维普资讯 http://www.cqvip.com

一种基于小波变换的图像鲁棒性盲水印算法

俞伟新[1],杨善超[2],龚声蓉[2]
(1.苏州农业职业技术学院 电子信息系,江苏 苏州 215008;
2.苏州大学 计算机科学与技术学院,江苏 苏州 215006)

摘 要:对数字水印技术的概念、特点、分类、模型等作了简单的介绍,给出一种基于小波变换的图像鲁棒性盲水印算法。实验表明,该算法能够很好地抵抗局部剪切的攻击。文中还结合实验结果对增强剪切攻击鲁棒性的技术进行了分析。

关键词:数字水印;鲁棒性;盲水印
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2006)07-0140-04

A Robust Blind Image Watermarking Algorithm Based on Wavelet Transformation

YU Wei-xin[1], YANG Shan-chao[2], GONG Sheng-rong[2]
(1. Electronic Information Department, Suzhou Polytechnical Institute of Agriculture, Suzhou 215008, China;
2. Computer Science and Technology School, Soochow University, Suzhou 215006, China)

Abstract: In this paper, a brief introduction of watermarking including notion, characteristics, classification, and model is given and then a robust blind image watermarking algorithm in wavelet domain is proposed. Experimental results show that, this algorithm is able to resist local cropping attack. A further analysis on enhancing the ability to resist cropping attack is made again according to experimental results.

Key words: digital watermarking; robustness; blind watermarking

0 引 言

随着以微电子技术为代表的信息产业的飞速发展,多媒体、计算机网络等进入寻常百姓家,数字化已深入人心,以Internet为先锋的网络化浪潮更是席卷全球。国际互联网是一个优秀的数字媒体发行系统,数字作品的传播和复制变得越来越容易,用户可以方便地下载或拷贝数字作品(图片、音乐、视频),因此版权作品被盗版的风险也随之剧增。数字作品所有者最早使用的方法是密码学,密码学只能保护传输中的内容,而内容一旦被解密就不再有保护作用了(盗版者可以购买产品,使用密钥获取无保护的内容副本,然后继续发行非法副本)。因此,迫切需要一种替代技术或者对密码学进行补充的技术,它应该甚至在内容被解密后也能够继续保护内容。数字水印则有能力满足这些要求,因为它把信息嵌入到数字作品里,而在一般使用中它不会被删除。即使经过解密、再加密、压缩、数-模变换和改变文件格式这些过程,设计巧妙的水印仍能继续保留在内容中,起到防止拷贝和版权保护的作用。

收稿日期:2005-10-31
基金项目:铁道部"铁路信息科学与工程"开放实验室基金资助项目(TDXX0501);江苏省自然科学基金资助项目(BK2003029);苏州大学211重点建设项目
作者简介:俞伟新(1967-),男,江苏吴县人,讲师,硕士,研究方向为图像中的数字水印技术。

1 数字水印概述

数字水印(digital watermark)技术,是通过一定的算法将一些标志性的信息直接嵌入到数字作品中,但不影响原作品的价值和使用,被嵌入的标志性的信息通常是不可见或不可察觉的,只能通过一些专用的检测器或阅读器才可以被检测或者被提取。这些标志性信息就是水印,水印可以是作者的序列号、公司标志、有特殊意义的图像或文本。数字水印与源数据(如图像、音频、视频数据)紧密结合并隐藏其中,成为源数据不可分离的一部分,并可以经历一些不破坏源数据使用价值或商用价值的操作而存活下来。数字水印可以判别作品是否受到保护,监视被保护数据的传播、真伪鉴别和非法拷贝、解决版权纠纷并为法庭提供证据[1]。

1.1 数字水印的特点

数字水印具有如下特点:

(1) 鲁棒性。

鲁棒性也称为健壮性、免疫性,是指嵌入水印后的数字作品在经过常规的信号处理操作后,仍能够检测到水印的能力。对图像的常规操作主要包括空间滤波、有损压缩、打印和扫描、几何失真(旋转、平移和图像缩放等)。

