基于信息隐藏技术的综述报告

陆皓喆[1)]

[1)](南开大学网络空间安全学院 天津 300350)

摘 要 本文主要概括介绍了信息隐藏技术的研究背景、信息隐藏技术的研究意义、信息隐藏技术的国内外的研究进展、本人对于信息隐藏技术研究的总结以及信息隐藏技术未来发展方向的期望。信息隐藏技术将信息嵌入传输载体的数字媒体中，利用数字媒体本身存在的数据冗余性和人类视觉感知系统的不敏感性，借助密码学、混沌理论、数字图像处理等技术对隐秘信息进行隐藏。它很好的实现对隐秘信息的有效保护，达到了信息在通信中安全传输的目的。信息隐藏技术与实际生活密切相关，因此信息隐藏技术在生活中被广泛应用。

关键词 信息隐藏技术；信息安全；通信；数字图像处理；数据冗余

Review report based on Steganography

Haozhe-Lu[1)]

[1)] (College of Cyber Science,Nankai University,Tianjin 300350)

Abstract This paper mainly introduces the research background of cryptography, the research significance of cryptography, the research progress of cryptography at home and abroad, my summary of cryptography research and the expectation of cryptography in the future development direction. Cryptography embeds information into the digital media of transmission carrier. It uses the data redundancy of digital media itself and the insensitivity of human visual perception system to hide the secret information by cryptography, chaos theory, digital image processing and other technologies. It achieves the effective protection of secret information, and achieves the purpose of safe transmission of information in communication. Cryptography is closely related to real life, so it is widely used in life.

Key words Cryptography; Information security; Communication; Digital image processing; Data redundancy

0 引言

伴随着互联网科技的高速进步以及移动设备的全面开花，越来越多的用户开始通过网络进行数据传输以及在互联网上发布自身的实时动态。如何确保在这个过程中的数据安全得到充分保证，已逐渐成为社会各界尤为关注的话题。近几年来，信息隐藏技术以其在隐秘通信和知识产权保护方面的显著优势，已然成为信息安全领域研究和关注的重点，受到了广大领域的广泛应用[1]。深入了解信息隐藏技术的各种类型，紧密关注其国内外发展的现状，有助于我们更有效地推动信息隐藏技术的发展和应用。

1 研究背景

1.1 信息隐藏技术的研究历史

信息隐藏技术（Steganography）是一门涉及隐藏信息在其他非明显载体中的技术。这种技术的目的是在不引起注意的情况下传递信息。与加密不同，它不是为了隐藏消息的内容，而是为了隐藏消息的存在。

研究信息隐藏技术的背景可以追溯到古老的

历史时期。在古代，人们就已经开始使用隐藏文字、隐藏消息的方法来保护信息的安全。[2]例如，古代的一些文献提到使用某种特定的墨水在纸张上书写信息，然后用另一种液体覆盖，只有在特定光照条件下才能看到隐藏的信息。

然而，现代信息隐藏技术主要受到数字化和计算机科学的发展影响。随着数字图像、音频和视频的普及，人们开始利用这些媒体载体来隐藏信息。其中最著名的例子是数字图像隐写术，它通过在图像中嵌入信息（通常是文字、图像或其他数据）而不影响图像外观来实现。

1.2 研究背景的分类

1.2.1 隐写术研究

专注于在图像、音频、视频等媒体中隐藏信息。这包括设计算法和方法来嵌入和提取信息，同时确保信息的安全性和完整性。

1.2.2 安全通信

信息隐藏技术在安全通信中扮演重要角色。它可以用于隐蔽传递机密信息，例如，在数字水印领域用于保护知识产权和版权。

1.2.3 隐私保护

在隐私领域，信息隐藏技术可以用于隐藏或模糊敏感信息，以防止隐私泄露。

1.2.4 数字水印

数字水印是信息隐藏的一个子领域，它专注于在数字媒体中嵌入不可见的标识，用于验证真实性、版权保护或跟踪来源。[3]

1.3 数字水印的未来

信息隐藏技术的研究已经成为信息安全、网络安全和数字媒体领域的一个重要分支。随着技术的不断发展，对隐写术和相关技术的研究也在不断进步，以适应不断变化的安全需求和威胁。

