信息隐藏技术在计算机网络战中的应用研究

周 芸[1], 邹振宁[2], 杨志强[2]

(1. 蚌埠坦克学院, 安徽 蚌埠 230013; 2. 电子工程学院, 安徽 合肥 230037)

摘 要: 信息隐藏技术作为信息安全领域的一门新兴学科, 在军事领域有着广阔的应用前景。主要介绍该项技术的含义、构成、分类、方法及在计算机网络战中的应用。

关键词: 信息隐藏; 网络安全; 网络战

中图分类号: TP393.08 文献标识码: A

Research on the Application of Information Hiding Technology in Computer Network Warfare

ZHOU Yun[1], ZOU Zhen-ning[2], YANG Zhi-qiang[2]

(1. Bengbu Tank Institute, Bengbu 230013, China;
2. Electronic Engineering Institute, Hefei 230037, China)

Abstract: As a new subject in the information security field, the information hiding technology has a good prospect in military field. This article mainly introduces the definition, constitution, classification, methods and application of computer network warfare.

Key words: information hiding; network security; network warfare

1 引言

计算机网络战是以计算机网络为主要目标, 以先进的信息技术为基本手段, 在整个网络空间所进行的各类攻防作战的总称。在网络空间的争夺中, 网络既是己方的薄弱环节, 也是对方攻击的重要目标。有效摧毁敌重要网络系统, 迅速达成一定的战略目的, 已成为敌对双方进行全面网络争夺和对抗的焦点, 这种对抗与争夺, 必然促使网络战成为新的作战样式登上战争舞台。信息隐藏技术在网络战中的应用, 可以通过战场 C^4ISR 系统利用文本、数字化的声音、图像等信息作为媒体, 对作战指挥的机密信息进行隐藏传输, 以防信息失密而贻误战机。因此研究信息隐藏技术在网络战中的应用有着重要的现实意义, 应成为今后网络战研究的重要方向。

2 信息隐藏技术

2.1 含义

随着 Internet 的发展, 国际上开始提出并尝试一种新的关于信息安全的概念, 开发设计出一种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普通的文件中, 然后再通过网络传递散发出去。这种技术称之为信息隐藏(Information Hiding) 或更严格地称为信息伪装(Steganography)技术, 它是集多门学科理论和技术于一身的新兴技术领域, 主要是利用人的感觉器官对数字信号的感觉冗余, 以数字媒体或数字文件为掩蔽物, 用空域掩藏和变化域掩藏等方式, 将被藏信息隐藏在掩蔽信息当中。

收稿日期: 2003-10-19

作者简介: 周芸(1975-), 女, 安徽人, 毕业于炮兵学院, 现为蚌埠坦克学院网络管理中心教员, 大学本科, 研究方向: 计算机网络技术; 邹振宁(1972-) 男, 电子工程学院在读研究生, 研究方向: 信息作战理论研究。

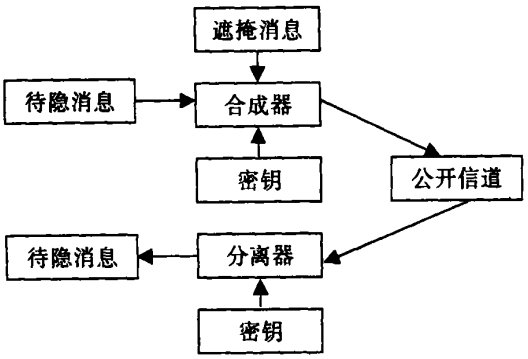

图 1　通常的信息隐藏系统

目前, 信息隐藏技术研究的领域包括信息隐藏、信息的产权认证、信息访问的合法身份认定等。其研究范围则涉及密码学、图像处理、模式识别、数学和计算机科学等领域。计算机网络中的信息隐藏技术, 简单说主要是指将特定的信息(指示、命令、决心、态势图等) 隐藏在数字化宿主信息(如文本、数字化的声音、图像、视频信号等)中的方法。

信息隐藏的目的不在于限制正常的资料存取, 而在于保证隐藏的信息不引起攻击者的注意和重视, 从而减少被侵犯的可能性, 在此基础上再使用密码学中的经典方法来加强隐藏信息的安全性, 可以起到保护信息的安全作用

