

与以往技术相比，可视密码的不同之处在于秘密及成员所持有的密文不是一串数值而是图像，而且在还原秘密时不需额外的设备及运算辅助，直接由人类视觉系统来解密，因此解密者不需具备密码学相关知识即可解密，这样就大大降低了成本及使用者的门槛。

现如今，已经提出了许多可视密码技术的拓展形式，如 S-Extended 可视密码，一般存取结构可视密码，像素不扩展型，叠像术，防止欺骗型等。



5.4 潜信道[11]

信道是人们有意设计用来传输各种信号的通道。而潜信道,又名隐信道,它是由 Simmons 在 1978 年为了证明当时美国用于核查系统中的安全协议的基本缺陷而提出的。

顾名思义,潜信道就是指普通人感觉不到又确实存在的信道,因而我们出于安全的需求就可利用这些感觉不到而又真实存在的信道来传送(或存储)机密信息。潜信道的种类很多,有些潜信溢是设计计者有意打下的埋伏,有些潜信道则是无意之中构建的。

潜信道和信隐藏中的另外一个分支——隐写

术的原理是基本一数的,不同的是,在隐写术中,隐藏秘密信息的载体对象是一个或者多个特定的文件,而潜信道技术用的载体对象是整个计算机通信系统。对于潜信道技术的发展和其在计算机秘密通信及数字签名等方面的应用,国外学者已经做了许多研究,而国内对这方面的研究却还处于起步阶段。

大体上，潜信道分为以下几类：

1.冗余型潜信道。对于任何通信系统,只要它允许冗余信息的存在就一定会有潜信道的存在。事实上,冗余信息所在之处就是隐信道。因为我们可以将冗余信息替换成秘密信息。

2 数字签名中的潜信道。事实上以 ELGamal 数字签名方案和 DSS 数字签名方案等为代的大多数数字签名方案中都存在潜信道。这种数子签名中的潜信道也是 Simmons 在 1985 年发现的（阈下信道）。

3.操作系统中的潜信道。如果通信双方都接人同一个计算机系统,就有许多方法来构造潜信道。如,当运行在一个特定安全级别的系统的部分(即一个共享资源能向另一个系统的一部分何能有不同安全级别提供服务时,潜信道就可能出现。此外,在 OSI 风络模型结构中也存在许多可以用来传输秘密信息的潜信道。

5.5 隐匿协议

网络协议信息隐藏（以下简称协议隐写）是一种利用数据包作为掩护载体，将秘密信息隐匿在网络协议的数据包之中的信息隐藏技术，它可以通过网络协议数据包中的保留、可选、未定义等字段和数据包的顺序、数量、到达时间、特定时间流量以及其它可被利用的特征，在网络中不同的主机之间建立隐蔽通信。大体上分为网络层、传输层和应用层网络信息协议的隐藏技术[12]

6 信息隐藏技术的分析

信息隐藏分析的目的就是如何判断一个看似普通的信息中是否隐藏有别的机密信息。信息隐藏分析与信息隐藏显然是一对矛盾中的两个方面。到目前为止，人们在信息隐藏的研究方面已经取得了不少有意义的结果，但是在信息隐藏分析方面的研究工作才刚刚开始。隐藏分析是发现隐藏的消息并使这些消息无效的一种技术。信息隐藏分析与密码分析有许多相似之处。密码分析者试图读懂加密信息，信息隐藏分析者试图检测隐藏信息的存在。在密码分析中，是对部分明文（也可能没有明文）和部分密文进行分析、在信息隐藏分析中，是在载体对象、伪装对象和可能的部分消息之间进行比较。密码技术的最终结果是密文，而信息隐藏技术的最终结果是伪装对象。被隐藏的信息可以加密也可以不加密，若隐藏信息是加密的，那么即使是隐藏信息被提取出来了，为了明白嵌入信息，也还需要应用密码破译技术。

下面列举几种基本的信息隐藏分析方法：

唯隐藏对象攻击；已知载体攻击；已知消息攻击；选择伪装对象攻击；选择消息攻击；已知伪装载体和伪装对象攻击；感官攻击；结构攻击；统计攻击；稳健性攻击；表达攻击；解释攻击；合法攻击等。

