无定位图的预测误差差值扩展可逆数据隐藏 *

熊志勇, 蒋天发
(中南民族大学 计算机科学学院, 武汉 430074)

摘 要: 将 Tian 差值扩展技术应用于彩色图像中,提出一种利用预测误差差值进行扩展嵌入的彩色图像可逆数据隐藏算法。针对传统差值扩展技术存在过分修改像素灰度值、须嵌入定位图等缺点,首先利用色彩分量间的相关性减小差值,并将差值扩展量分散到两个色彩分量中;其次,对直方图平移技术进行改进,使得同等嵌入率下图像质量达到最佳;最后由两个色彩分量中像素的预测值之和决定可用于扩展嵌入的像素,无须保存溢出定位图,提取端在提取信息时可无损地恢复原始图像。实验结果表明,与其他算法相比,该算法在同等嵌入率下可取得更好的图像质量,算法复杂度更低。

关键词: 可逆数据隐藏; 预测误差差值扩展; 直方图平移; 溢出定位图
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)03-1015-04
doi:10.3969/j.issn.1001-3695.2010.03.057

Reversible data hiding using prediction error difference expansion without location map

XIONG Zhi-yong, JIANG Tian-fa
(*College of Computer Science, South Central University for Nationalities, Wuhan* 430074, *China*)

Abstract: This paper proposed a reversible data hiding algorithm for color images using prediction error difference expansion. To avoid the drawback of Tian's algorithm which must embed a location map and the quality decline of stego-images from excessive modulation to pixels, this algorithm using correlation of color components to decrease difference and disperse smaller expansion to two components, and improved histogram shifting technique to improve the quality of stego images, the embedding pixels was determined with sum of prediction values, so the algorithm did not need location map. Experimental results show the quality of stego-image is significantly improved, and the complexity is lower, when compared with other new or classical algorithms.

Key words: reversible data hiding; prediction error difference expansion; histogram shifting; overflow location map

0 引言

图像数据隐藏一般分为两类,即可逆隐藏和不可逆隐藏。如果接收方在提取信息的同时,还可以无损地恢复原始载体图像,这种技术称为可逆数据隐藏。近年来, Tian[1] 提出的差值扩展技术在可逆数据隐藏领域受到越来越多的关注。利用差值扩展进行可逆数据嵌入的算法通常能够提供较大的嵌入容量,而且差值扩展技术具有很好的可塑性,可用于整数 Haar 小波系数、图像的预测误差等不同的差值,改造成适合不同目的的嵌入算法。目前国内外已有不少 Tian 差值扩展技术的变形和延伸[2~6]。但这些方法存在一些共同的缺点,主要表现在三个方面:a)过分利用像素对的差值,载体图像质量严重下降;b)需要嵌入压缩的溢出定位图,增加了算法复杂度,同时降低了嵌入容量和图像质量;c)研究对象局限于灰度图像。

文献[2]提出将差值扩展与差值直方图平移相结合的技术,其主要优点是在同等嵌入率下大幅度提高图像质量,分五个版本详细讨论差值扩展和预测误差扩展方法。该算法可以根据负载大小选择合适的阈值 T,调整嵌入容量,从而使图像质量在当前负载下达到最佳,但算法需要存储外部像素的最低位,并对这些像素进行 LSB 替换,这种替换降低了载体图像的质量,却不会带来任何容量的增加。Coltuc 等人在文献[7]中提出一种基于可逆对比图的嵌入方法,在像素对的一个像素中嵌入分类信息,在另一像素中嵌入水印(或信息),他们的可逆嵌入方法无须嵌入溢出定位图等辅助信息即可在提取端成功地恢复原始图像,但变换后像素对的差值是原差值的三倍,比 Tian 差值扩展的差值还要大,载体图像质量下降更严重。文献[8]提出一种无定位图的无损嵌入方法。该方法先扫描整个图像,记录所有不可扩展像素对周围八个像素的最大值和最小值之差 d_i,并求出其最小值 $ND_{\min}$,由 $ND_{\min}$ 和阈值 T 控制嵌入容量,嵌入时,若 $d_i < ND_{\min}$ 而且 $d_i \leqslant T$,则用差值扩展嵌入数据,其他像素对保持不变。由于嵌入数据不改变周围像素值,提取时用同样的方法判断像素对中是否嵌入数据,他们的方案也无须嵌入溢出定位图。上述判断方法($d_i < ND_{\min}$)排出了许多可扩展像素对,尤其是在不可扩展像素对较多时,嵌入容量下降极为严重甚至不可嵌入,因此仅适于不可扩展像素对较少的图像,普适性较差。最近我国学者还将差值扩展方法应用到 SVG[9] 和矢量数字地图[10],通过扩展相邻顶点坐标的差值嵌入数据或水印,虽然这两种方法都无须嵌入定位图,但是算法