2.2　构成

信息隐藏系统的构成通常可以用图 1 来表示, 其中合成器用于将待隐信息通过密钥使用某种算法嵌入到遮掩消息中, 形成外部特征与遮掩消息相同的隐写文档。该文档通过公开信道进行传输, 接收到隐写文档的一方, 通过与合成器相对的分离器, 将待隐信息从隐写文档中分离出来。目前通常用文字、图像文件、语音文件以及其它多媒体文件作为遮掩消息。

2.3　分类

随着研究的不断深入, 信息隐藏技术取得了很大的发展, 根据应用目的不同形成了不同的特征, 即不可见性、不可测性和鲁棒性。不可见性是指嵌入信息后不引起原始信息质量的下降, 即不显著改变遮掩消息的外部特征。不可测性是针对怀有敌意的第三方而言, 要求在被隐藏消息的有效期内, 第三方难以检测到某信息中隐藏有其它消息, 或是难以获取被隐藏消息的内容。鲁棒性即要求嵌入待隐藏消息的方法有一定的稳定性, 并且被隐藏的消息不能被轻易地去掉。当隐写文档经过某种改动后, 嵌入的消息应保持其完整性或能够反映出这种改动, 并在一定正确概率的基础上可以被检测到。若敌意的第三方试图通过某些处理去掉或修改嵌入的信息时, 也只应会引起对遮掩消息原有外部特征的明显改变。

3　信息隐藏技术在计算机网络安全中的作用

信息隐藏之所以比密码加密的方法进行保密通信具有自己的优势, 是因为以信息隐藏方式实现隐蔽通信, 除通信双方以外的任何第三方并不知道秘密通信这个事实的存在, 这就较之单纯的密码加密更多了一层保护, 使得网络加密机制从“看不懂”变为“看不见”, 以不至成为好事者攻击的目标。

3.1　数据保密

在因特网上传输的一些秘密数据要防止非授权用户截获并使用, 这是网络安全的一个重要内容。信息隐藏技术在军事上的应用, 可以将一些不愿为人所知的重要标识信息用信息隐藏的方式进行隐蔽存储。像军事地图中标明的军备部署、打击目标, 卫星遥感图像的拍摄日期、经纬度等等, 都可用隐藏标记的方法使其以不可见的形式隐藏起来, 只有掌握识别软件的人才能读出标记所在。

3.2　数据安全可靠

由于隐藏的信息是被藏在宿主图像等媒体的内容之中, 而不是文件头等处, 因而不会因格式的变换而遭到破坏。同时隐藏的信息具有很强的对抗非法探测和非法破解的能力, 可以对数据起到安全保护的作用。

3.3　数据免疫

所谓免疫是指不因宿主文件经历了某些变化或处理而导致隐藏信息丢失的能力。某些变化和处理包括: 传输过程中的信道噪声干扰、过滤操作、再取样、再量化、数/模、模/数转换, 无损、有损压缩、剪切、位移等。

4　算机网络战中对隐藏信息的检测

对隐藏信息的检测主要是为了更好的找到攻击的突破口。目前, 多数研究攻击的重点是如

何破坏被隐藏信息, 它的前提是已知被攻击对象藏有不可见信息。然而, 信息隐藏的最大特点是, 在公共信道或是军事专用信道中信息流量非常大, 里面什么信息都有, 即使在个别信息中隐藏有机密信息, 想要从这么多的信息中将其检测出来, 也不是一件容易的事。况且敌我双方均可以用公共信道来传递秘密信息, 如何从大量看起来不值得怀疑的信息中检测出可能藏有秘密的信息, 是一项很复杂的技术工程。如果不能分辨哪个媒体藏有信息, 使用破坏性攻击技术就无从谈起, 为此检测技术将起到关键的作用。检测技术可以分为异常检测和特征检测两类。

4.1 异常检测

异常检测指根据网络用户的行为和数据包的统计特性来判断是否进行了隐蔽通信, 而不依赖于具体行为是否出现来检测, 检测与系统相对无关, 通用性较强。异常检测主要用到概率统计的方法, 检测器根据网络用户对象的行动建立一个用户特征表, 通过比较当前特征与已存储定型的以前特征, 从而判断是否是异常行为。用户特征表需要根据两个方面的分析结果不断地加以更新。一是对新近出现信息隐藏工具的隐藏方式, 隐藏数据的统计特征分析得出的结果; 二是审计记录。用于描述特征的变量类型有: (1) 流量; (2) 数据包中特征数据分布; (3) 范畴尺度; (4) 数值尺度。

