信息隐藏技术及其攻击方法*)

吴树峰　黄刘生　卢继军　陈国良
(中国科学技术大学计算机科学与技术系　合肥230027)

Information Hiding and Countermeasures*)

WU Shu-Feng　HUANG Liu-Sheng　LU Ji-Jun　CHEN Guo-Liang
(Department of Computer Science and Technology, University of Science and Technology of China, Hefei 230027)
E-mail: lshuang@ustc.edu.cn　http://www.ustc.edu.cn

Abstract Information Hiding Technology has a long history. With the development of Digital Technology, it has become a newly evolved discipline and a hot research area. Since the first Information Hiding Workshop held in 1996, the technology has been widely applied to areas such as multimedia, signal processing and protection of software Intellectual Property, but the research work in secure communication is relatively fewer. Based on success of developing a steganography tool for communication, this article summarizes the current progress in the research of Information Hiding Technology systematically, and analyzes possible countermeasures against various Information Hiding techniques.

Keywords Information hiding, Steganograpy, Steganalysis, Countermeasure

1 引言

近年来，随着数字技术的发展，传统的媒体技术已从模拟化向数字化转变。但数字媒体的易于拷贝和拷贝的保真特性，使版权保护更加困难，从而使数字媒体中隐藏版权信息的研究，成为信息隐藏技术中的数字隐秘术最成功的应用领域。此类技术主要包括两种：水印（Watermark）和指纹（Fingerprint）。它们的区别在于用途不同：水印技术是在数字媒体中嵌入人感官上难以察觉的版权信息，这些信息在数字媒体的传播中难以除去，可以证明数字媒体的版权拥有者；而指纹技术主要用于在数字媒体中嵌入使用者的身份标记，使之在非法传播媒体时难以除去自己的身份标记，从而对司法取证等提供方便，有关它们的具体技术介绍见文[1]。类似的技术亦出现在IP领域（VLSI设计），用来证明设计的拥有者[2]。早期IBM在发布PC机的时候，为了防止对PC ROM的盗版，采用的Software Birthmark技术[3]也可以认为是一种水印技术。此外，在基于内容的图像检索系统中，我们可以利用信息隐藏技术中数字载体和嵌入信息的不可分割性，在返回的图像中嵌入图像的属性信息，但对图像的质量并无大碍[4]。在远程监控和远程医疗等对数据整体一致性要求比较高的领域，也可以应用信息隐藏技术的载体和迁入信息的不可分割性，来提高通信信息的整体一致性。

随着Internet网络的迅速发展，数字通信手段已成为人类社会活动不可缺少的重要组成部分。但由于Internet是一个易受攻击的开放网络，数字通信的安全问题随着电子商务、电子政务的普及将直接危及商业、军事乃至社会和国家的安全。目前，网络通信的安全手段仍以传统的加密通信为主，各种电子邮件加密工具较多。这种通信方法在敌对环境下，对付敌对势力及国家就可能危及通信安全。因为加密通信易引起对手的猜疑及感知"机密信息"的存在，导致强大的对手动用各种手段破密，即使在短时间内不能破密，也已使通信双方的位置或身份信息基本暴露无遗，从而导致此后的通信处于对手的监控之下，此时就意味着通信的安全已经受到损害。如何使对手无法感知"机密信息"的存在，确保通信双方在交换信息时不受对手猜疑，正是数字隐秘术必须研究的内容。根据Kuhn[5]定义：隐秘术是一种通信技术，它的目的恰恰就是要隐藏通信本身的存在。与密码学不同，密码学中的潜在对手是知道有一个机密信息在传输，而隐秘术的目的却是将机密通信的内容隐藏到一些普通的明文信息中，麻痹对手，使其无法感知机密信息通信的存在。遗憾的是隐秘术应用于安全通信领域的研究工作相对较少，这是因为通信的文件容量一般远大于版权信息的容量，其隐藏的难度较大，且目前电子商务及电子政务的普及程度不够。但我们认为，该领域将是一个非常有前途的研究领域，因此我们已开发出一个可用于电子邮件的信息隐藏通信工具[6]。

