

基于完整上下文预测的可逆数据隐藏

罗剑高¹ 韩国强²

(广东农工商职业技术学院计算机系 广州 510507)¹

(华南理工大学计算机科学与工程学院 广州 510006)²

摘要 提出一种非线性、自适应、基于完整上下文的梯度调整预测算子 FCGAP。FCGAP 适用于图像可逆数据隐藏算法。在 FCGAP 中,目标像素的预测值等于 4 邻域像素值的加权平均,加权系数由与目标像素最近距离的 12 近邻确定。采用 FCGAP,提出一种高容量低失真的可逆数据隐藏算法。实验结果表明,FCGAP 能充分利用上下文信息,提高像素预测精度,基于 FCGAP 提出的可逆数据隐藏算法相比已有可逆数据隐藏算法具有更好的容量-失真性能。

关键词 可逆数据隐藏,无损数据隐藏,可逆图像水印,预测误差扩展,完整上下文预测

中图分类号 TP391 **文献标识码** A

Reversible Data Hiding Based on Full Context Prediction

LUO Jian-gao¹ HAN Guo-qiang²

(Department of Computer, Guangdong AIB Polytechnic College, Guangzhou 510507, China)¹

(School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China)²

Abstract We propose a nonlinear, adaptive, gradient-adjusted predictor based on full context (FCGAP). FCGAP is suitable for reversible image data hiding. In FCGAP, the predicted value of target pixel is equal to the weighted average of 4 neighborhood pixels, and the weighted coefficients are computed by 12 nearest neighbor pixels. Based on FCGAP, a reversible data hiding is proposed, which can provide high data embedding capacity and low distortion. Experimental results demonstrate that FCGAP can more fully utilize context information, and has better prediction accuracy of pixels than other predictors; the reversible data hiding based on FCGAP has better capacity-distortion performance compared with other state-of-the-art algorithms.

Keywords Reversible data hiding, Lossless data hiding, Reversible image watermarking, Prediction error expansion, Full context prediction

1 引言

可逆数据隐藏(RDH; reversible data hiding)是一种不仅可从含秘载体(隐藏了目标数据的载体)中提取目标数据且能把含秘载体恢复成原宿主的信息隐藏技术,适用于对宿主失真特别敏感的数据隐藏应用。图像 RDH(通常也称为可逆图像水印、无损图像水印、可擦除图像水印等)最早用于敏感图像(如医学图像)认证^[1],随着数据嵌入能力的提高,图像 RDH 除可满足日趋完善的敏感图像认证应用^[2,3]要求外,还被扩展到敏感图像隐秘通信、内容标注^[4]等应用领域。

RDH 是一个可逆的处理过程,设计一个嵌入容量-失真性能理想的 RDH 算法关键在于发现适用于 RDH 的有效可逆变换。近几年,基于预测误差扩展(PEE, prediction-error expansion)的图像 RDH 算法得到研究人员的广泛关注。因具有更好利用宿主空间冗余的能力,PEE 相比无损压缩^[5]、像素对差值扩展^[6]、像素整数变换^[7]、像素差直方图位移变换^[8]等更适用于图像 RDH,文献中一系列 PEE 图像 RDH 算

法^[9-13]的良好性能充分验证了 PEE 的有效性。对于 PEE 图像 RDH 算法,数据隐藏量和含秘载体的失真度在很大程度上取决于 RDH 所采用预测算子的性能。预测算子预测越准确,宿主冗余挖掘就越充分,预测误差值就越小,预测误差扩展引入的失真就越小。已有 PEE 图像 RDH 算法所采用的预测算子通常借鉴压缩领域中的预测方法,如 Thodi 等^[9]使用无损 JPEG 压缩标准中的 MED(median edge detector)、Li 等^[10]使用 CALIC 编码算法中的 GAP^[14](gradient-adjusted predictor)。随着 RDH 技术的进步,研究人员注意到,从压缩领域借鉴过来的预测方法仅使用当前像素半方向的近邻像素作为预测上下文(half context 半方向上下文),无法充分利用当前像素的近邻信息,其预测精度受到限制;图像压缩编、解码过程中使用半方向上下文预测的原因是由于当前像素之后的像素值是完全不可知的,因此无法被用于构造预测上下文,但这个限制在图像数据隐藏领域却是可以避免的。曾等^[11]提出基于 4 邻域(作者称之为全方向)的像素预测算子,宿主被划分为两个相互交错的像素集,当前像素利用处在另一像