信息检测研究的意义在于，一方面可以促使信息隐藏技术被合法使用，另一方面可以进一步促进隐藏算法的深入研究。

7 信息隐藏技术的应用

信息隐藏技术由于其难以破解的特点，在很多领域都有应用。信息隐藏的最直接应用就是机密通信。在发信端，将待保护的信息隐藏到公开的信息中，再通过公开信道传给收信方。在收信端，根据事先约定好的信息隐藏提取法从收到的信息中提取出机密信息。现在，能够实现机密通信的方法已经不少了，比如，加密通信、扩展频谱调制、流星散射传输、跳频通信等。与加密通信类似，基于信息隐藏的机密通信也可以分为三类：无密钥信息隐藏通信、私钥信息隐藏通信和公钥信息隐藏通信。除此之外，还可用于攻击“多安全级别”系统；再某种场合隐匿自己的身份，如个人隐私；实现匿名通信；数字水印技术保护知识产权；电子商务中用于数据保密、防伪等。

8 总结与展望

信息隐藏技术经过现代化发展，形成了破解难度大、覆盖范围广、安全系数高等特点，已成为信息保护领域不可或缺的一部分，其与密码技术相结合，可以使信息的安全性大大提升。信息隐藏技术的研究小到影响个人隐私的保护、知识产权的保护，大到事关国家的根本利益，作为未来情报战的重要组成部分，信息隐藏技术必将对战争的进程和胜败产生重大影响。目前国内外对于信息隐藏技术的研究已经逐步完善，渐成体系，但某些领域的研

究，如潜信道等领域的研究还需进一步完善。对于潜信道的研究，国外已取得初步进展，而我国还刚刚起步，未来还需要深入研究。

许多问题如鲁棒性、真伪鉴别、版权证明、音频、视频及软件水印等方面仍需比较完美的解决方案。对于载体的选取，什么样的载体可以在隐藏大量信息后还能保持品质不被人的感知系统所察觉；什么样的隐藏方式，可以既能隐藏大量信息，又不会过大地破坏载体品质；如何在隐藏大量信息后尽量降低对产品鲁棒性和免疫性的影响……，这些因素之间的平衡，需要不断地探索。

现代化信息隐藏技术虽然是新兴技术，但发展迅速，技术种类分支繁多，本文仅介绍了其中一小部分技术，以及部分技术中的部分方法，无法面面俱到，欠缺地方还很多，望批评指正。作为一名信息安全专业的本科生，我需要学习的东西还很多，以后我会继续学习更多的专业知识，持续关注国内外信息隐藏技术的发展，争取今后能在相关领域获得突破，做出贡献。

参 考 文 献

[1]展鹏飞.信息隐藏技术及应用领域研究[J].无线互联科技,2021,18(18):85-86.

[2]刘峰，张鹏.信息隐藏技术及其应用[J].天津大学电子信息工程学院，1006-7442<2001>01-0001-04

[3]卢利琼,吴东.基于图像的空域隐藏算法研究[J].岭南师范学院学报,2015,36(03):105-111.

[4]C -T.Hsu.J-L Wu . Hidden walemarks in images.IEEETrans on Image Proxxswing.1999,8(1):58-68

[5]I. Cox etc Sexume spread spectrum waleark ing fa multimeedia . IEEE Trans on Imag Proxsesing 1997,6(12):1673~1687.

[6]林榕,董克权.基于图像的信息隐藏技术综述[J].装备制造技术,2007,(06):78-80.

[7]闫伟齐,丁玮,齐东旭.一种基于动直线的多幅图像分存方法[J].软件学报,2000,(09):1176-1180.

[8]庄建忠.数字水印技术研究[J].电脑知识与技术,2009,5(24):6779-6781.

[9]廖继旺,彭可.一种可用于版权保护的小波包数字水印技术[J].科技信息,2009,(24):32-33.

[10]Stefan Droste. New results on visual cryptography, LNCS 1109, Advances in Cryptology, Proceedings of Crypto'96, Springer Verlag, 1996, 401-415

[11]黎静.IP 数据报中的潜信道分析[J].四川教育学院学报

[12]葛金明.基于 Internet 网络协议的信息隐藏技术[J].科技资讯,2010(05):12+14.DOI:10.16661/j.cnki.1672-3791.2010.05.167.