隐秘术一旦被犯罪分子或敌对力量采用，将会对人类社会和国家安全构成极大的威胁。例如，据新闻报道[7]，本·拉登在策划911行动当中，就使用了隐密术来隐藏有关的通信联络。因此，隐秘分析（Steganalasis）技术及其攻击方法的研究日益重要。同时研究隐秘分析方法能够对设计更健壮的隐秘方法提供帮助。正如密码技术的发展促使了密码分析及其破解技术的发展一样，随着隐秘术的发展，隐秘分析技术及其攻击方法的研究近年来也得到了迅速的发展，并推动了安全操作系统、安全关键数据库系统以及安全通信协议的建立。例如对Covert Channels的研究[8]，致力于建立一个安全的操作系统，以限制进程之间利用进程间通信系统的漏洞进行隐秘通

*)国家重点基础研究发展规划973资助项目(G1998030403)；中科院支持高水平大学建设重点项目。吴树峰　硕士生，主要研究领域为信息安全。黄刘生　教授，博士生导师，主要研究领域为高性能计算，信息安全。卢继军　硕士生，主要研究领域为信息安全。陈国良　教授，博士生导师，主要研究领域为高性能计算。

信，使病毒和木马对系统的侵入变得更加困难；对 Sublimal Channel[9]的研究，致力于发现通信协议中认证机制的漏洞，以消除利用这些漏洞在认证消息中隐藏信息的可能。

2 信息隐藏的原型和基本概念

经典的信息隐藏是 Simmons 于1983年最初用"囚犯问题"[10]做出说明的。Alice 和 Bob 在狱中计划一次越狱，但他们所有的通信都需经过看门人 Willie 的检查。若 Willie 在他们传递的消息中发现任何秘密信息，就会加以阻止，故 Alice 和 Bob 必须找到一种办法来交换隐藏信息。看门人对两个囚犯之间通信的消息可采用不同的对策，当 Willie 仅对囚犯间的通信消息进行检查，若未发现可疑信息就原样传送，则 Willie 被称为消极的看门人 PW(Passive Warden)；若 Willie 不管囚犯之间的通信是否真有秘密消息都进行删改处理，并尽量不改变字面上的原意，则 Willie 就是一个积极的看门人 AW(Active Warden)。传统意义上的信息隐藏(隐秘术)通常针对 PW，只要能够骗过 PW，使其未发现隐藏信息就算成功。而目前在版权保护方面采用的信息隐藏技术(数字水印和数字指纹)就必须面对 AW 的攻击。

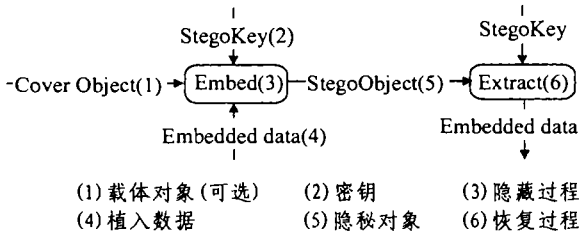

图1

一个通用的信息隐藏模型如图1所示。其中的植入数据是希望秘密发送的消息，它隐藏于一个掩饰性的载体对象(cover object)中。载体对象的类型可以是文本、图像、音频、视频等文件，载体既可以从外界输入到隐藏过程，也可以直接在隐藏过程中产生。隐藏过程的输出是隐秘对象(stego object)。隐藏过程由一个隐秘密钥控制，使得恢复过程仅限于那些已知密钥的人。

信息隐藏技术的安全性准则和加密技术的 Kerckhoff 原则相似，即使对手是 AW，假设他已知我们所使用的隐藏方法，亦可通过密钥的选取来确保安全性。但在保密通信等领域，信息隐藏技术与加密技术相比的优点是它可抵御 PW 的攻击。

3 信息隐藏的技术进展

信息隐藏技术有两个前提：人类的感知分辨能力是有限的；信息隐藏的载体必须有信息冗余。现有的许多信息隐藏软件都是基于这两个前提来达到信息隐藏的目的。

3.1 原始的方法

从信息隐藏的历史来看，它是一种古老而有趣的技术。人们远在古代就已了解到它的重要性，并创造出各种各样的隐藏信息方法。比如，古希腊人将消息写在写字板上，然后在上面覆盖上一层蜡，这样的写字板看上去就像是空白一样，从而躲过检查。最有名的信息隐藏技术是隐形墨水和微写术。隐形墨水曾被大量应用于信息隐藏，不过随着通用显影设备的出现，该方法已基本上被摒弃；另一种古老的技术就是微写术，在极微小的尺度上进行书写或在掩饰文本上打孔，它将图像或文本块按比例缩小成文本中细微的点。随着现代数字技术的发展，信息隐藏技术也发展到了一个全新的阶段。