本文受国家自然科学基金项目(61070090, 61003270),国家自然科学基金广东省联合基金项目(U1035004),广东省重大科技专项基金(2010A080402005)资助。

罗剑高(1971—),男,博士,副教授,主要研究方向为图像处理、数字水印、信息安全, E-mail: 13924226966@139.com; 韩国强(1962—),男,博士,教授,博士生导师,主要研究方向为图像处理、多媒体技术。

素集上的 4 邻域进行加权计算。Cheng 等^[12]提出几个基于 4 或 8 邻域的较为简单的预测算子，宿主首先被分割成相互交错的 4 个子集，当前像素值利用处在其他子集中的 4 或 8 邻域像素值进行预测。Yang 等^[13]提出一种基于 4 邻域的梯度加权预测算子 (GEDP: gradient-based edge direction prediction)，把宿主划分成两个相互交错的像素集，当前像素值利用处在另一像素集上的 4 邻域进行加权预测，加权系数基于一组 5×5 的模板运算，利用局部梯度特征获得。

曾等^[11]、Cheng 等^[12]及 Yang 等^[13]提出的基于 4 或 8 邻域的预测算子虽比基于半方向上下文的预测算子更为有效，但对当前像素上下文的利用还不是很充分，且使用时受诸如需划分子集的限制。针对这些不足，本文提出一种基于完整上下文的梯度调整预测算子，为描述方便，我们把它简称为 FCGAP (full context GAP)。FCGAP 无需子集划分，当前像素上下文信息利用得更为充分。采用 FCGAP，提出一种有效的 PEE 图像 RDH 算法。

2 预测误差扩展

在描述本文提出的算法之前，先回顾文献[9]中 PEE 的相关内容。

文献[9]中的 PEE 变换包含两个基本过程：像素预测误差计算、基于预测误差扩展的像素值变换。

在数据嵌入端，首先通过某种像素预测算子，对宿主 I 的当前像素值进行预测，设当前像素值为 x ，其预测值为 \hat{x} ，则预测误差 e 定义为：

$$e = x - \hat{x} \quad (1)$$

然后进行如下基于 e 扩展的数据嵌入：

$$e' = \begin{cases} e + \Delta + 1, & \text{if } e > \Delta \\ e - \Delta - 1, & \text{if } e < -\Delta - 1 \\ 2e + b, & \text{other} \end{cases} \quad (2)$$

式中， Δ 为大于等于 0 的数据嵌入容量参数，用于控制 RDH 的数据嵌入容量和载体的嵌入失真，RDH 可嵌入的数据总量等于 e 处在区间 $[-\Delta - 1, \Delta]$ 的像素量。 b 为嵌入的数据比特 (0 或 1)。由扩展后的预测误差 e' 可得到嵌入数据后的像素值 x' ：

$$x' = \hat{x} + e' \quad (3)$$

由式(1)一式(3)，可知：

$$x' = \begin{cases} x + \Delta + 1, & \text{if } e > \Delta \\ x - \Delta - 1, & \text{if } e < -\Delta - 1 \\ x + e + b, & \text{other} \end{cases} \quad (4)$$

在数据提取端，设含密图像为 I' 。如果由 I' 能计算到与嵌入端相同的各像素预测值 \hat{x} ，则可以通过式(1)一式(3)的逆操作式(5)一式(7)实现嵌入数据的提取和宿主 I 的恢复：

$$e' = x' - \hat{x} \quad (5)$$

$$e = \begin{cases} e' - \Delta - 1, & \text{if } e' > 2\Delta + 1 \\ e' + \Delta + 1, & \text{if } e' < -2\Delta - 2 \\ \lfloor e'/2 \rfloor, & \text{other} \end{cases} \quad (6)$$

$$x = e + \hat{x} \quad (7)$$

嵌入的数据由式(8)依次对满足条件的 e' 进行模 2 计算得到：

$$b = \text{mod}(e', 2) \text{ if } 2\Delta + 1 \geq e' \geq -2\Delta - 2 \quad (8)$$