收稿日期: 2009-07-21; **修回日期**: 2009-08-28 **基金项目**: 国家民委重点科研基金资助项目(MZY02004)

作者简介:熊志勇(1965-),男(土家族),湖北恩施人,副教授,主要研究方向为软件信息安全、数字水印、多层分布式系统开发(zhiyx@scuec.edu.cn);蒋天发(1954-),男,湖北荆门人,教授,主要研究方向为网络安全、多媒体数字水印.

不适合彩色和灰度图像(位图)。

国内外学者仍不断提出新的差值扩展嵌入方法的变形或改进方案[11,12]。文献[11]利用预测误差扩展嵌入数据,通过改进嵌入公式和直方图平移技术(双阈值),使定位图变得更加稀疏,提高定位图的压缩率,从而增加嵌入容量,图像质量也有一定的改善。文献[12]改变 Tian 算法的像素分组方法,像素对互相重叠,也就是 N 个像素被分成 $N-1$ 对,这样新的像素对始终有一个像素未修改,与传统的重复嵌入相比,嵌入容量和图像质量都有很大的提高。但这两种方案均需要嵌入定位图和可改变差值的 LSB 位流。目前所提出的基于差值扩展的可逆嵌入算法大多数都是针对灰度图像。虽然,祝玉新等人[13]对彩色图像的蓝色分量进行 Haar 小波变换,嵌入可逆水印,但此方法与 Tian 差值扩展算法没有本质的区别。为此,本文将 Tian 的差值扩展技术应用于彩色图像中,提出了一种基于双分量预测误差差值扩展的彩色图像可逆嵌入方法。

1 双分量预测误差差值扩展

1.1 传统差值扩展

文献[1]中引出的差值扩展算法,可实现在一对像素中嵌入 1 bit 信息。设 x、y 是相邻两个像素的灰度值,$x,y\in[0,255]$,$x\geqslant y$,则这两个像素值的均值 l 和差值 h 可用下式计算

$$l=(x+y)/2,h=x-y \tag{1}$$

文中,整数除法均采用下取整。式(1)的逆变换为

$$x=l+(h+1)/2,y=l-h/2 \tag{2}$$

这个可逆的整数变换即整数 Haar 小波变换。把需要嵌入的 1 bit 信息 w 按式(3)嵌入。式(3)就是差值扩展的嵌入公式。

$$h'=2\times h+w \tag{3}$$

1.2 单分量预测误差扩展

自然图像中像素值之间存在着很强的相关性,这是图像压缩和线性预测编码的基础。相邻像素的相似度随着像素距离的增加而逐渐减小,邻近像素在统计意义上应有最大的相关性,当前像素通过其邻近像素来预测的准确度也应最高[14]。对任一指定的像素,可以用最邻近像素的平均值来预测当前像素的值,当前像素值 a 与预测值 $\hat{a}$ 之差即为预测误差,$p=a-\hat{a}$。嵌入 1 bit 信息 w,其预测误差变为

$$p'=2\times p+w \tag{4}$$

嵌入信息的像素值

$$a'=\hat{a}+p' \tag{5}$$

RGB 真彩图像的三个色彩分量都是独立而清晰的灰度图像,因此相邻像素的相关性也适于彩色图像的各色彩分量,用以上嵌入方法可以在色彩分量中嵌入数据,称这种嵌入方法为单分量预测误差扩展。Tian 差值扩展实际上也是利用预测误差嵌入数据,由于仅用相邻的一个像素进行预测,没有考虑周围像素的变化趋势,预测准确性不高,预测误差偏大。为了提高预测准确性,利用最小距离下像素值的强相关性,选择最邻近的四个像素(上下左右)作为预测像素,计算四个预测像素的平均值,并将其作为当前像素的预测值。

1.3 双分量预测误差差值扩展

自然图像的三个色彩分量之间存在密切的相关性[15],在一个特定的区域内,两个色彩分量中对应像素的预测准确度应保持一致,即预测误差非常接近,预测误差的差值很小。图 1(a)(b)是 200×200 Lena 彩色图像蓝色(B)和绿色(G)分量的预测误差直方图(峰值分别为 3 088 和 3 073),图 1(c)是 BG 分量的预测误差差值直方图(峰值 6 710)。图 1 所示的结果表明,预测误差集中在 0 附近,而且两个色彩分量间预测误差的差值比单分量预测误差更小。