3.2 以数字图像为载体

数字图像是一种隐藏数据信息的良好载体，现有的大部分研究(包括数字水印技术)也都是针对它来进行的。一般选择载体图像时都会选择较复杂精细的图像。很显然，如果一幅图像有大面积的颜色渐变区域，那么将隐藏信息嵌入之后，在渐变区域中会出现明显的图像失真；而图像越复杂、越精细，它所能隐藏的信息容量也越大，越不易被检测到。

最经典的信息隐藏方法有 LSB(最低有效位算法，也称为噪声插入算法)。它利用人类视觉对某些细微特征不敏感性，修改图像颜色信息的最低有效位，使图像信息产生轻微的变化而不易被人类视觉感知。该方法除了修改图像数据的 LSB 位之外，也可修改图像数据的其它某些位，其实质是在图像中引入高频噪声，因为在图像的低频部分(图像的大片平滑区域)容易被察觉。在文[11]中，作者提出了基于图像分存于多张其它图像中的方法，在得到多张分存图像后，使用他们的算法能够恢复原来隐藏的图像。另有一些隐藏方法如 Patch-Work，Texture Block Coding 使用图像区域为单位来隐藏信息[12]，而不像 LSB 和文[11]等方法隐藏信息的单位是图像的一个像素或者变换域中的一个系数。

更健壮的方法通过直接操作载体图像的变换域，把信息插到图像变换的系数中。由于它把信息插入图像中对人类视觉有意义的部分，而不是采用 LSB 所用的方法，因而可以抵御有损编码和其他一些具有信号失真的图像处理过程。例如，Cox[13]等人提出了一种图像水印方法，他们在数字图像的离散余弦变换中，将水印植入到图像变换后得到的对人类感官敏感的若干个高频系数，这种方法获得的图像对 JPEG 压缩具有高度的健壮性。其它的一些变换，如小波变换[14,15]和离散傅立叶变换[16,17]也都可以用于信息隐藏。

由于 Internet 上许多图像格式是基于调色板的，如 GIF 和 PNG 文件，因此针对这类图像文件的信息隐藏方法也很多。其中主要的方法有两种：第一种是将信息嵌入调色板，而不修改图像本身的数据。例如，对于 GIF 图像，可通过替换指定像素与当前调色板的颜色，改变图像的影射关系来隐藏信息。Gifshuffle[18]使用一种无损图像的信息隐藏方法，它将 GIF 图像的调色板中的颜色集看成是有序集，颜色的每一种排列代表一个整数，用此整数来隐藏信息。这类方法较易实现，但其嵌入的信息较少。第二种方法是将数据嵌入到图像数据区域中。这种方法具有更大的嵌入容量，但比第一种方法更难实现。文[19]给出了一种新的方法来实现在图像中插入信息。它先利用伪随机数发生器来选择嵌入信息的像素点位置，对每个像素点，从图像的调色板中查找与之最相近的颜色。然后从中选择与待嵌入的信息奇偶性相同的颜色，替换原有像素点的颜色信息。此外，扩频(spread spectrum)技术[20]应用于图像水印[21]和隐秘术[22,23]也能产生很好的效果。

在文[24]中，对不同格式图像文件的信息隐藏能力和实现方法进行了讨论。文[25]着重对压缩图像的隐藏能力作了估计。文[26]介绍了目前一些在图像中隐藏信息的工具。

3.3 以数字音频为载体

LSB 方法同样可用于数字音频和视频。相编码[12]是数字音频特有的隐藏方法，将数字音频信号的起始信号的相位作为隐藏信息的手段，音质改变最难以察觉。对数字音频来说，回音隐藏(Echo Hiding)[27]是一种新颖的变换编码技术。它在

文件中插入人类感知无法察觉的短回声(毫秒级),例如在音频信号中插入0.5ms的回声延迟,则代表信号"0";插入1ms的回声延迟,则代表信号"1"。另外根据人类听觉在听到一个强度较高的信号之后的瞬间内对相近频率的弱音不敏感的特点,利用强音来掩饰(Masking)相邻的微弱信号,利用此特性来隐藏信息[28]。此外,图像和音频文件中未使用的文件头部也可用来存放信息。唱片工业界对自身利润的保护,促使了数字音频中嵌入数字水印来证明版权,相关的技术见文[29]。