3 基于完整上下文预测的 RDH

按某种次序逐一对宿主像素进行第 2 节的 PEE 变换时，当前像素的部分邻域已完成变换，部分邻域还处在初始状态，现有预测算子在对当前像素进行预测时，通常对已做了变换的邻域不加利用，致使一些十分重要的预测信息得不到利用。

由式(4)可知，PEE 变换过程中像素值的变化量不大于 $\Delta + 1$ 。为了避免像素值过大变化导致失真性能的恶化， Δ 一般取较小的值 (当待嵌入数据量较大， Δ 无法满足容量需求时，可通过执行多次可逆数据嵌入过程解决)，因而，有理由相信已做变换的邻域像素值与当前像素仍保持着较强相关性，可以作为预测当前像素值的参考。我们还注意到，有效的 RDH 算法要求含密图像与宿主图像之间不应有较明显的视觉差异，换句话说，含密图像很大程度上保留了宿主图像的像素纹理、梯度等特性，所以，已做变换的邻域像素值同还未变换的邻域像素值一样，可以用于计算目标像素位置的像素值梯度，而有效的梯度信息对像素预测是非常有帮助的。基于以上两点观察，本文提出基于 12 最近邻像素的像素值预测法——FCGAP (GAP based on full context)，在此基础上，提出一种大容量的图像 RDH 算法，为叙述方便，本文宿主默认为 8bit 灰度图像。

3.1 基于 12 近邻像素的像素预测

文献[14]提出的 GAP 是一个简单而有效的非线性像素预测算子。为方便接下来的预测算子描述，如图 1，令：

$$\begin{aligned} I_m &= I_{(i, j-2)}, I_{me} = I_{(i+1, j-2)}, I_{mw} = I_{(i-1, j-1)}, I_n = I_{(i, j-1)}, \\ I_{nw} &= I_{(i+1, j-1)}, I_{uw} = I_{(i-2, j)}, I_w = I_{(i-1, j)}, I_e = I_{(i+1, j)}, I_{ee} = \\ I_{(i+2, j)}, I_{se} &= I_{(i-1, j+1)}, I_s = I_{(i, j+1)}, I_{sw} = I_{(i+1, j+1)}, I_{ss} = I_{(i, j+2)} \end{aligned} \quad (9)$$

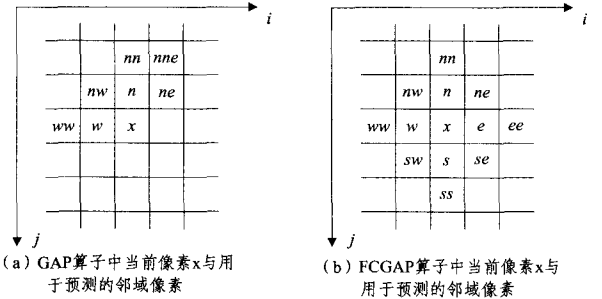


图 1 当前像素与用于预测的参考像素的位置关系

GAP^[14]用半方向的近邻分别估计当前像素 $I(i, j)$ 处水平方向和垂直方向上的像素值梯度 d_h, d_v ：

$$\begin{cases} d_h = |I_w - I_{uw}| + |I_n - I_{nw}| + |I_n - I_{ne}| \\ d_v = |I_w - I_{mw}| + |I_n - I_m| + |I_e - I_{me}| \end{cases} \quad (10)$$

根据 d_h, d_v ，计算 $I(i, j)$ 的预测值 $\hat{I}(i, j)$ ：

$$\hat{I}(i, j) = \begin{cases} I_w, & \text{if } d_v - d_h > 80, & \text{强水平边} \\ I_n, & \text{if } d_v - d_h < -80, & \text{强垂直边} \\ (\bar{I} + I_w)/2, & \text{if } 80 \geq d_v - d_h > 32, & \text{水平边} \\ (3\bar{I} + I_w)/4, & \text{if } 32 \geq d_v - d_h > 8, & \text{弱水平边} \\ (\bar{I} + I_n)/2, & \text{if } -8 \leq d_v - d_h < -32, & \text{垂直边} \\ (3\bar{I} + I_n)/4, & \text{if } 8 \leq d_v - d_h < -8, & \text{弱垂直边} \end{cases} \quad (11)$$