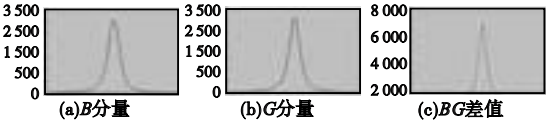


图1 LenaBG分量预测误差及差值直方图

将传统差值扩展方法进行推广以适应负整数,对任意两个色彩分量,由下式计算预测误差 p_1、p_2 的均值和差值

$$l=(p_1+p_2)/2,h=p_1-p_2 \tag{6}$$

对应的逆变换为

$$\begin{cases}p_1=l+(h+1)/2,p_2=l-h/2 & |l\geqslant 0,h\geqslant 0\\ p_1=l+h/2,p_2=l-(h-1)/2 & |l\geqslant 0,h<0\\ p_1=l+h/2,p_2=l-(h+1)/2 & |l<0,h\geqslant 0\\ p_1=l+(h-1)/2,p_2=l-h/2 & |l<0,h<0\end{cases} \tag{7}$$

把需要嵌入的 1 bit 信息 w 按如下方式嵌入:

$$h'=2\times h+w \tag{8}$$

当 $|p_1|<|p_2|$,$|p_1+p_2|=1$,$w=0$ 时,$|h|$ 为奇数,$|h'|$ 为偶数,经式(7)变换后,所得 p_1',p_2' 符号相反,且 $|p_1'|=|p_2'|$,在恢复时将出现错误。例如,$p_1=2$,$p_2=-3$,由式(6)可得,$l=0$,$h=5$,由式(8)得,$h'=2\times 5+0=10$,再由式(7)可得,$p_1'=0+(10+1)/2=5$,$p_2'=0-10/2=-5$,恢复时,$p_1=0+(5+1)/2=3$,$p_2=0-5/2=-2$,与原始值不符。

造成以上错误的原因是采用下取整求平均值,丢失了平均值的符号。为了解决此问题,本文改用求和

$$s=p_1+p_2,h=p_1-p_2 \tag{9}$$

相应的逆变换为

$$\begin{cases}p_1'=p_l\pm(h+1)/2,p_2'=p_2\mp h/2 & |s\geqslant 0,h\geqslant 0\\ p_1'=p_l\pm h/2,p_2'=p_2\mp(h-1)/2 & |s\geqslant 0,h<0\\ p_1'=p_l\pm h/2,p_2'=p_2\mp(h+1)/2 & |s<0,h\geqslant 0\\ p_1'=p_l\pm(h-1)/2,p_2'=p_2\mp h/2 & |s<0,h<0\end{cases} \tag{10}$$

其中:±表示嵌入时 +,恢复时 −。把需要嵌入的 1 bit 数据 w 按如下方式嵌入

$$h'=h+w \tag{11}$$

提取和恢复时

$$w=lsb(h'),h=(h'-w)/2+w \tag{12}$$

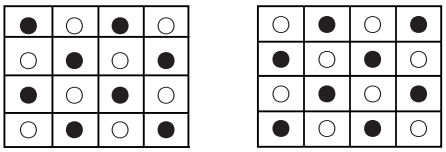
其中:$lsb(.)$ 为取最低位函数。嵌入数据时,用式(11)计算 h',将 h' 代入式(10)可得 p_1'、p_2',$p_1'-p_2'$ 仍为 $2\times h+w$,再由式(5)计算新的像素值 a_1'、a_2',实现在两个色彩分量中嵌入 1 bit 数据;图像恢复时,用式(12)计算 h,仍用式(10)和(5)计算像素值。由于嵌入过程是对两个色彩分量的预测误差的差值进行扩展,将其称为双分量预测误差差值扩展。

2 基于预测误差差值扩展的可逆数据隐藏

2.1 像素分组

在提取信息和恢复图像时,必须保证像素的预测值与嵌入时一致,即嵌入数据不能改变像素的预测值,为此本文将像素分成两组,如图 2 所示。其中●表示待预测的像素(待嵌入信息),用最邻近的四个预测像素(用○表示)进行预测,图像边界上的像素,用相反方向的预测像素代替所缺的像素,如图像左边界像素,由于缺少左预测像素,用上下右右像素进行预测,依此类推可处理其他边界像素。经过分组,所有待预测的像素都存在对应的预测像素,而且不受嵌入数据的影响。