目前已有很多以数字音频为载体进行信息隐藏的软件。例如,MP3Stego[30]不仅可以有效地隐藏普通信息,还可制作MP3音频文件中的水印,它在压缩过程中隐藏信息到MP3的比特流中;StegoWav[31]和Steghide[32]软件可以将文件隐藏到Microsoft的WAV格式文件中。Steghide采用LSB方法,将信息隐藏到载体中的最低有效位中。

3.4 以数字视频为载体

数字视频和数字图像在作为载体时,很多信息隐藏的方法都是类似的。最常见就是往数字视频中加入版权标志的数字水印信息。

此外,文[33]给出了一种通过电磁发射将信息隐藏到视频中的方法。该方法使隐藏信息对一般用户不可见,而对于那些安装了修改过的电视接收器的用户则可以重现。许多更复杂的方法则是使用扩频技术来植入信息到视频信号中。

需要说明的一点是,从信息隐藏的能力来说,音频、视频文件和图像是一样的。但是作为使用的信息隐藏载体来看,相对更加小巧的图像文件比音频、视频文件要通用一些。

3.5 以文本为载体

以文本为载体的信息隐藏的方法在数字技术出现以前就已经存在了,像藏头诗就是一种信息隐藏的方法,类似的方法如在文章上盖上一个事先设计好的一个模板,模板镂空的地方出现的字(字母)连起来就是秘密的消息。微写术是基于印刷技术的方法,类似的方法有文本间距法(Text Shifting)[34],它使用特定的间距来表示信息,这种技术现在仍然可以应用在数字排版文件格式如PDF、PS中,用作数字水印或者隐藏信息。

与以上基于图像、声音、视频等数字化的模拟信号方法不同,因为文本传递的是信息而不是信号,故文本载体无可用的信号处理模型,而自然语言处理的研究又尚未达到足够成熟的地步,使得以文本为载体实现信息隐藏的难度较大,也使得攻击基于文本语义模型的信息隐藏变得更难。

简单的文本信息隐藏方法(如StegParty[35])一般使用特定的规则在原文中加入语法拼写错误或者使用同义替换的方法来隐藏信息。较为复杂的方法都是根据所要隐藏的信息来产生隐秘文本,而不像其它载体的方法是先选择载体,然后再加工成隐秘对象。例如,Textto[36]事先设定一些句子结构,其中空缺的句子成分是由事先商定好的单词表中的单词来填充,单词的选择则由待隐藏的信息来指导。Textto所产生的文章没有语法错误,但可能会有一些单复数和词形变化的错误。我们则使用Markov链方法实现了一个隐藏信息的工具,生成的隐秘文本类似于被采样的载体文本,其特点是可用来隐藏图像、文本等多种数据类型组合的文件,且被隐藏的文件大小不受限制[6]。

更复杂的方法可采用自然语言处理,使产生的隐秘文章更自然。TextHide[37]是在自动地对载体文本进行同义改写的过程中,将信息隐藏在改写的方法、同义词的选择之中。NiceText[38]能够产生近似自然语言的文本,它采用定制的词汇,模仿给定样本的写作风格来生成文章,或者使用上下文无关的文法来控制输出文章的写作风格,在生成文章的过程中嵌入隐藏信息。文[39]提出的设想是,将他们的基于递归语义网络的文本生成系统用于信息隐藏,在构造特定领域的递归语义网络后,只要将其生成文章时的网络路径选择作为隐藏信息的手段即可,非领域专家很难判断其生成的文章片段是否由机器生成。

文本的版权保护同样要研究数字水印技术[40],由于自然语言处理研究还不成熟,故文本的水印技术较为原始,基于数字排版格式、句子重写或插入空格等方法所研制的文本水印,其健壮性都有待提高。

以上的方法都是针对英语文本,目前对中文文本为载体的信息隐藏技术的研究很少。

3.6 其它载体及方法

除上述讨论的方法外,还有许多其它的载体和方法已被用于信息隐藏。例如,可利用载体中未使用的或保留的空间来存放隐秘信息,这种方法不会导致载体文件的质量下降(如图像失真)。一般来说,操作系统存储文件时通常会在分配给文件的块中留出部分空置的空间,使实现基于文件系统的隐秘存储系统成为可能。隐秘的存储系统使合法用户(知道存储的内容名称和密钥)能够看到和访问存储的信息,而非法用户即使对系统有物理上的访问权也无法知悉被隐秘信息的存在,更不用说去非法查看[41]。

另一种在文件中隐藏信息的方法是创建一个隐秘的分区。正常启动的系统是看不出这些分区的。但若使用一些磁盘配置工具(如,DOS的FDISK),则隐藏的分区就会暴露出来。