式中， $\bar{I} = (I_w + I_n)/2 + (I_{nw} - I_{mw})/4$ 。

如前所述，在 RDH 中，已做变换的邻域像素同未做变换

的邻域像素一样,可以作为预测当前像素值的参考像素。借鉴 GAP,本文提出一种适用于 RDH 的基于完整上下文的像素预测算子——FCGAP,如图 1(b)所示,当前像素值利用 12 个最近邻像素预测:

首先估算当前像素 $I(i, j)$ 处水平方向和垂直方向上的像素值梯度 d_h, d_v :

$$\begin{cases} d_h = |I_w - I_{ww}| + |I_n - I_{nw}| + |I_n - I_{ne}| + |I_e - I_{ee}| + |I_s - I_{sw}| + |I_s - I_{se}| \\ d_v = |I_n - I_{nw}| + |I_w - I_{nw}| + |I_w - I_{sw}| + |I_e - I_{se}| + |I_e - I_{se}| + |I_s - I_{se}| \end{cases} \quad (12)$$

然后由式(11)预测 $I(i, j)$, 式中 $\bar{I} = (I_w + I_n + I_e + I_s) / 4$ 。

基于 FCGAP 的 RDH,按从上到下、从左到右的顺序依次对宿主像素进行数据嵌入处理:对于某个具体的待处理的当前像素 $I(i, j)$,利用 6 个已执行变换处理的近邻像素值 $I'_m, I'_{nw}, I'_n, I'_{ne}, I'_{ww}, I'_w$ 和 6 个初始近邻像素值 $I_e, I_{ee}, I_{sw}, I_s, I_{se}, I_{ss}$ 计算预测值和预测误差,执行预测误差扩展的数据嵌入。数据提前时,按从下到上、从右到左的顺序依次对含秘图像进行相应的逆处理:某个具体的待处理的当前像素 $I(i, j)$, $I_e, I_{ee}, I_{sw}, I_s, I_{se}, I_{ss}$ 为已执行逆处理的像素恢复值, $I'_m, I'_{nw}, I'_n, I'_{ne}, I'_{ww}, I'_w$ 为还未进行逆处理的像素值。显然,对于每个待处理的像素,数据嵌入阶段和数据提取阶段计算出的预测像素值是相同的,可保证第 2 节 PEE 逆操作的正确性。

需指出的是,对于处在边界上的像素,执行式(11)、式(12)时,可用对应的镜像像素替代不存在的一些近邻像素值。如对 $I(1, 1)$ 来说,不存在 $I_m, I_{nw}, I_n, I_{ne}, I_{ww}, I_w$, 计算时,可分别用对应的映射像素 $I_s, I_{sw}, I_s, I_{se}, I_{ee}, I_e$ 代替。

3.2 基于 FCGAP 的 RDH 数据嵌入

本小节对本文 RDH 算法数据嵌入阶段的相关过程进行具体说明。

3.2.1 多层嵌入

为限制像素值变化的幅度,本文 RDH 中约定 Δ 在 $[0, 15]$ 范围取值, Δ 用 4 比特表示。PEE 图像 RDH 算法单层(单次)嵌入的数据量不大于 1bpp(bit per pixel 每像素比特),为嵌入更大的数据量,可执行多层嵌入,这是可逆数据隐藏相对常规数据隐藏所特有的属性。本文 RDH 在执行多层嵌入时,层与层之间的数据嵌入过程相对独立,为了在数据提取时能识别数据提取的最末层(对应着数据嵌入阶段的首层),可用 1 比特作为层标示位,具体安排见 3.2.2 节。

3.2.2 辅助信息及待嵌入载荷结构

为了在数据提取端能够正确地执行嵌入端数据处理的逆变换,需要知道嵌入端嵌入数据时所用的一些参数,这些参数我们称之为辅助信息。

一般地, RDH 算法的辅助信息包括两个方面:数据嵌入参数;灰度溢出相关信息。

由于扩展嵌入过程中,像素值增加或减少一个不大于 $\Delta + 1$ 的值可能导致一些像素的值越出像素值范围(8bit 级的灰度像素取值范围为 $[0, 255]$),破坏变换的可逆性。本文 RDH 在预测误差扩展嵌入数据操作前采用灰度压缩的预处理来解决这个问题。为保证数据嵌入操作后的灰度值处在 $[0, 255]$,先把载体灰度值变换到 $[\Delta + 1, 254 - \Delta]$,变换信息用标示比特串 F 记录: F 初值为空,从上到下、从左到右的