用多重嵌入的方法可以提高嵌入容量。其中奇数次嵌入用图2(a)所示的分组方案,偶数次嵌入时,像素角色对调,如图2(b)所示。



(a)奇数次嵌入　　(b)偶数次嵌入

图2　像素分组图

2.2　差值直方图平移

为使图像质量在特定负载下达到最佳,本文采用文献[2]类似的直方图平移技术。以 *BG* 分量为例,将所有●像素的 *B*、*G* 分量预测误差的差值以直方图的形式表示,根据负载大小确定阈值 *T*,把直方图划分为内部区域和外部区域,如图3所示。

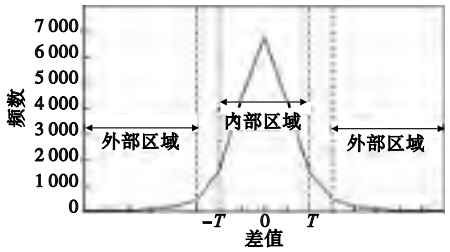


图3　差值直方图平移示意图

内部区域$[-T,T]$所对应的差将进行扩展嵌入,而外部区域$[-h_l,-T-1]$和$[T+1,h_r]$的差值沿横轴向外侧平移,以避免扩展后的内部区域和外部区域重叠。这里 h_l 和 h_r 分别为直方图左端和右端的非零端点,根据式(10)(11),内部区域扩展后变为$[-2T,2T+1]$,因此,外部区域要分别向左和向右移至$[-h_l-T,-2T-1]$和$[2T+2,h_r+T+1]$。避免内部区域和外部区域重叠的目的是保证在提取数据时可以无损地恢复原始图像。与文献[2]不同的是,本文只在内部区域嵌入信息,而对外部区域只进行平移而不替换最低位,相应地,在提取信息时,仅提取$[-2T,2T+1]$范围内差值的最低有效位。

2.3　差值分类及分布特点

2.3.1 *差值分类*

无论是内部区域扩展还是外部区域平移,均可能发生像素值溢出问题。色彩分量中灰度值限制在0~255,因此用式(5)嵌入数据后,色彩分量中的灰度值也必须在此范围内,即

$$p' \in [-\hat{x}, 255-\hat{x}] \tag{13}$$

在实际嵌入之前,先将所有差值进行分类。根据差值 h 的大小,将差值分为以下三类:

a)可扩展差值(Ⅰ类)。在内部区域,当 $h<0$ 时,$w=0$,$h\geqslant 0$时,$w=1$,用式(11)计算 h',再用式(10)计算相应的 p_1' 和 p_2',若 p_1'、p_2' 均满足式(13),则对应的差值即为可扩展差值。

b)可平移差值(Ⅱ类)。在外部区域,当 $h<0$ 时,$h'=-T$,$h>0$ 时,$h'=T+1$,用式(10)计算相应的 p_1' 和 p_2',若 p_1'、p_2' 均满足式(13),则对应的差值即为可平移差值。

c)其他差值(Ⅲ类),包括内部不可扩展和外部不可平移差值。

2.3.2 *差值分布特点*

由式(13)可知,像素预测值 $\hat{x}$ 越接近0越容易产生下溢,越接近255越容易产生上溢。也就是说,在自然图像中Ⅲ类差值的分布是不均匀的,而Ⅰ和Ⅱ类差值的分布则相对均匀。这种差值分布的差异性可用于Ⅲ类差值的定位,用长度为512的一维数组 *NSD* 作为Ⅲ类差值的分布表,数组元素的初值均为0,按图2对像素进行分组,对任一●像素,设 *sa* 为像素中两个色彩分量的预测值之和,$sa=\hat{x}_1+\hat{x}_2$,若预测误差差值 h 为Ⅲ类差值,则 $NSD_{sa}=1$。嵌入数据时,若 $NSD_{sa}=1$,像素值保持不变,对应的Ⅰ类差值不嵌入信息;若 $NSD_{sa}=0$,对Ⅰ类差值,用差值扩展嵌入信息,对Ⅱ类差值进行平移,这样嵌入和平移都不会出现溢出,也就不需要定位图。为验证该方案的可行性,从西安交通大学人工智能与机器人研究所东方人脸库(AI&R)的视点子库中随机选取1 000幅图像,图像大小为320×240。对 *GR* 分量组合进行统计(嵌入一次)。实验结果如表1所示,表中损失容量表示不能用于嵌入信息的Ⅰ类差值总数。实验表明:单次嵌入的平均负载能力大于0.4 bpp,与使用定位图的方法相比,损失容量大于压缩定位图的位流长度,导致平均负载能力下降约0.02 bpp,但实际嵌入的辅助信息(文件头和分布表)少很多,因此图像质量有所提高。另外,嵌入和图像恢复过程不需要压缩和解压定位图,算法复杂度降低。