OSI网络模型中的协议也有空可钻,如网络传输信息的TCP/IP包的头部就有未使用的空间。其中,TCP包和IP包的头部就分别有6 bit和2 bit的保留位,TCP包中有初始序列值和Ack序列值可供利用,目前基于此方法的隐秘通信工具已经公开出现[42]。在每个通信信道中,可供利用的包数量有成千上万,因此在信道不被怀疑的情况下,这是一种极好的隐秘通信方法。

4 信息隐藏技术的局限性和攻击方法

为了对付犯罪分子和敌对力量利用隐密通信技术来破坏社会和国家的安全,有必要研究隐秘分析技术。而在版权保护领域,为了设计强度更高,更安全的版权标记(水印、指纹),必然要对版权隐藏技术进行性能分析,寻找可能的攻击方法,并且研究盗版者破解版权标记的方法。

上述的隐秘分析和对版权标志的攻击可以说是对信息隐藏技术攻击的两大领域,将其抽象到"囚犯问题",可将攻击技术分成两大类:检查者是PW或者AW。对于在隐秘通信中使用的隐秘术,检查者只要发现了通信内容中含有隐秘消息并采取适当措施,就已挫败了隐秘通信的企图(PW);而对于版权标记,隐藏信息的存在性是已知的,检查(攻击)者的目的就是将其中的标记去除或使其失效,即篡改数字媒体的内容(AW)。当然对经典隐秘术的攻击也包含了AW的方法,而对版权标记的攻击只会使用AW方法。

简单地使用LSB方法在数字媒体中无论是嵌入隐秘通信信息还是版权标记,都是强度最低的。LSB将隐秘信息藏匿于数字媒体的噪音处,检查者只要对通过检查的数字媒体都进行一次低通的降噪滤波,就会极大地破坏隐匿信息而基

本无损于普通信息。对于在静态图像中使用 LSB 嵌入的隐藏信息，目前已有成熟的检测方法。对于操纵调色板来进行 LSB 隐藏信息的方法，都会在调色板中留下明显的特征：同一调色板中相同或相似的颜色多得异常，很容易检测出来甚至直接恢复出隐秘消息[43]；即使是对24位全彩色的图像进行的 LSB 隐藏方法，同样会在图像中留下比较明显的特征：图像中颜色数比正常图像多得多，且相似的颜色亦很多；检测时用 LSB 嵌入信息，隐秘图像的这种特征并不会增强[44]。其它操纵调色板而无损图像的隐藏信息方法无法抵御 AW 的攻击，检查者只需将图像的调色板随机打乱，并相应修改像素索引值，在丝毫不影响正常的图像传输的条件下，挫败在调色板中隐藏信息的企图。基于图像变换域的信息隐藏方法对 PW 攻击比较有效，但对于 AW 攻击，它所隐藏的信息将大受损害，隐藏容量大大降低。在图像中隐藏信息应该采用未公开的图像，否则检查者可使用图像原本进行 Known Cover 攻击[45]。

对于在音频中隐藏信息，Echo Hiding 已可用 Cepstrum 谱分析结合强力攻击(brute force)的方法来消除回音[46]。因为在失同步条件下难以提取隐藏在音频中的信息，所以对于在音频中随机引入无法察觉的短小停顿、对声音进行重新采样、轻微改变音频数据的播放时间长度等隐藏方法可用失同步来攻击[47]。在视频中隐藏信息的特有方法很少，主要原因是数字视频文件太大、不利于传输，且视频技术一般就是音频和图像技术的结合。

因为 Text Shifting 和单词间空格插入法较简单，故容易检测出异于正常文本的特征，并可通过消除这些特征来破坏隐藏信息。Textto 产生的文章具有易被识破的统计特征，如生成的文章中句子结构只有固定的几种，一些单词出现频率异常。其它方法在文本中隐藏信息较困难，故检测其中隐藏的信息也较难。攻击基于词法或语法的隐藏方法需要有很高的自然语言处理能力和计算能力，才能发现被检查信息的异常；或者能对被检查信息进行正确无损的同义改写。

对于基于文件系统的秘密存储方法，若检查者知道秘密存储的方法，隐藏信息就再无藏身之处。基于网络协议包的隐藏效果较差，因为目前的 Internet 路由器很可能会对协议包的保留域进行修改，可以设计对付这种隐秘消息的安全路由器，将保留域值擦除即可。

