基于数字图像的信息隐藏技术综述

陈 雅
(淮阴师范学院计算机系 江苏 淮安 223000)

【摘 要】：本文简要介绍了基于数字图像的信息隐藏技术的基本概念和原理，给出了图像信息隐藏系统的通用模型和关键技术同时，对于图像信息隐藏技术的主要应用领域进行了分析。

【关键词】：数字图像 信息隐藏

一、引言：

20 世纪 90 年代以来，信息技术的飞速发展已经从根本上改变了人们相互沟通的模式。存放在服务器上的文档、图片、音乐等各种资料可以从世界的每一个角落方便地下载，这些特性很容易被盗版者所利用，给作品带来了很大的不安全性。为了解决信息安全和版权问题，人们首先会想到的是信息加密(Encryption)。信息加密的目的在于将可读的内容转变为无法识别的内容，使得截获这些信息的人无法阅读，同时信息的接收者能够验证接收到的信息是否被其他人篡改或替换过。而加密方法有一个致命的缺点，那就是它明确地提示攻击者哪些是重要信息，容易引起攻击者的好奇和注意，并有被破解的可能性，而且一旦加密文件经过破解后其内容就完全透明了；攻击者还可以在破译失败的情况下将信息破坏，即使是合法的接收者也无法阅读信息内容。针对密码技术的上述弱点，近年来，国际上开始提出了一种新的信息安全的概念，并开发出了一种不同于传统密码学的技术—信息隐藏技术。

二、图像信息隐藏系统概念与原理：

1、图像信息隐藏系统概念、模型

图像信息隐藏系统是指以数字图像为载体，将需要保密的信息以噪声的形式隐藏于公开的图像中，但是噪声必须不为人眼所觉察，从而逃避可能的检测者，以达到传递秘密信息的目的的系统。

通常，一个图像信息隐藏系统的一般化模型如图 1 所示：

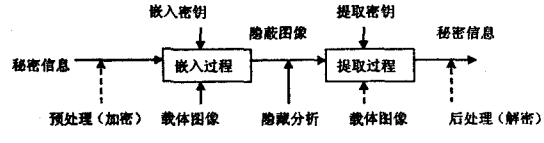

图 1

2、图像信息隐藏技术的性能指标

根据信息隐藏的原理和目的，信息隐藏系统一般应满足下列要：

1)隐蔽性：包括不可感知性(Imperceptibility)和不可检测性(Undetectability)。

2)隐藏信息量(Capacity)：指在不影响图像质量的前提条件下，所能嵌入的最大信息量。

3)鲁棒性(Robustness)：也称免疫性(Immunity)，指不因隐蔽载体图像的某种改动而导致隐藏信息丢失的能力。

三、基于数字图像的信息隐藏算法：

在数字图像中嵌入秘密信息的算法主要有空间域(Spatial Domain)和变换域(Transformation Domain)两类。

1、空间域(Spatial Domain)算法

空间域隐藏技术是指将秘密信息嵌入数字图像的空间域中，即对像素灰度值进行修改以隐藏秘密信息。下面介绍几种典型的空间域隐藏技术算法：

(1)LSB 算法

该算法通过调整载体图像的最低若干有效位来隐藏信息，致使所隐藏信息在视觉上很难被发觉，而且只有知道秘密信息嵌入的位置才能正确提取出秘密信息。LSB 有较大的隐藏信息量，而且可以满足隐蔽性的要求，但由于使用了图像不重要的像素位，算法的鲁棒性差，秘密信息很容易被滤波、图像量化、压缩、几何变形等操作所破坏。

(2)Patchwork 算法

Bander 等人提出的 Patchwork 算法是一种基于统计特性的信息隐藏算法。该算法在载体图像中利用伪随机数选择 N 对像素点(ai,bi)，然后针对每个像素点的亮度值，做如下操作：

$$\begin{cases} a_i=a_i+1 \\ b_i=b_i-1 \end{cases} \quad i=1,2,\ldots N$$

使得整幅图像的平均亮度保持不变。也就是说，该算法假设任意像素之差是零均值随机变量，任选 N 对像素，增加对比度而不改变平均亮度，使该均值偏移而隐藏信息。该算法克服了 LSB 算法改变图像统计特性的不足，并对 JPEG 压缩、FIR 滤波以及图像裁剪有一定的抵抗力，但嵌入的信息量有限，且对串谋攻击的抵抗力较弱。