2 研究意义

研究信息隐藏技术具有多方面的意义，涵盖了信息安全、通信隐私、数字版权保护等多个领域。以下是关于信息隐藏技术研究的一些重要意义。

2.1 隐私保护和通信安全

信息隐藏技术可以用于隐蔽地传递机密信息，从而确保通信的安全性。通过将信息嵌入到其他媒体中，可以防止敏感信息在传输过程中被窃听或截获。

2.2 数字版权保护

数字水印是信息隐藏的一种应用，可用于保护数字内容的版权。通过在数字媒体中嵌入不可见的标识，可以追踪和验证内容的来源，防止未经授权的复制和传播。

2.3 抵抗隐写分析

随着信息隐藏技术的发展，隐写分析也在不断进步。对抗隐写分析是信息隐藏研究的重要方面，以确保嵌入的信息不容易被检测和破解。

2.4 网络安全与数字取证

信息隐藏技术对网络安全和数字取证领域具有重要影响。它可以用于在网络通信中隐藏恶意活动的迹象，同时也可以用于数字取证，以发现并还原隐藏的信息。

2.5 社交媒体与隐私保护

随着社交媒体的普及，人们分享大量个人信息。信息隐藏技术可以用于保护用户的隐私，通过在图像或其他媒体中隐藏个人信息，以减少潜在的隐私泄露风险。

2.6 安全水印技术

在医疗图像、地理信息系统（GIS）等领域，安全水印技术可以确保数据的完整性和真实性，防止未经授权的篡改。

2.7 对抗信息战争

在信息战争中，隐藏和保护通信的重要性愈发显著。信息隐藏技术可以用于确保军事、政府和企业之间的敏感信息在传输和存储中的安全。

2.8 研究意义的总结

总体而言，信息隐藏技术的研究意义广泛而深远，涉及到信息安全、隐私保护、版权保护等多个领域，为数字化社会的各个方面提供了重要的支持

和解决方案。

3 国内外的研究进展

3.1 国际上的研究进展

随着互联网科技的迅猛发展，信息隐藏技术开辟了广阔宽广的发展前景以及广泛的应用场景。全球学术界对于信息隐藏领域的研究及其重视程度均达到空前的高度。自 1996 年伦敦剑桥首次召开的信息隐藏学术研讨会以来，学术界陆续于 1998 年 4 月份在波兰召开第二届代表性会议，1999 年 9 月份在德国召开第三届；第四届于 2001 年 4 月份在美国揭幕，2002 年 10 月份在荷兰迎来了第五届，而第六届则于 2004 年 10 月份在加拿大繁华的多伦多正式举办。上述几次学术会议显著推动了信息隐藏理论与技术的蓬勃发展。另一方面，诸多全球知名学府例如伦敦剑桥大学、美国麻省理工学院、MIT 大学，德国的 Erlangen-Nuremberg 大学，IBM 研究中心，NEC 美国研究所及至关重要的 AT&T Bel 实验室等众多科研机构纷纷设立专门的部门投入到该领域的研究工作中。此外，欧州共体也积极推动相关研究项目的深入进展。国际标准化组织也提出了 MPEG-4 的参照架构，这一框架允许将视频编码，加密技术以及水印技术有机地融合在一起。

下面简单介绍几种国际上通用的信息隐藏技术。

3.1.1 嵌入标志型信息算法

Hirose 在相关文献[4]中阐述了一种在 C 源代码中嵌入用户独特标识的算法。该算法主要原则是通过一种单一的程序转换来表示一个字节信息。这种程序转换涉及到改变指令的编码方式（例如把 n++转化为 n=n+1），以及调整无依赖关系指令的顺序（例如将 i=1,j=2 修正为 j=2,i=1）等。当执行解码时，只需将被改变的程序与原始程序进行对比，即可获取隐藏在其中的水印信息。这种方法与利用修改文本编排格式来表现水印信息的文档水印技术有着异曲同工之妙。

3.1.2 动态图水印算法

Collberg 和 Thomborson 在相关文献[5]中所提出的动态图水印算法乃当前最具潜力的水印技术之一。该算法的核心构想是采用两枚极度大素数的乘积作为水印信息，然后将其巧妙地融入于程序动态构建的拓扑结构图之中。水印信息的主要编码策略有基数—K 编码，排列图编码，枚举编码以及基于多项式多项式乘积树（PPCT）的编码等等。此种算法与程序运行状态紧密关联，因此具有卓越的隐蔽性及高度的鲁棒性。