为了设计更健壮的数字水印技术，同时伴随着盗版的猖獗，使得对数字版权标记的攻击成为目前研究最多的领域。攻击数字水印的手段至少有以下几种[48]：存在性攻击、鲁棒性攻击、解释性攻击。存在性攻击是修改数字媒体的内容，使检测水印的过程无法检测到水印的存在，其实水印依然存在；鲁棒性攻击致力于消除水印或削弱其存在性；解释性攻击则是使数字水印即使最终被检测出来也无法证明其真伪。有的方法是三种攻击兼而有之。Stirmark 是目前对大多数的图像水印系统都很有效的攻击软件[46,47]，Stirmark 在图像中引入微小到难以察觉的随机扭曲、旋转、裁减、拉伸，削弱了数字水印的存在性，同时又扰乱了图像内容，迷惑检测过程。另外 Mosaic 方法针对多数水印软件都要求图像的大小有一个下限的特点，将图像分裂成足够小的碎片，以阻止水印的检测。利用水印的弱点，攻击者可以伪造一个数字水印植入图像中，使其中的真水印无法证明其版权[49]。很多水印系统只需在同一图像中植入多个水印，就可能使所有的水印都无法检测出来，该方法类似对信道的阻塞式干扰。可以说数字水印还远没有达到所宣称的健壮程度，目前已有人提出用可见水印来保护图像版权[50]。

很显然，基于低级信息(如符号和位置)的信息隐藏技术易于受到攻击，而基于高级信息(如图像的内容、文本的语法和语义)的信息隐藏系统则有更好的鲁棒性。

信息隐藏技术到现在还远未发展成熟，比如在隐秘通信发起之前，通信双方必须共享一个秘密(嵌入信息时使用的密钥)，而密码通信并没有这个要求，因此文[34]提出了公钥隐秘术的设想，因为今后一段时间内统计方法仍将是检测隐秘信息的主要有效手段，故只要隐秘系统不改变载体的统计特征，则没有密钥就无法检测出隐秘信息的存在。

结束语 本文介绍了信息隐藏技术的原理和目前基于各种不同载体的信息隐藏技术进展，以及这些技术的局限性及其攻击方法，探讨了信息隐藏技术可能的应用领域，并指出隐秘通信因其重要性将会是一个非常有价值的研究领域。

参 考 文 献

1 Swanson M D, Kobayashi M, Tewfik A H. Media Data-Embedding and Watermarking Technologies. In: Proc. of the IEEE, 1998, 86(6): 1064～1087

2 Qu G. Publicly detectable techniques for the protection virtual components. In: Proc. of the 38th Conf. on Design Automation Conf., 2001. 474 ～ 479

3 Anonymous. Talk on software birthmarks. Counsel for IBM Corporation, BCS Technology of Software Protection Special Interest Group, London 1985

4 Areepongsa S, Kaewkamnerd N, Syed Y F, et al. Exploring On Steganography For Low Bit Rate Wavelet Based Coder In Image Retrieval System. In: Proc. of TENCON '00, , Kuala Lumpur, Malaysia, 2000, 3: 250～255

5 Kuhn M G. Steganography Mailing List, URL: http: // www. thur. de/ulf/stegano/announce. html

6 吴树峰，黄刘生，等. 一个基于 Markov 链方法的文本隐藏信息工具:[技术报告]. 合肥:中国科学技术大学，2001. 9

7 Sieberg D. Bin Laden exploits technology to suit his needs, CNN Sep. 21, 2001 Posted: 11: 16 AM EDT (1516 GMT)

8 Moskowitz I, Kang M. Covert Channels - Here to Stay? In: Proc. of COMPASS'94, Gaithersburg, MD, IEEE Press, 1994. 235～243

9 Simmons G J. Subliminal Channels: Past and Present. European Transaction on Telecommunications, 1994, 5(4): 459～473

10 Simmons G J. The prisoners' problem and the subliminal channel. In: Proc. IEEE Workshop Communications Security CRYPTO'83, Santa Barbara, CA, 1983. 51～67

11 丁玮，齐东旭. 数字图像变换及信息隐藏与伪装技术. 计算机学报，1998, 21(9): 838～843

12 Bender W, Gruhl D, Morimoto N, et al. Techniques for data hiding. IBM System Journal, 1996, 35(3&4): 313～336

13 Cox I J, Kilian J, Leighton T, et al. A secure, robust watermark for multimedia. In: R. J. Anderson, ed. Information hiding: First international workshop, in lecture Notes in Computer Science, Berlin, Germany: Springer-Verlag, 1996, 1174: 183～206