如果假设: $C_1, C_2, \cdots C_n$ 分别是用于描述特征的变量 $N_1, N_2, \cdots N_n$ 的异常程度值, C_i 值越大说明异常程度越大。则这个特征值可以用有 C_i 值的加权平方和来表示:

$$C = {}_1c_1^2 + {}_2c_2^2 + \cdots + {}_nc_n^2, \quad {}_i > 0$$

其中 ${}_i$ 表示每一特征的权重。

如果选用标准偏差作为判别准则, 则标准偏差: $\sigma = \sqrt{C/(n-1) - \mu^2}$ 其中均值 $\mu = C/n$

如果某 C 值超出了 $\mu \pm d\sigma$ 就认为出现异常。

这种方法的优越性在于能应用成熟的概率统计理论。但也有一些不足之处, 如: 统计检测对利用数据包之间的关联性进行隐藏不敏感, 也就是说, 完全依靠统计理论可能漏检那些利用彼此关联事件的隐藏行为; 其次, 定义是否隐藏的判断阈值也比较困难, 阈值太低则漏检率提高, 阈值太高则误检率提高。

4.2 特征检测

特征检测是运用已知隐藏方法, 根据已定义好的隐藏模式, 通过判断这些隐藏模式是否出现来检测。这种方法由于依据具体特征库进行判断, 所以检测准确度很高, 并且因为检测结果有明确的参照, 能为分析管理人员做出相应措施提供了方便。主要缺陷在于与具体系统依赖性太强, 维护工作量大, 而且将具体隐藏手段抽象成知识也很困难, 并且检测范围受已知知识的局限。

5 计算机网络战中信息隐藏的技术支持

5.1 空域算法

空域算法就是直接改变图象元素的值, 一般是在图象元素的亮度或色带中加入隐藏的内容。这种方法比较有代表性的是最不重要比特位 (the least Significant Bits, 简称 LSB) 方法, 该方法也是最早被应用的信息隐藏方法。利用 LSB 算法可以在 8 色、16 色、256 色以及 24 位真彩色图像中隐藏信息。对于 256 色图像, 在不考虑压缩的情况下, 每个字节存放一个像素点, 那么一个像素点至少可隐藏 1 位信息, 一幅 640×480 的 256 色图像至少可隐藏 640×480= 307200 位 (38400db) 的信息。对于 24 位真彩色图像, 在不考虑压缩的情况下, 三个字节存放一个像素点, 那么一个像素点至少可隐藏 3 位信息, 一幅 1024×768 的 24 位真彩色图像至少可隐藏 1024×768×3= 2359296 位 (294912db) 的信息。其主要优点是可以实现高容量和较好的不可见性, 具有很好的隐蔽性, 其原理也比较简单, 实现起来比较容易。但是该算法容易被第三方发现和得到从而遭到破坏, 对图象的各种操作如压缩、剪切等, 都会使算法的可靠性受到影响。

5.2 频域算法

频域算法就是利用某种数学变换, 将图象等用频域表示, 通过更改某些频域系数加入待隐消息, 然后再利用反变换来生成隐藏有其它信息的图象等。目前已有的方法, 主要集中在离散傅立叶变换 (DFT), 离散余弦变换 (DCT), 小波变换 (DWT), 图像自适应嵌入算法等。现以 DCT 变

换域数字水印算法为例作一说明, 其嵌入过程见图 2 所示。

该类算法是水印最初研究的热门问题, 也是目前发展得比较成熟的领域。它具有鲁棒性强、隐蔽性好的特点。传统的算法往往通过修改 DCT 变换后的中、低频系统来实现水印嵌入。之所以选择中、低频系数, 是因为人眼的感觉主要集中在这一频段, 人眼对图像处理过程也不会改变这部分数据。而对高频系数的修改将难以抵御有损编码压缩、低通滤波等攻击。

由于 JPEG、MPEG 等压缩算法的核心是在 DCT 变换域上进行数据量化, 所以通过巧妙地融合水印过程与量化过程, 就可以使水印抵御这些有损压缩。此外, DCT 变换域系数的统计分布有比较好的数学模型, 可以从理论上估计水印的信息量。