表1　自然图像Ⅲ类差值统计分析结果($T=2$)

	Ⅲ类差值	占用预测和	损失容量	压缩定位图	分布表长度	负载能力
最大	1 251	82	10 788	8 023	506	0.466
最小	0	0	0	0	0	0.300
平均	178	32	2 840	1 550	350	0.406

2.4　信息嵌入过程

按 *BG*、*GR* 和 *RB* 顺序选择色彩分量组合,对每一分量组合,按如下过程嵌入待隐藏数据:

a)初始化。令 pass=0,按图2(a)的方案对像素进行分组。

b)生成Ⅲ类差值分布表。创建两个长度为512的一维数组 *EN* 和 *NSD*,所有元素的初值均为0。其中 *EN* 为Ⅰ类差值直方图,*NSD* 为差值分布表。按光栅扫描顺序扫描整幅图像,计算●像素的预测误差差值 h 以及预测和 *sa*,根据 *sa* 及差值类型生成Ⅰ类差值直方图 *EN* 和差值分布表 *NSD*。用 $NSD_{\max}$ 和 $NSD_{\min}$ 表示差值分布表的上、下非零端点,其初值分别为0和512,若 $NSD_{\max}\geqslant NSD_{\min}$,则分布表的有效长度 $L_T=NSD_{\max}-NSD_{\min}+1$;否则,表明不存在Ⅲ类差值,$L_T=0$。

c)构造辅助信息。辅助信息由文件头和差值分布表组成。其中文件头的第1 Byte为标志字节(X),接着的1 Byte为阈值 T,紧跟其后的部分依次是差值分布表的上下非零端点(各2 Byte)、负载长度(4 Byte)。文件头共10 Byte,位流长度80。辅助信息的位流长度 $L_A=L_T+80$。

d)确定辅助信息嵌入位置。首先生成一幅与载体图像大小相同的二值图像作为辅助定位图,将所有像素初始化为黑色,用于临时记录辅助信息的嵌入位置,并用初值为0的记数器 A 记录所选像素中Ⅰ类差值的数量。用嵌入密钥 key 作为种子,随机选取一组位置不重复的●像素作为辅助信息的嵌入位置,并在辅助定位图中将选定的位置标记为白色。由于提取端事先并不知道阈值和差值分布表,无法从可扩展差值中提取辅助信息,本文用 LSB 替换的方法直接嵌入辅助信息。对选定的像素,若像素的相对位置为奇数,选择第1分量作为嵌入分量,否则第2分量为嵌入分量。保存嵌入分量灰度值的最低

位组成 LSB 位流(长为 L_A),计算预测误差差值 h、预测和 sa,若 h 为Ⅰ类差值且 $NSD_{sa}=0$,记数器 A 加 1。

e)计算负载能力。b)生成的Ⅰ类差值直方图 EN 中记录了每一预测和 sa 对应的Ⅰ类差值的频数,先计算可用于扩展嵌入的Ⅰ类差值数 pl_c,从 $sa=0$ 开始,若 $NSD_{sa}=0$,pl_c+EN_{sa},$sa+1$ 直到 511 为止。实际负载能力 $pl=pl_c-A-L_A$,若负载长度 PL 大于或等于 pl,$PL=PL-pl$,pl 存入文件头,否则,将实际需要嵌入的负载长度 PL 存入文件头,$PL=0$。

f)嵌入数据。辅助信息和 d)生成的 LSB 位流是数据提取和恢复图像所必需的信息,将和负载一起嵌入载体图像中。重新扫描图像,若辅助定位图对应位置为白色,则从辅助信息流中取 1 bit 数据替换嵌入分量灰度值的最低位。若辅助定位图对应位置为黑色,且 $NSD_{sa}=0$ 时,若 h 为Ⅰ类差值则从信息流中取 1 bit 数据 w,用式(11)计算 h',再用式(10)计算相应的 p_1' 和 p_2',若 h 为Ⅱ类差值,只作平移处理而不嵌入信息:当 $h<0$ 时,$h'=-T$,$h>0$ 时,$h'=T+1$,用式(10)计算相应的 p_1' 和 p_2',再由式(5)计算新的像素值 a_1'、a_2';若 $NSD_{sa}=1$,像素保持不变。