14 Podilchuk C I, Zeng W. Digital image watermarking using visual models. In: Human Vision and Electronic Imaging II, B. E. Rogowitz, T. N. Pappas, eds. San Jose, CA: IS&T, SPIE, 1997, 3016: 100～111

15 Kundur D, Hatzinakos D. A robust digital image watermarking method using wavelet-based fusion. In: Proc. IEEE Int. Conf. Image Processing, Santa Barbara, CA, 1997. 544～547

16 Boney L, Tewfik A H, Hamdy K N. Digital watermarks for audio signals. In: Proc. 1996 IEEE Int. Conf. Multimedia Computing and Systems, Hiroshima, Japan, 1996. 473～480

17 O'Ruanaidh J J K, Pun T. Rotation, scale and translation invariant spread spectrum digital image watermarking. Signal Processing, 1998, 66(3): 303～317

18 Kwan M. GifShuffle. URL: http: // ww. darkside. com. au/ gifshuffle/

19 Fridrich J. A New Steganographic Method for Palette-Based Images. In: Proc. of the IS&T PICS Conf. Savannah, Georgia, 1999. 285～289

20 Scholtz R A. The origins of spread spectrum communications. IEEE Trans. Commun. 1982, 30: 822～853

21 Swanson M D, Zhu B, Tewfik A H. Transparent robust image watermarking. In: Proc. IEEE Int. Conf. Image Processing, 1996, 3: 211～214
22 Marvel L M, Retter C T. A methodology for data hiding using images. In: Military Communications Conf. 1998. MILCOM 98. Proc. IEEE, 1998, 3: 1044 ～1047
23 Marvel L M, Boncelet C G, Retter C T. Spread spectrum image steganography. IEEE Trans. on Image Processing, 1999, 8(8): 1075～1083
24 Mastronardi G, Castellano M, Marino F. Steganography effects in various formats of images. A preliminary study. In: International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IEEE, 2001. 116 ～119
25 Ramkumar M, Akansu A N. Capacity Estimates for Data Hiding in Compressed Images. IEEE Transactions on Image Processing, 2001, 10(8): 1252～1263
26 Johnson N F, Jajodia S. Steganography: seeing the unseen, In: IEEE Computer, Feb. 1998. 26～34
27 Gruhl D, Bender W, Lu A. Echo hiding. In: Information Hiding: 1st Int. Workshop (Lecture Notes in Computer Science), R. J. Anderson, ed. Berlin, Germany: Springer-Verlag, 1996, 1174: 295～315
28 Swanson M D, Zhu B, Tewfik A H, et al. Robust audio watermarking using perceptual masking. Signal Processing. (Special Issue on Watermarking), 1998, 66(3): 337 ～ 355
29 Swanson M D, Zhu B, Tewfik A H. Current state of the art, challenges and future directions for audio watermarking. In: 1999 IEEE Intl. Conf. on Multimedia Computing and Systems, 1999, 1: 19～24
30 Petitcolas F A P. MP3Stego. URL: http: // www. cl. cam. ac. uk/～fapp2/ steganography/ mp3stego
31 Pulcini G. StegoWav. URL: http: // www. radiusnet. net/crypto/steganography/Java/stegowav. zip
32 Hetzl S. Steghide. URL: http: // steghide. sourceforge. net/
33 Kuhn M G, Anderson R J. Soft tempest: Hidden data transmission using electromagnetic emanations. In: Information Hiding: 2nd Int. Workshop (Lecture Notes in Computer Science), D. Aucsmith, Ed. Berlin, Germany: Springer-Verlag, 1998, 1525: 124～142
34 Anderson R J, Petitcolas F A P. On The Limits of Steganography. IEEE Journal of Selected Areas in Communications, 1998, 16 (4): 474～481
35 Hugg S E. StegParty. URL: http: // www. fasterlight. com/hugg/projects/stegparty. html
36 Maher K. TEXTO. URL: ftp: // ftp. funet. fi/pub/crypt/steganography/texto. tar. gz
37 Grosse P. TextHide. URL: http: // www. compris. com/TextHide/en/
38 Chapman M T. Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text. Computer Science Master Thesis at The University of Wisconsin-Milwaukee May 1997, URL: http: // www. ctgi. net/nicetext/
39 Bulhak A C. On the simulation of postmodernism and mental debility using recursive transition networks. Dept Computer Science Technical Reports, Dept Computer Science, Monash Univ, Melbourne Australia: [Technical report CS 96/264]. 1996. 1～12
40 Compris. com GmbH. TextMark - Protect your texts with digital watermarks! URL: http: // www. compris. com/general/en/autoTextMark. html
41 Anderson R J, Needham R, Shamir A. The Steganographic File System. In: 2nd Intl. Workshop on Information Hiding, Portland, Oregon, USA. 1998. 73 ～ 82
42 Rowland C H. Covert Channels in the TCP/IP Protocol Suite. URL: http: // www. psionic. com/papers/covert/
43 Johnson N F, Jajodia S. Steganalysis of Images Created using Current Steganography Software. In: 2nd Intl. Workshop on Information Hiding, Portland, Oregon, USA. 1998. 273 ～ 289
44 Fridrich J, Du R, Long M. Steganalysis of LSB encoding in color images. In: 2000 IEEE Intl. Conf. on Multimedia and Expo, 2000, 3: 1279～1282
45 Bartel J. Steganalysis: An overview. URL: http: // www. sans. org/infosecFAQ/encryption/steganalysis2. htm
46 Petitcolas F A P, Anderson R J, Kuhn M G. Information Hiding - A Survey. Proceedings of IEEE, 1999, 87(7): 1062～1078
47 Petitcolas F A P, Anderson R J, Kuhn M G. Attacks on Copyright Marking Systems. In: Second workshop on information hiding, Lecture Notes in Computer Science, Portland, Oregon, USA, 1998, 1525: 218～238
48 Craver S, Yeo B L, Yeung M. Technical trials and legal tribulations. In: Commun. ACM, 1998, 41(7): 44～54
49 Craver S, Yeo B L, Yeung M. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications. In: IEEE Journal of Selected Areas in Communications, Special issue on copyright & privacy protection. 1998, 16 (4): 573～586.
50 Braudaway G W, Magerlein K, Mintzer F. Protecting Publicly-Available Images with a Visible Image Watermark. Proc. SPIE, 1996, 2659: 126～33