(2) 安全性。

维普资讯 http://www.cqvip.com

数字水印的安全性就是指它对抗蓄意窜改或恶意攻击的能力,也就是说加入水印和检测水印的方法对没有授权的第三方是保密的而且不可轻易被破解,即使黑客也不能读出(数字水印也需要加密)。水印系统对安全性的要求在很多应用中有很大不同。

(3) 隐蔽性。

隐蔽性也称为不可见性、透明性等,是指水印嵌入到多媒体作品中后,水印信息和作品集成在一起,既看不到水印,也不会引起原作品被感知质量的下降。

(4) 确定性。

数字水印应能为受到版权保护的多媒体作品的归属提供完全可靠的证据,也就是说,数字作品所携带的版权信息能够被惟一确定地鉴别,以判定数字作品的真正所有者。

1.2 数字水印的分类

(1)根据数字水印的稳健性将其分类:鲁棒水印和易损水印。通常鲁棒水印主要用于版权保护,而易损水印则用于数据作品的完整性保护。

(2)根据数字水印的嵌入技术的不同可以将其分为时空域数字水印和变换域数字水印。

较早的数字水印算法从本质上来说都是时空域上的,通过改变某些像素的灰度将要隐蔽的信息嵌入其中,将数字水印直接加载在数据上。时空域方法可以细分为最低有效位法、Patchwork 方法及纹理映射编码方法、文档结构微调方法[2,3]。

基于变换域的技术可以嵌入大量比特的数据而不会导致不可察觉的缺陷,往往通过改变频域的一些系数的值,采用类似扩频图像的技术来隐藏数字水印信息。这类技术一般基于常用的图像变换,基于局部或全部的变换,这些变换包括离散余弦变换(DCT)、小波变换(DWT)、傅氏变换(FT 或 FFT)以及哈达马变换(Hadamard Transform)等等。其中基于分块的 DCT 和分型的 DWT 是最常用的变换之一。频域方法具有如下优点:a.在频域中嵌入的水印的信号能量可以分布到所有的像素上,有利于保证水印的不可见性;b.在频域中可以利用人类视觉系统的某些特性,更方便、更有效地进行水印的编码。不过,频域变换和反变换过程中是有损的,同时其运算量也很大,对一些精确或快速应用的场合不太适合[3,4]。

数字水印的系统模型如图 1 所示。

2 基于小波变换的图像鲁棒性盲水印算法

文中给出一种能够抵抗剪切攻击的小波域鲁棒性数字水印算法。这种水印算法是将水印图像排列并置乱后,嵌入到小波变换第二级的高频子带当中。水印提取采用相反的提取方法。水印的提取不需要原图像,也不需要水印图像,属于一种盲水印。实验证明这是一种非常有效的抵抗剪切攻击的水印算法。

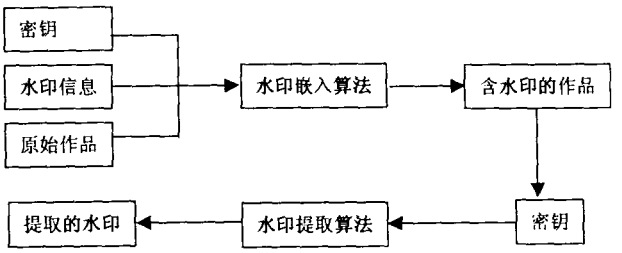


图 1　水印的嵌入与提取过程

根据人类视觉系统(HVS)的特性,嵌入到图像的高频子带中能够设计出不可见性良好的水印算法。利用小波变换能够很好地对图像进行多分辨率分解,选择较好的高频子带,而且整体小波变换消除了 DCT 变换所带来的块效应。因此,选择在小波域上来实现数字水印算法。图 2 给出了小波做两级小波分解的结构图(如图 2(a))和小波变换后的图像(如图 2(c)),在小波变换后的图像中,高频显示的是系数的绝对值。