离散余弦变换(DTC) 是图像处理中比较常用的一种频域变换。变换定义如下:

$$S(v,u)=\frac{C(u)}{2}\frac{C(v)}{2}\sum_{y=0}^{n}\sum_{x=0}^{n}s(y,x)\cos\frac{(2x+1)u\pi}{2n}\cos\frac{(2y+1)v\pi}{2n}$$

离散余弦反变换(IDCT 变换):

$$S(y,x)=\sum_{v=0}^{n}\frac{C(v)}{2}\sum_{u=0}^{n}\frac{C(u)}{2}s(y,x)\cos\frac{(2x+1)u\pi}{2n}\cos\frac{(2y+1)v\pi}{2n}$$

其中 $u=0$ 时 $C(u)=1/\sqrt{2}$, $u>1$ 时　$C(u)=1$

频率域法有以下优点: 一是嵌入的水印信号能量可以分布到空间域的所有像素上, 有利于保证水印的不可见性; 二是人类视觉系统 HVS 的某些特性可以更方便地结合到水印编码过程中; 三是频率域法可与国际数据压缩标准(如 JPEG, JPEG2000, MPEG 等) 兼容, 从而实现在压缩域(compressed domain) 内的水印编码。

5.3　文档结构微调方法

即在通用文档图像中隐藏特定二进制信息, 使数字信息能经过轻微地调整文档中的结构来完成编码。这些结构包括: 垂直移动行距; 水平调整字距; 调整文字特性。该算法可以抵抗一些标准的文档操作, 如照像复制和扫描复制, 但该技术也容易被经验丰富的攻击者破坏, 而且仅适用于文档图像。

5.4　Patchwork 方法

Patchwork 法是任意选择 N 对图像点, 在增加其一点亮度的同时, 相应的降低另一点的亮度值, 以在这一调整的过程中隐藏 1bit 的信息于数字媒体之中。该算法具有较高的不易查觉性, 并对有损压缩编码(JPEG) 和一些带有恶意攻击的处理等有抵抗的能力。

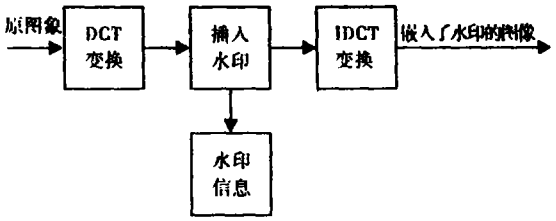

图 2　基于 DCT 变换的数字水印嵌入过程

5.5　纹理块映射编码方法

将数字信息隐藏于数字图像的任意纹理部分之中, 并将隐藏信息的纹理映射到另一纹理相似的区域。该算法对于滤波、压缩和扭转等操作具有抵抗的能力, 但仅适于具有大量任意纹理区域的图像, 且尚不能完全自动完成。信息隐藏实现原理如图 3 所示。

6　计算机网络战中信息隐藏的方法

在现代战争中, 即使通信内容已被加密, 敌方也会从发现一个信号而迅速发起对发送者的攻击。由于信息隐藏技术与其它信息安全技术相比使秘密信息具有更强的不可视性, 因此它在网络战中具有广阔的应用前景, 其隐藏的方法主要有:

6.1　利用扩展频谱通信传递信息

扩展频谱通信就是将待传送的信息数据用伪随机编码调制, 实现频谱扩展后再传输, 接收端采用同样的编码进行解调和相关处理, 恢复原始信息数据。在作战指挥过程中利用这种信息隐藏技术, 将消息拆分成简短的连续部分, 把集中于较窄频段的待传送信息展宽到较宽频带, 通过一个预先安排好的频率序列发送出去, 实现信息在更广泛的频率带宽上进行传输, 达到隐蔽通信的目的。