g)若 pass = 1 进入下一步。若 pass = 0,令 pass = 1,用图 2(b)所示的方案对像素进行分组,进入 b)继续嵌入数据。

h)若数据已全部嵌入,则结束循环。否则,选择下一分量组合,进入 a)。

2.5　隐藏数据的提取和图像恢复

数据信息的提取和图像恢复不需要原始图像,提取端需要两个参数,即嵌入密钥 key 和负载长度 PL。参数由嵌入端提供。辅助信息的嵌入位置由密钥决定,因此不知道密钥就无法提取数据,如果隐藏数据被正确提取,可根据需要恢复原始图像。具体的提取和恢复过程如下:

a)将含密图像拷贝到内存。

b)信息检测。在提取之前先进行检测,判断待测图像中是否嵌入数据。按 BG、GR 和 RB 顺序选取色彩分量组合,对每一分量组合,令 pass = 1,用图 2(b)所示的方案对像素进行分组,用密钥 key 作为种子,随机选取一组位置不重复的●像素,按嵌入过程 d)的方法对像素进行分类,提取 8 bit 数据组成标志字节,若标志字节与嵌入时相同(X),表明图像中确有嵌入数据信息,进入下一步提取数据;若无标志信息,选择下一分量组合继续检测,若所有分量组合均未检测到标志信息,表明没有嵌入数据,直接结束。

c)初始化。令 pass = 1,用图 2(b)方案对像素进行分组。

d)提取辅助信息。首先生成一幅与载体图像大小一致的二值图像作为辅助定位图,所有像素初始化为黑色。用嵌入密钥 key 作为种子,随机选取一组位置不重复的●像素,并在辅助定位图相应位置标记为白色。对选定的像素,提取嵌入分量灰度值的最低位写入辅助信息流,嵌入分量的选取方法与嵌入过程相同。当已提取 80 bit 辅助信息时,还原文件头并计算差值分布表的有效长度 L_T,继续提取 L_T bit 辅助信息,还原差值分布表 NSD。

e)提取数据。扫描图像,若辅助定位图的像素为黑色,计算对应●像素的预测误差 p_1' 和 p_2'、预测误差差值 h' 以及预测和 sa,若 $NSD_{sa}=0$,$h'\in[-2T,2T+1]$,则用式(12)提取 1 bit 数据并求出原始差值 h,将 h 代入式(10)计算 p_1 和 p_2,再由式(5)可得原始灰度值 a_1 和 a_2;若 $NSD_{sa}=0$,$h'\notin[-2T,2T+1]$,当 $h'<0$ 时,$h=-T$,$h'>0$ 时,$h=T+1$,用式(10)计算相应的 p_1 和 p_2,再由式(5)可得原始灰度值 a_1 和 a_2。从提取的信息流中分离负载和 LSB 位流。

f)恢复辅助信息嵌入位置的像素。扫描辅助定位图,从 LSB 位流中取 1 bit 数据替换嵌入分量灰度值的最低位。

g)若 pass = 0 进入下一步。若 pass = 1,令 pass = 0,用图 2(a)所示的方案对像素进行分组,进入 d)继续提取数据。

h)若数据已全部提取,则结束循环,此时可根据需要将内存中的数据写入图像,从而恢复原始图像。否则,选择前一分量组合,进入 c)。

3　实验结果及分析

采用 C++Builder6 开发平台进行仿真实验,图 4 是选取的几个典型的例子。其中第三幅为西安交通大学人工智能与机器人研究所东方人脸库(AI&R)的视点子库中的正面彩色图像 V_1173_10。对所选的四幅图像在红绿分量嵌入隐藏信息($T=2$),能保持较高的嵌入率(>0.75 bpp)和图像质量(PSNR>49 dB),如图 5 所示。表 2 中列出了色彩分量间预测误差差值扩展算法和单分量预测误差扩展方法在相同阈值下的嵌入率和 PSNR 对比实验结果。为了在同等条件下对比,单分量预测误差扩展方法在每一像素中从红绿分量中随机选取某一分量嵌入信息。实验结果表明:本文提出的双分量预测误差差值扩展算法充分利用自然图像色彩分量之间的相关性,将很小的差值扩展量($h+w$)分散到两个色彩分量中,减小了对图像的修改量,图像质量和嵌入率均有明显提高。

图4　原始图像示例

图5　嵌入信息的图像(*GR*组合，*T*=2)

表 2　嵌入率和 PSNR 对比结果(GR 组合,$T=2$)