(上接第120页)

表3 CARBA Finder 系统方法与 RM-ODP 函数对应关系表

CARBA MAFFinder 方法	RM-ODP 函数
Register_agent	Engineering Interface Reference Tracking Function
Register_agent_system	
Register_place	
Lookup_agent	Trading Function
Lookup_agent_system	
Lookup_place	
Unregister_agent	Engineering Interface Reference Tracking Function
Unregister_agent_system	
Unregister_place	

总结 移动 agent 不同于基于过程的 RPC(如 OSF/DCE 中的),也不同于面向对象的对象引用(如 OMG/CORBA, OLE/DCOM 和 Java/RMI 中的),其独特的对象传递思想和卓越的特性给开放系统带来了巨大的革新。目前国内技术界大多从人工智能的角度来研究 agent,所以很难实用化;我们另辟蹊径,从开放系统、分布处理的角度对其作深入研究,为移动 agent 的实用化作出了一些有益的探索。我们通过 MASIF 规范建立了 CARBA 结构,并以 ODP 规范为理论工具,验证了 CARBA 具有较高的开放程度,这样从遵循理论到实践,从实践再返回理论的原则,建立了新一代开放系统框架,解决了传统开放系统中协作性、移动性和实时性等问题。

参 考 文 献

1 刘锦德. 对于开放系统内涵的澄清. 计算机应用, 1997, 17(6): 1～3
2 电子科技大学微机所. 开放系统中互操作技术的发展和前景: [中国国防科学技术报告]. 2000
3 OMG Joint Submission Mobile Agent System Interoperability Facility. Nov. 1997. available via ftp: // ftp. omg. org/pub/docs/orbos/97-10-05. pdf
4 张云勇, 胡健, 刘锦德. 新一代开放系统核心架构研究. 计算机科学, 2002, 29(2): 78～80, 59
5 ISO/IEC IS 10746-1 | ITU-T X. 901, ODP-RM Part1: Overview, 1995
6 ISO/IEC IS 10746-2 | ITU-T X. 902, ODP-RM Part2: Foundation, 1995
7 ISO/IEC IS 10746-3 | ITU-T X. 903, ODP-RM Part3: Architecture, 1995
8 ISO/IEC IS 10746-4 | ITU-T X. 904, ODP-RM Part4: Architecture Semantics, 1995