(a) 小波分解结构图　　(b) 原图像　　(c) 小波分解后的图像

图 2　图像的小波分解

2.1 算法的原理

水印图像为二值图像,尺寸为 $N \times N$,水印图像的尺寸相对于载体图像要小得多。水印图像所能嵌入的区域也就比水印的尺寸大得多。如果嵌入的区域尺寸为水印图像尺寸的 n 倍,嵌入的水印其实是相当于一幅分辨率为 $N \times N$、灰度级为 n 的一幅图像。设这幅图像为 I。水印提取相当于提取出遭到破坏的 I 图像的过程。水印图像分 n 次嵌入到载体图像的不同区域,当一个区域被破坏后,其他区域的水印仍然能够很好地存在。水印被破坏了的区域,在提取时相当于对 I 图像某个或多个位平面引入了噪声,而未被破坏的位置灰度值仍然是很高的。局部的破坏只能影响该图像的一个或几个位平面。水印信息代表了图像 I 中比较有规律的位平面。I 图像中的这些位平面的重要性是相同的。如果被破坏的位平面是少量随机噪声点的话,水印信息应该能够被容易地辨认出来。这就是本水印算法的基本思想。

2.2 数字水印嵌入与提取过程

假设载体图像为灰度图像,尺寸为 $M \times M$,水印图像为二值图像,尺寸为 $N \times N$,对应的系数矩阵为 Matrix_W,

维普资讯 http://www.cqvip.com

本实验中 $N=64$,要嵌入的高频子带 HL2,LH2,HH2,尺寸分别为 $\frac{M}{4}\times\frac{M}{4}$。以下为水印实现过程。

2.2.1 水印嵌入算法

(1)载体图像做两级小波变换,变换之后的系数矩阵为 Matrix。

(2)水印信息的生成。

①将水印图像按照顺序排列成 $\frac{M}{4}\times\frac{M}{4}$ 大小,分别存放于 $\text{Matrix}_l^l(l=1,2,3)$ 当中,它们分别对应子带 HL2,LH2,HH2。

排列的方法是:

$$\text{Matrix}_l^l[i][j]=\text{Matrix}_W[i\%N][j\%N]$$

②分别利用3个密钥对矩阵 $\text{Matrix}_l^l(l=1,2,3)$ 进行置乱。

文中采用 Arnold 变换对 3 个矩阵进行置乱。对于正方形数字图像,离散化的 Arnold 变换定义为:

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\bmod N,\ x,y\in\{0,1,\cdots,N-1\}$$

其中,N 为图像的宽度和高度。Arnold 变换的迭代次数不一样,置乱效果不一样,当迭代的次数为迭代周期的一半时,置乱效果最佳[5]。

文中的算法使用迭代次数做为置乱的密钥,对 3 个矩阵采用不同的密钥进行置乱,这样就能够保证每个位置的水印信息能够更加随机地映射到不同的位置,从而增强了剪切攻击的鲁棒性。

(3) 混沌序列的生成。

生成一个长度为 $\frac{M}{4}\times\frac{M}{4}$ 的 0,1 混沌序列,并排列成矩阵 Matrix_C,尺寸为 $\frac{M}{4}\times\frac{M}{4}$。混沌序列的初始值作为密钥。混沌序列的生成是为了保证水印信息嵌入后的安全性[6~8]。