6.2　利用流星猝发通信传递信息

利用微流星体电离轨迹进入地球大气层时反射无线电波的特性建立起来的通信称为流星

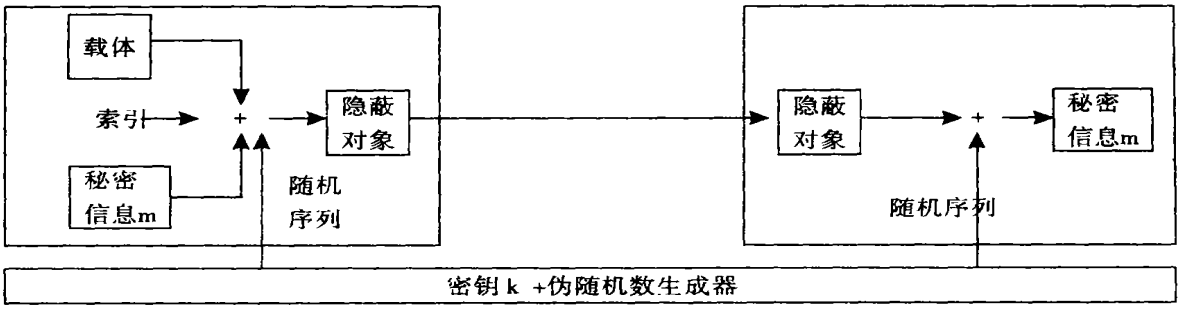

图 3 信息隐藏实现原理

猝发通信, 具有轨迹迅速散射, 信号强度快速衰减等特征, 在作战指挥信息传达过程中, 利用流星轨迹发送猝发数字数据, 可以达到信息隐藏的目的。

6.3 利用文本文件传递信息

在信息传输过程中, 将秘密信息经加密后嵌入到所选定的文本(该文本本身不包含秘密信息, 不应引起敌方的注意)中, 通过选定的传输线路将伪装对象传递给接收方。接收方利用相应的密钥把秘密信息提取出来, 从而实现隐蔽通信。

6.4 利用视频通信传递信息

在利用视频通信系统进行秘密通信时, 发送方将秘密信息经过加密嵌入到所选定的视频流中, 通过选定的传输线路将伪装对象传递给接收方。接收方利用相应的密钥把秘密信息提取出来, 从而实现隐蔽通信。

6.5 利用图像、数字声音传递信息

在利用图像、数字声音传递秘密信息时, 发送方将秘密信息经过加密嵌入到所选定的图像、数字声音文件的噪声成份中, 通过传输路线将伪装对象传递给接收方。接收方利用相应的密钥把秘密信息提取出来, 从而实现隐蔽通信。

此外, 为了控制秘密信息在系统中的访问权限和防止秘密信息意外失、泄密, 必须对密钥的使用进行严格的控制。对于不同密级的信息在嵌入伪装载体时采用不同的密钥, 同时对于不同的用户根据其访问权限赋予不同的密钥。这样对于同一个伪装对象, 即使所有用户都能访问到, 但对于其中的秘密信息, 只有拥有相应密钥的用户才能提取出来, 其它用户无权, 也无法提取出来。这样就从技术上控制了对秘密信息的访问权限和秘密信息在系统内部的安全。

7 结束语

任何一种信息安全技术都不是完美、无懈可击的, 信息隐藏技术在实际应用中也需要一定的条件并有其自身的局限性。为了减少秘密通信的双方的存取难度, 一般要求嵌入方和提取方拥有相同的密钥。信息隐藏技术的局限性主要体现在两个方面: 一方面, 秘密信息被嵌入伪装对象中, 它的传输方法、途径和信道都将由伪装对象决定, 如果伪装对象在传输过程中被干扰、破坏, 那么秘密信息的安全性将无法保证; 另一方面, 敌方若拥有相同的技术就有可能在通信信道上对嵌有秘密信息的伪装对象进行检测, 并证明秘密信息的存在, 甚至有可能提取出秘密信息。既便是无法提取出秘密信息, 敌方也可能以同样的算法嵌入一些无关的信息, 以至于在不破坏伪装对象的情况下使秘密信息无法被正确提取。因此, 为了抵抗各种可能的攻击, 必须选择合适的伪装载体并不断改进嵌入算法。

参考文献

1 罗守山. 信息隐藏技术[J]. 中国数据通信, 2002, (10)
2 周瑞辉. 信息安全的新兴领域—信息隐藏[J]. 计算机应用研究, 2001, (7)
3 苏育挺. 隐蔽通信中的数据伪装技术[J]. 天津通信技术, 1998, (3)
4 李燕. 数字媒体版权保护和信息保密的新途径—数字水印技术[J]. 桂林航天工业高等专科学校学报, 2002, (2)
5 郭震华. 隐藏信息及其对抗方法的研究[C].