图像	本文算法			单分量预测误差扩展		
	嵌入率	PSNR(G)	PSNR(R)	嵌入率	PSNR(G)	PSNR(R)
Lena	0.91	50.16	50.80	0.53	45.25	45.25
Baboon	0.85	49.42	49.91	0.21	43.88	43.85
V117310	0.79	49.72	50.17	0.49	44.81	44.80
Peppers	0.75	49.29	50.14	0.52	45.32	45.33

表 3 列出了本文算法和嵌入定位图算法在不同阈值的嵌入率和 PSNR 值。其中,所用直方图为色彩分量间预测误差差值直方图,直方图平移采用文献[2]算法,按 2.2 节所述的方法进行改进(即外部不改变),实验对象为 200×200V_1173_10 彩色图像的 GR 分量组合。实验结果表明:与使用定位图的方法相比,负载能力下降 0.02 bpp 左右,但实际嵌入的辅助信息少,图像质量有所提高(0.10 dB 左右)。

表 3　不同阈值下嵌入率和 PSNR 值对比实验

阈值	本文算法(无定位图)			嵌入定位图		
	嵌入率	PSNR(G)	PSNR(R)	嵌入率	PSNR(G)	PSNR(R)
0	0.327	54.05	55.78	0.342	54.15	55.70
1	0.651	51.53	51.68	0.672	51.51	51.56
2	0.790	49.72	50.17	0.822	49.65	50.00
3	0.859	48.77	48.89	0.892	48.68	48.71

4　结束语

针对 Tian 算法存在过分修改像素对值、(下转第 1028 页)

$$T_1 = M_T(\text{不信任}) = (1,0,0,0,0)$$
$$T_2 = M_T(\text{有点信任}) = (0,1,0,0,0)$$
$$T_3 = M_T(\text{信任}) = (0,0,1,0,0)$$
$$T_4 = M_T(\text{非常信任}) = (0,0,0,1,0)$$
$$T_5 = M_T(\text{完全信任}) = (0,0,0,0,1)$$

计算出信任值后,将根据具体的隶属度函数计算出信任值对应的信任向量 $V = \{v_1, v_2, v_3, v_4, v_5\}$。其中 $v_i (i = 1, 2, 3, 4, 5)$,然后信任级别的确定可通过如下方式之一来计算:

a)基于格贴近度的计算方式。当得到信任向量 V 之后,计算它与各个级别的贴近度 $\sigma(V, T_i) = (V \circ T_i) \wedge (1 - V \ 7 \ T_i)$,这里 $\circ$ 和7 分别表示内积和外积,然后取最大值即可得出相应的信任级别。

b)基于去模糊化处理。当得到信任向量 $V = \{v_1, v_2, v_3, v_4, v_5\}$。其中 $v_i (i = 1, 2, 3, 4, 5)$ 之后,根据去模糊化函数 $DF(V) = \sum_{i=1}^{5} v_i m_i$。其中 v_i 是 V 中的第 i 个元素,m_i 表示第 i 个位置,这样便得出一个介于 1 ~ 5 的数值,然后根据最邻近原则确定信任级别。

4 模糊认证过程

有了认证路径的计算方法后,就可以此为基础对基本 PKI 认证过程进行扩展。假设网络中的通信实体 A 要向 B 发送消息 m,那么他们的通信过程如下:$A \rightarrow B \{M, Sig_A(M), PUB_A, Cer(A)\}$。其中 $Sig_A(M)$ 是 A 利用自己的私钥对消息 M 的签名,PUB_A 是 A 的公钥,Cer(A)是为 A 的证书。当 B 接收到上述消息之后,首先使用 CA 公钥来验证 Cer(A)的合法性,再通过 PUB_A 来验证签名 $Sig_A(M)$ 来决定消息的真实性,然后 B 根据自己的信任树来计算对 A 的信任值 $\mu_R(B, A)$,根据信任值来决定消息的信任级别。一般来说对于重要消息要求的信任值要相对较大,从而信任级别要相对较高。

5 结束语

本文中根据模糊逻辑对基于证书的 PKI 认证方式进行了扩展,以模糊图论为基础对认证路径的构造以及信任值的传递计算规则进行了研究,并根据计算出来的信任值给出了一种直观的信任推理机制来确定信任级别,为网络认证的研究提供了一条新的思路。

参考文献:

[1] 唐文,胡建斌,陈钟. 基于模糊逻辑的主观信任管理模型研究[J]. 计算机研究与发展,2005,42(10):1654-1659.