(4) 水印信息的嵌入。

嵌入的方法是:

$$\text{Matrix}_l^l[i][j]=\text{Matrix}_l^l[i][j]\oplus\text{Matrix}_C[i][j]$$

(5)载体图像做两级小波逆变换,生成嵌入水印之后的图像。

2.2.2 水印提取算法

(1)嵌入水印后的图像(可能已经遭受攻击)做两级小波变换。

(2)混沌序列的生成。

按照与嵌入时相同的方法和密钥生成相同的混沌序列,并排列成矩阵 Matrix_C。

(3) 水印信息的提取。

①结合混沌序列矩阵,将小波变换后的子带 HL2,LH2,HH2 的嵌入信息提取出来,分别存放于 3 个相同尺寸的矩阵 $\text{Matrix}_l^l(l=1,2,3)$ 当中。提取的方法是:

$$\text{Matrix}_l^l[i][j]=\text{Matrix}_l^l[i][j]\oplus\text{Matrix}_C[i][j]$$

②对提取出的信息矩阵 $\text{Matrix}_l^l(l=1,2,3)$ 分别进行逆置乱,还原出水印图像排列成的矩阵[9]。

(4) 水印图像的生成。

嵌入的水印信息相当于一幅分辨率 $N\times N$、灰度级为 $\left(\frac{M}{4N}\right)^2$ 的纯白色图像。令 $\max=\left(\frac{M}{4N}\right)^2$,设置分辨率为 $N\times N$ 灰度级 max 矩阵 I,用于保存提取出的数据。I 的每个元素初值为 0。

① 灰度矩阵的生成。

提取的方法是:

$$I[i][j]=I[i][j]+\text{Matrix}_l^l[i\%N][j\%N]$$

因为图像有可能已经遭受攻击,所以,每一个位平面中提取出的信息可能有很多是错误的,只有一部分 $I[i][j]$ 的值为 max。

② 灰度矩阵的归一化。

当所有嵌入位置都提取完成后,对每个(i,j) 位置上的值 $I[i][j]$ 采用:$I[i][j]=I[i][j]/\max$ 进行规一化。规一化之后的 $I[i][j]$ 代表的是(i,j) 位置被提取出 $W=1$ 的成功率。

③ 设定阈值,生成水印图像。

设置一个阈值 T,$T\in(0,1)$,当 $I[i][j]<T$ 时 $I[i][j]=0$,否则 $I[i][j]=255$;利用矩阵 I 生成提取出的水印图像。

2.3 实验结果及分析

载体图像尺寸为 512×512 的 lena 图像(如图 3 (a)),水印图像为一幅二值图像(如图 3 (b)),尺寸为 64×64。混沌序列密钥 $X_0=0.3$,$\lambda=2$。采用 Arnold 置乱技术,HL2,LH2,HH2 子带水印置乱迭代次数分别为 17,39,31。逆置乱的迭代次数分别为 96 - 17,96 - 39,96 - 31 (HL2,LH2,HH2 子带的尺度为 128×128,Arnold 置乱迭代的周期为 96)。图 4 中给出了未遭受攻击的嵌入水印后的图像(如图 4 (a))和提取出的水印图像(如图 4 (b))。

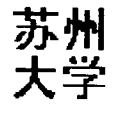
攻击二:对嵌入后的图像进行大面积的剪切,得到图 5(a)。提取水印时,$T\in(0.01,0.5)$ 时提取效果较好,在 $T=0.13$ 能够取得最好的提取效果。图 5(*b*)、(*c*)、(*d*) 分别为 $T=0.01$、$T=0.13$、$T=0.5$ 时提取出的水印。