(3)纹理映射编码方法

该方法通过把图像的一种纹理块复制到该图像中具有相似纹理特性的区域来完成信息的嵌入，恢复时必须计算自相关特性。该算法对于滤波、压缩和扭转等操作具有抵御能力，但仅适于具有大量任意纹理区域的图像，而且尚不能完全自动完成，需人工干预。

2、变换域(Transformation Domain)算法

变换域算法主要是通过修改载体图像某些指定的频域系数来嵌入数据。考虑到对低频区域系数的改动可能会影响到载体图像的感知效果，而高频系数又容易被破坏，因此，一般选取信号中频区域上的系数来隐藏信息。

比较常见的变换技术有离散余弦变换(DCT)及离散小波变换(DWT)。下面介绍这两种典型的变换域隐藏技术算法：

(1)DCT 算法

DCT 是图像处理中常用的一种频域变换方法。基于 DCT 域的图像信息隐藏算法的一般步骤为，首先对载体图像分块进行二维 DCT 变换，然后用秘密信息对 DCT 系数进行调制，最后对新的系数作离散余弦反变换(IDCT)，即可得到伪装图像，完成信息隐藏过程。

(2)DWT 算法

DWT 是一种多尺度空间频率分解。基于 DWT 域的图像信息隐藏算法的一般步骤为，首先对载体图像进行多级离散小波变换，得到不同分辨率下的细节子图和逼近子图，然后用秘密信息对 DWT 系数进行调制，最后对嵌入秘密信息后的小波系数进行相应级别的离散小波逆变换，完成信息隐藏过程。

变换域算法的主要优点有：(1) 在变换域中嵌入的信号能量可以分布到空间域的所有像素上；(2) 在变换域 (下转第 18 页)

淮阴师范学院青年教师科研基金项目 项目号：06HSQN070

搜索树的资源开销大,有可能拖垮服务器。树的数据结构复杂,算法把树上每个叶子必须亲历一次,在遍历操作中无法加速优化,如果枝叶少则求解快,枝叶多时则求解慢,因此在某些起点三次乘车求解仅需十几秒,而在某些起点三次乘车求最优解则需要数分钟,乘客有时无耐心等待查询结果的返回。三次乘车树形结构复杂,构建耗时,若不依靠索引优化加速则无实用价值。

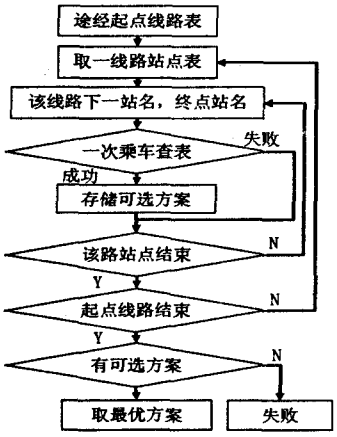

图 3 最优二次乘车算法

查表法:算法简单,在并发任务越多时,越能表现出消耗资源少的优势,特别适于应用于互联网络、移动网络这样多用户的环境下。数据结构简单为线性表,以检索号有序,应用顺序表中的二分查找法提高搜索速度。福州共有 810 个站点,两两互通的" 一次乘车互通最优表" 共 51650 行,用二分查找法平均 0.006743 秒可找到指定行。而树形搜索算法在应用数据库索引技术对构建树提速后平均为 0.092690 秒才得到最优解。查表法需要在每一次线路发生更改都要重新构建互通表。重新计算任意两车站不换乘互通最优解,采用树形搜索算法加以索引优化,耗时约一小时,因此重建工作宜放在变更线路后的夜间闲时由服务器自动完成。

4.4 结论

本论文提出的查表法一改以往换乘算法只重研究不重实用的特点,算法简单,性能优异,消耗资源少,支持同时查询的并发数大。在互联网络及移动通讯网络中将有良好的表现,应用前景良好。

5. 结束语

本课题是"城市交通集成系统的多智能体博弈模型研究"一个子课题,该算法挂入我院正在研制的交通信息短信平台,支持多并发查询能力很好,工作稳定。正在接受广泛测试,并收集公交乘客路线需求,为下一阶段公交智能调度的研究做数据准备。