3.1.3 基于 JAVA 的水印算法

Akito 和 Hajimu 提出了一种专门针对 Java 程序的水印算法。此算法的基本概念在于在源代码中构造非执行的 if 选择结构，在这种结构体之中插入操作代码。鉴于编译后的 Java 字节码所具有的特性，通过改变虚拟选择结构中的操作码来隐蔽水印信息，因为在 if 结构体中的代码不会被执行，所以对此部分代码进行符合语法规则的修改并不会对软件的正常执行产生影响。但是，该算法的水印存在易于被攻击者察觉且鲁棒性较弱的问题。

3.2 国内的研究进展

在国内学术界，对信息隐藏也给予了高度重视，多次举办信息隐藏技术研讨会。1999 年 12 月 11 日我国信息安全领域的三位院士何德全、周仲义、蔡吉人与北京电子技术应用研究所在北京联合发起召开了中国首届信息隐藏暨多媒体信息安全学术研讨会(CIHW) ,与会专家讨论和分析了我国信息安全面临的形势及信息隐藏技术的发展策略与前景 2000 年 6 月在北京、2001 年 9 月在西安、2002 年在大连、2004 年在广州、2006 年 8 月在哈尔滨、2007 年 11 月在南京、2009 年 3 月湖南、2010 年 9 月在成都、2012 年 4 月在北京邮电大学、2013 年 10 月在西安武警工程大学,先后又举行了十届信息隐藏学术会议,为信息隐藏技术研究提供了一个广阔的学术交流平台，推动了全国信息隐藏研究的发展，促进了多学科交叉研究,展示了国家信息安全领域的最新研究成果。同时，国内也有许多研究机构来从事信息隐藏相关的研究，如北京邮电大学的信

息安全中心、北京大学电子学系、中国科学院自动化所模式识别国家重点实验室等，体现了我国对信息隐藏技术的重视。

4 对该研究的总结

鉴于当前互联网环境下，多媒体数据的形式呈现多样化，类型丰富，规模庞大，对于在互联网上通过信息隐藏方式进行通信以及对此类通信进行监测的重要性日益凸显，由于所暴露的信息安全问题也愈发凸显，对信息隐藏技术的深入研究显得尤为重要，并且科学技术的进步和新兴技术的应用为信息隐藏技术提供了坚实的技术支撑。[6]

5 未来发展方向的展望

信息隐藏技术的实现形式多种多样，运用简洁灵活，无疑将在未来更多、更广的信息防护领域发挥作用。然而，目前这项技术仍然处于发展阶段，在理论体系上仍在不断地成熟和完善，尤其是在实际应用环节中还需进一步的改善，例如数字水印模型的构造，抵抗攻击能力的提高等。信息隐藏技术犹如一柄双刃剑，在未来的应用中我们必须全面利用其技术特质，发挥其跨越多个领域、多个学科的整合技术优势，为信息安全的传输尽一份力量。可以预见到，信息隐藏技术在未来将会有着极其广阔的发展空间。

参 考 文 献

[1] 陈波,谭运猛,吴世忠.信息隐藏技术综述.计算机与数字工程，2005.02.

[2] 徐迎晖.文本载体信息隐藏技术研究.北京邮电大学博士论文，2006:12.

[3] 赵翔，郝林. 数字水印综述.计算机工程与设计，2006.06 第 27 卷第 11 期.

[4]Hirose N,Okamoto E,Mambo M.A proposal for software protection. In:The 1998 Symposium on Cryptography and Information Security [C].SCIS’98.Hamanako,1998:2-7.

[5] Christian C ， ThomborsenSoftware water marking:models and dynamicembeddings [C] . In: Aiken A,etal. eds. Proceedings of the 26th Annual SICPLANAIGACT Symposium on Principles of Programming Languages (POPL ’ 99) . Association for Computing Machinery Press.Texas,1999:311-324.

[6] 朱建忠.信息隐藏技术及其应用研究.福建广播电视大学学报，2007 年第 3 期.

Author1, **Haozhe-Lu,born in 2004,now studies in Nankai University.**

Background

Steganography is the technique of hiding information in other non-obvious media. The aim of this technique is to convey information without attracting attention. Unlike encryption, it is not designed to hide the content of a message, but its existence.

The research background of steganography can be traced back to ancient historical period. In ancient times, people have begun to use the method of hiding words and hiding messages to protect the security of information. For example, some ancient texts mention the use of a certain ink to write a message on a piece of paper and then cover it with another liquid so that the hidden message can only be seen under certain lighting conditions.

However, modern steganography is mainly influenced by the development of digitization and computer science. With the popularity of digital images, audio and video, people have begun to use these media carriers to hide information. The best known example of this is digital image steganography, which is achieved by embedding information (usually words, images, or other data) into an image without affecting its appearance.