(a) 载体图像 lena (b) 水印图像

图 3 实验测试图像

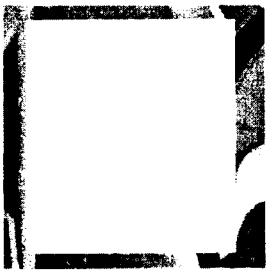
维普资讯 http://www.cqvip.com

(a) 未受攻击的嵌入水印后图像



(b) 提取出的水印

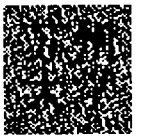
图 4　未受攻击的实验图像



(a)遭受大面积的剪切攻击的嵌入水印的图像

(b) T=0.01

(c) T=0.13



(d) T=0.5

图 5　遭受攻击后的提取图像

正确提取时,嵌入"1"提取出"1",或者嵌入"0"提取出"0"。错误提取时,嵌入"1"提取出"0",或者嵌入"0"提取出"1"。随着图像被破坏程度的加剧以及破坏范围的增大,正确提取的概率变小,而错误提取的概率变大。水印图像嵌入过程中排列了 max 次,在每一次排列中,由于遭受攻击,提取出的图像可能无法辨认,而在相应位置的其他的排列中,却很有可能是正确的。max 次排列的图像,对于水印图像上每个像素点,有 x 次正确提取,有 y 次错误提取,$x + y = \max$。可见水印信息排列的次数 max 对于检测的成功率非常重要。嵌入水印图像排列的次数越多,就越能够拉开错误提取次数与正确提取次数的差距,也就越能够抵抗对水印的攻击。在遭受攻击后,应该选择一个中间值进行分割,一定存在一个阈值,使得提取出的图像与原水印图像最接近。

3　结束语

实验表明,文中提出的基于小波变换的图像鲁棒性盲水印算法,能够很好地抵抗对图像局部剪切的攻击。当图像的一部分遭到攻击之后,其他未遭受攻击的部分的嵌入信息仍然能够正确地提取。只有当所嵌入区域的信息全部被破坏时,水印才无法提取,鲁棒性也就失去。实验表明在(0,1)之间存在一个值 X,使得当 $T = X$ 时,提取的水印图像具有最好的质量。

参考文献:

[1] Cox I J. 数字水印[M].北京:电子工业出版社,2003.

[2] 常　敏. 数字图像水印综述[J].计算机应用研究,2003(10):1-3.

[3] 侯振华,陈生潭.脆弱性数字水印研究[J].计算机应用,2003,23(12):106-108.

[4] 刘瑞祯,王蕴红,谭铁牛.基于图象内容的数字水印模型[J].中国图象图形学报,2001,6(6):556-562.

[5] 李　兵,徐家伟.Arnold 变换的周期及其应用[J].中山大学学报(自然科学版),2004,43(2):139-142.

[6] 刘振华,尹　萍.信息隐藏技术及其应用[M].北京:科学出版社,2002.

[7] 纪　震,李慧慧,肖薇薇,等.基于混沌序列的数字水印信号研究[J].电子学报,2004,32(7):1131-1134.

[8] 张家树,田　蕾.一种新的基于密钥的混沌数字水印方法[J].通信学报,2004,25(8):98-101.

[9] Wolfgang R B,Podlchuk C I,Delp E J. Perceptual Watermarks for Digital Images and Video[J]. Proceedings of the IEEE. 1999,87(7):1108-1126.

(上接第 139 页)

(3)根据接收的查询请求初始化 EJB 组件或对查询请求分发,对查询请求分发的处理就是调用相应 stubs 对象的 certi_wm 方法,传递的参数就是接收的查询请求。

(4)最后将 stubs 对象的非空返回结果给调用者,如果有多个不为空,合并结果集或构造错误消息给调用者。

4　结束语

利用 Web Services 技术将 Web 上现有的学历学位证书验证系统集成,设计并实现了证书验证系统,方便用户的查询。系统的实现对基于 Web Services 的技术应用研究有一定的借鉴意义。

参考文献:

[1] 郑小平..NET 精髓-Web Services 原理与开发[M].北京:人民邮电出版社,2002.

[2] 陈锦辉,王景皓.XML 与 JAVA 程序设计大全[M].北京:中国铁道出版社,2002.

[3] 郑晓东,王志坚.一种基于 Web Service 的分布式计算模型研究及其实现[J].计算机工程与应用,2004(1):144-147.

[4] Allamaraju S. J2EE 服务器端高级编程[M].闻道工作室译.北京:机械工业出版社,2001.

[5] Girdley M. J2EE 应用与 BEA WebLogic Server[M].邢国庆等译.北京:电子工业出版社,2002.