参考文献:

1. 杨佩昆.智能交通运输系统体系结构[M].上海:同济大学出版社,2002.34~36.
2. 黄卫,陈里得.智能运输系统(ITS)概论[M].北京:人民交通出版社,2001.130~131.
3. 王炜,杨新苗,陈学武.城市公共交通系统规划方法与管理技术[M].北京:科学出版社,2002.263~269.
4. 尹倩贤,王健军.上海市公共交通出行问询系统的开发及应用[J].城市公共交通,2001,(2):33~36.
5. 王炜,过秀成.交通工程学[M].南京:东南大学出版社,2000.13~14.
6. 钱颂迪.运筹学[M].北京:清华大学出版社,2000.265~267.
7. 王炜.道路交通工程系统分析方法[M].北京:人民交通出版社,2004.114-115.
8. 李文勇,王炜,陈学武.公交出行路径蚂蚁算法[J].交通运输工程学报,2004,4:103-105.
9. 周新年,林炎.我国旅游交通现状与发展对策[J].综合运输,2004,11:49~52.

(上接第 6 页)

中,人的感知系统的某些掩盖特性可以更方便的结合到编码过程中,可以提高算法的鲁棒性;(3)变换域方法与大多数国际标准兼容,可直接实现压缩域内的算法,提高效率。

四、图像信息隐藏的应用:

随着多媒体技术的飞速发展和互联网的迅速普及,信息隐藏在政府、军事情报部门、银行系统、商业系统等诸多领域发挥着重要作用,广泛应用于通信保密、数字作品的版权保护、商务活动中的票据防伪、验证资料的完整性与添加标题等方面。

1、通信保密

我们可以运用信息隐藏技术对那些涉及国家安全的军用卫星图片、军用设施图纸、电子商务的敏感信息、重要文件的数字签名以及个人隐私等秘密信息进行保密,确保这些信息在互联网上被安全、快捷地传递与使用。

2、数字作品的版权保护

为了保护数字服务提供商的正当利益,抵制未经授权的拷贝和发行,信息隐藏技术中的"数字水印"、"数字指纹"等将著作权、公司标志、有特殊意义的文本、购买者序列号等重要信息嵌入数字图像多媒体数据中,以防止非法拷贝或者用来跟踪、追查盗版者及盗版产品的出处。

3、商务活动中的票据防伪

票据防伪是在彩色打印机、复印机输出的每幅图像中嵌入唯一的、不可见的数字水印。当需要时,可以通过实时地扫描票据来判断水印的有无,辨别票据的真伪。此外,各种电子票据也需要一些非密码的认证方式,数字水印技术为各种电子票据提供不可见的认证标志,增加电子票据的伪造难度。

4、验证资料的完整性

信息隐藏技术通过在数字媒体中嵌入脆弱水印的方法来保护媒体,一旦资料被篡改,水印就被破坏,这样可以很容易验证和识别资料的完整性。

5、添加标题

标识信息往往比文件内容更具有保密价值,有时没有标识信息的文件甚至是无法使用的。但直接将这些重要信息标一记在原始文件上又很危险。对此,信息隐藏技术将标识信息隐藏在原始文件中,使其不能被直接读取,而只有通过特定的阅读程序才能被读取。

五、结论

本文提出了图像信息隐藏技术的基本概念和原理,给出了图像信息隐藏系统的通用模型。分析了基于数字图像的信息隐藏算法。并对信息隐藏技术的主要应用领域进行了概括。

参考文献:

1. 刘振华,尹萍.信息隐藏技术及其应用.北京:科学出版社,2002.
2. Fabien A.P.Petitcolas, Ross J.Anderson, Markns G. Knhn.Information Hiding---A Survey. Processings of the IEEE,1999,87(7)
3. Bender W, Gruhi D, Morimoto N, et al. Techniques for data hiding. IBM System Journal. 1996.
4. 刘瑞祯,谭铁牛 数字图像水印研究综述 通信学报.2000 21(8).
5. 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 2
6. 王君 基于数字图像的信息隐藏技术 2005 1
7. 张永红 基于数字图像的信息隐藏技术研究及应用 2006 4
8. 张坤 数字图像信息隐藏理论与算法研究 2006 3