[2] JASANG A. A logic for uncertain probabilities [J]. International Journal of Uncertainty Fuzziness, Fuzziness and Knowledge-based Systems, 2001,9(3):279-311.

[3] BLAZE M, FEIGENBAUM J, KEROMYTIS A D. Trust management for public-key infrastructure [C]//Proc of Cambridge Security Protocol International Workshop. Berlin: Springer-Verlag,1998: 59-63.

[4] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open networks [C]// Proc of the 3rd European Symposium on Research in Computer Security. London:Springer-Verlag,1994: 3-18.

[5] 张仕斌,何大可,遠藤誉. 模糊自主信任建立策略的研究[J]. 电子与信息学报,2006,28(8):1492-1496.

[6] 谢冬青,冷键. PKI 原理与技术[M]. 北京:清华大学出版社,2004:79-80.

[7] 彭祖赠,孙韫玉. 模糊数学及其应用[M]. 武汉:武汉大学出版社,2004:182-188.

(上接第 1018 页)须嵌入溢出定位图、不适合彩色图像等缺点,提出一种基于色彩分量间预测误差差值扩展的彩色图像可逆数据隐藏算法。该算法将差值扩展量分散到两个色彩分量中,减少了对图像的修改,从而提高含密图像质量。信息提取不需要原始图像,提取端不需要溢出定位图即可提取数据并恢复原始图像,算法实现和运算效率都具有一定的优势。辅助信息的嵌入位置由密钥决定,隐藏数据相对安全,信息检测简单、高效,避免在不含隐藏数据的图像中提取信息。实验表明,该算法在不影响嵌入容量和图像质量的基础上,提高了嵌入、检测和提取的效率,有利于批量嵌入。算法的不足之处在于,当Ⅲ类差值比较分散时,嵌入容量受到限制,下一步的工作重点是在消除定位图的前提下提高嵌入容量。

参考文献:

[1] TIAN Jun. Reversible data embedding using a difference expansion [J]. IEEE Trans on Circuits and Systems for Video Technology,2003,13(8):890-896.

[2] THODI D M, RODRIGUEZ J J. Expansion embedding techniques for reversible watermarking [J]. IEEE Trans on Image Processing, 2007,16(3):721-730.

[3] ALATTER A M. Reversible watermark using the difference expansion of a generalized integer transform [J]. IEEE Trans on Image Processing,2004,32(8):1147-1156.

[4] 陈开英,胡永健,李健伟. 利用差值扩展进行可逆数据隐藏的新算法[J]. 计算机应用,2008,28(2):455-459.

[5] 邓世文,刘焕平,叶宏宇. 基于 Laplacian 残差扩展的可逆嵌入算法[J]. 计算机工程与应用,2008,44(3):110-113.

[6] 彭德云,王嘉祯. 基于错误控制编码的差值扩展可逆数字水印[J]. 计算机工程,2007,33(21):18-20.

[7] COLTUC D, CHASSER J M. Very fast watermarking by reversible contrast mapping[J]. IEEE Signal Processing Letters,2007,14(4): 255-258.

[8] LIN C, YANG S, HSUEH N. Lossless data hiding based on difference expansion without a location map [C]//Proc of Congress on Image and Signal Processing. 2008:8-12.

[9] 周璐,胡永健,曾华飞. 用于矢量数字地图的可逆数据隐藏算法[J]. 计算机应用,2009,29(4):990-993.

[10] WU Dan, WANG Guo-zhao, GAO Xiao-liang. Reversible watermarking of SVG graphics[C]//Proc of International Conference on Communications and Mobile Computing. 2009:385-390.

[11] HU Yong-jian, LEE H, LI Jian-wei. DE-based reversible data hiding with improved overflow location map [J]. IEEE Trans on Circuits and Systems for Video Technology,2009,19(2):250-260.

[12] CHRYSOCHOS E, VARSAKI E E, FOTOPOULOS V, *et al*. High capacity reversible data hiding using overlapping difference expansion [C]//Proc of Workshop on Image Analysis for Multimedia Interactive Services. 2009 :121-124.

[13] 祝玉新,孙星明,杨恒伏. 基于 Haar 小波的彩色图像可逆水印算法[J]. 计算机应用研究,2007,24(6):165-169.

[14] 杨边,陆哲明,徐殿国,等. 基于邻近像素的低复杂度预测矢量量化图像压缩编码算法[J]. 电子学报,2003,31(5):707-710.

[15] 曹文伦,彭国华,秦洪元,等. 利用色彩分量相关性的彩色图像分形编码方法[J]. 计算机工程与应用,2004,40(22):51-55.