(下转第 54 页)

假设齿轮的第Ñ 组公差的精度等级是 9 级, 第Ò 组公差的精度等级是 8 级, 第Ó 组公差的精度等级是 8 级, 齿轮齿厚精度等级标注为:

9—8 —8*GH*　　*GB* 10095 —88

根据该种标注方法, 求齿厚上下偏差值表为:

$$G = -6f_{pt} = -6\times 20 = -120(\mu m)$$

$$H = -8f_{pt} = -8\times 20 = -160(\mu m)$$

实际计算偏差值与查表选取的偏差值相差:

$$\triangle E_{SS} = -120-(-99) = -21(\mu m)$$

$$\triangle E_{Si} = -161-(-160) = -1(\mu m)$$

显然, 按查表计算的最能反映齿侧间隙的齿厚上偏差并不能保证所希望的最小极限侧隙。由于齿轮回差与$(E_{SS}+E_{S1})$成正比, 这样单对齿轮的回差也随之增大, 没能将回差控制在齿轮精度等级所能达到的最小范围。因此, 对有高精度传动的齿轮, 必须按照实际计算的齿厚偏差进行标注, 才能通过控制齿厚偏差控制齿侧间隙, 进而达到控制回差的目的。按实际计算值进行标注如下:

$$9-8-8\ (^{-0.99}_{-0.16}) \qquad GB\ 10095-88 \qquad (13)$$

这种标注符合参考文献[1] 4. 3 中的关于齿厚极限偏差超出表 2 所列范围或偏离较大时, 不受 14 种分级代号限制而按实际计算值进行计算的补充说明。

b) 通过控制公法线长度偏差来控制齿厚偏差。对于有较高精度要求的中、小齿轮, 常用的齿厚测量方法是用公法线长度测量来保证的, 因此, 通过控制公法线长度偏差控制齿厚偏差来保证侧隙以达到控制回差也是可行的。由式(10)、(11)、(12)可知, 公法线长度偏差的计算把齿圈径向跳动公差考虑在内, 这样, 使齿厚偏差的精确性更高, 所以更合理。

6　减小回差措施

a) 接触游丝发。在主、从动齿轮增设辅助齿轮, 使辅助齿轮始终给主动齿轮单方向力矩, 使主、从动齿轮单方向接触, 可消除由侧隙产生的回差;

b) 用弹簧消除侧隙造成的回差。将所有几何参数相同的两个齿轮合并成一个齿轮, 两个齿轮用弹簧连接, 一个与轴固定, 另一个与轴滑配, 一起转动时靠弹簧力消除回差;

c) 装配法。把啮合间隙最小的齿轮配对装在一起, 以减小回差。

此外, 还有调整中心法、采用可调齿厚齿轮等方法可以消除回差。

7　结论

通过上述分析、讨论可知, 产生回差的主要原因是保证齿轮正常传动和润滑的齿侧间隙造成的。在伺服驱动和某些特殊装置的齿轮传动系统中, 对回差的要求是十分严格的, 必须加以控制。实践证明, 通过控制齿厚偏差来控制齿侧间隙, 以达到控制回差的目的是可行的, 且效果良好。

参考文献

1　王文义. 仪表齿轮[M]. 北京: 机械工业出版社, 1982

2　齿轮手册编委会. 齿轮手册[M]. 北京: 机械工业出版社, 1993

3　田玉顺. 公差与配合技术手册[M]. 北京: 北京出版社, 1982

4　王广涛. 公差与配合技术测量[M]. 北京: 中国铁道出版社, 1980

5　天津大学. 精密机械设计基础[M]. 北京: 中国铁道出版社, 1989

6　哈尔滨工业大学. 机械设计基础[M]. 北京: 机械工业出版社, 1981

(上接第 35 页)

军事电子信息学术会议论文集, 2002

6　R. G. van Schyndel, A. Z. Tirkel, C. F. Osborne. A digital watermark[J]. In Int. Conf. on Image Processing. IEEE. 1994, 2: 86-90

7　B. Pfitzmann. Information hiding terminology [M]. In: Randerson(Ed). Information Hiding. Berlin: Springer, 1996