次序依次变换参与 Δ 扩展变换的像素,如当前灰度值 $x \in [0, \Delta]$ 或 $[255 - \Delta, 255]$,则令 $x = x + \Delta + 1$ 或 $x - \Delta - 1$,同时在 F 末尾追加 1 位值为‘1’的标示比特;如当前像素值 $x \in [\Delta + 1, 2\Delta + 1]$ 或 $[254 - 2\Delta, 254 - \Delta]$,则 x 不变,在 F 末尾追加 1 位值为‘0’的比特;其他情况不做处理。在数据提取、图像恢复端,根据 F 可对图像块像素执行相应的逆操作,恢复到灰度压缩前的状态。

本文 RDH 数据嵌入参数仅含两个:第 2 节定义的 Δ 和 3.2.1 节的层标示比特。

为了实现数据的盲提取和宿主的盲恢复,即不需要额外数据传输的隐藏数据提取和原始载体恢复,我们对上述辅助信息的传送进行如下处理:

首先收集宿主头 4 像素 LSB 上的比特,设为 L ,同时置这些像素的 LSB 为 0,用下式更新待嵌入的数据 D :

$$D = L + D \quad (13)$$

当前嵌入层标示比特 f 与当前溢出信息标示比特串 F 作为待嵌入数据的一部分实现传送,待嵌入载荷的结构安排如下:

$$P = f + F + D \quad (14)$$

多层嵌入过程中非最末层的层嵌入参数 Δ 取值约定为 15,无需传送处理,最末层的 Δ 用宿主头 4 像素 LSB 比特表示; D 为当前层待嵌入的数据,当前载荷 P 在当前层数据嵌入后的剩余部分作为下一层的待嵌数据 D ,即首层待嵌数据 D 为式(13)定义的数据,其他层的待嵌数据 D 为上一层载荷 P 执行嵌入后的剩余部分;首层嵌入令 f 为 1,其他为 0。

在数据嵌入过程中,当给定的待隐藏数据被完整嵌入后,为保证嵌入过程的可逆,需嵌入一些填充比特。为了在数据提取端,能分辨填充比特,本文 RDH 作如下处理:以‘0’比特作为有效嵌入数据的结束标示,即有效数据完整嵌入后,紧接着嵌入一个‘0’比特;用比特‘1’作为填充比特。数据提取时,丢弃提取比特串中最末‘0’比特及之后的比特序列,可得到嵌入端嵌入的数据 D 。

3.2.3 数据嵌入过程及容量参数 Δ 的确定

数据嵌入端的数据嵌入处理过程由 3 个部分组成:容量参数与 LSB 置换;宿主灰度值压缩;像素预测误差计算及预测误差扩展变换,其中容量参数 Δ 由迭代过程确定,具体过程描述如下:

(1)收集宿主头 4 个像素 LSB 的比特,设为 L ,同时置这些像素 LSB 为 0;用式(13)更新待嵌入的数据 D 。

(2)令 Δ 为 15。

(3)对当前宿主(用于比特置换的头 4 像素除外)进行数据嵌入处理;执行灰度压缩;构造当前待嵌入载荷;执行载荷数据的扩展嵌入。

(4)如当前载荷嵌入完毕,令 $\Delta = \Delta - \lceil \Delta / 2 \rceil$,进入末层嵌入阶段,重新执行第 3)步,重复该过程,直至 Δ 为能满足载荷数据完整嵌入的最小值;否则,用当前载荷嵌入 P 的剩余部分更新待嵌数据 D ,用当前含秘载体更新宿主,转第 3)步执行新一层的数据嵌入。

(5)用填充比特完成扩展变换过程,最后用表示当前 Δ 的 4 比特更新宿主头 4 像素的 LSB,结束数据嵌入过程。

3.3 数据提取、宿主恢复

数据提取、宿主恢复过程是数据嵌入阶段的逆过程,具体步骤如下:

1) 提取含秘图像 I' 头 4 像素 LSB 比特, 将其换算为容量参数 Δ , 同时把这些 LSB 置 0。设提取的数据 D 初始为空。

2) 从图像 I' 末尾位置开始, 按从下到上、从右到左的顺序依次计算预测误差, 进行相应的逆变换, 提取数据, 恢复像素值(用于比特置换的头 4 像素除外)。设该阶段提取的数据比特串为 B' , B' 比特串次序倒转得到当前层提取的比特串 B 。

3) 从当前 B 的前端比特中读取嵌入层标示 f 和溢出信息, 进行相应的灰度压缩恢复, 舍弃当前辅助信息比特后的 B 为 D' , 用 $D'+D$ 更新 D 。

4) 如果 f 为 0, 用当前层输出图像更新 I' , 用 15 更新 Δ , 然后转到第 2) 步; 否则用 D 头 4 比特更新当前层输出图像头 4 个像素的 LSB, 更新后的图像为恢复的宿主, 舍弃 D 头 4 比特和末尾的填充比特, 得到所求的目标数据 D , 过程结束。

4 实验及结果分析

为验证 FCGAP 及文中 RDH 算法的有效性, 我们在 Matlab 平台上实现了文中 RDH 算法, 并与有代表性的典型 RDH 算法进行性能之间的比较。实验中, 待嵌入的数据由 Matlab 的随机函数产生, 宿主选用 USC-SIP1 图像数据库^[15]中多种不同性质的图像。

图 2 是实验中 4 幅有代表性的测试图, Lena、Plane 代表平滑或较平滑图像, Baboon、Barbara 代表全局纹理或局部纹理较丰富的图像。用作性能比较的典型 RDH 算法中, Li 等^[10]采用的是基于半方向上下文的 GAP 算子, 该算法的贡献是提出了一种能根据局部区域特征自适应地调整数据嵌入方式的方法, 可有效地利用宿主图像的局部特征, 通过增加平滑区域的数据嵌入比例降低数据嵌入的整体失真; 曾等^[11]、Yang 等^[13]算法所采用的像素值预测算子是目前最为有效的预测算子之一。曾等^[11]算法中的预测算子与 Luo 等^[16]类似, 都借用了较为有效的插值技术, 不过由于其仅仅基于 4 邻域, 无法利用其他邻域信息, 因而冗余信息的挖掘还不充分。Yang 等^[13]算法中的预测算子在预测当前像素值时, 参与计算的像素不都是最近邻, 因而冗余的挖掘也不是太充分。本文采用的 FCGAP 在预测当前像素值时利用的是最近邻 12 像素的信息, 相比曾等^[11]和 Yang 等^[13]算法中的预测算子具有更高的机会获得理想的相关信息, 从而得到更准确的预测值。

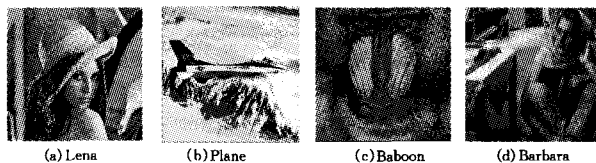
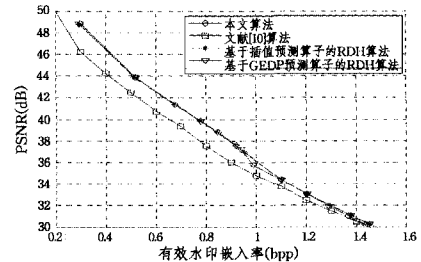


图 2 测试图像

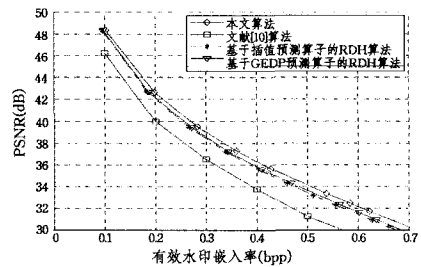
实验中, 为方便考察 FCGAP 有效性, 分别基于 FCGAP、曾等^[11]采用的插值预测算子、Yang 等^[13]采用的 GEDP 算子按 3.2 节和 3.3 节所述实现 3 个多层嵌入的 RDH 算法, 它们之间的区别仅在于所采用的预测算子不同。后 2 个算法用于验证本文基于 FCGAP 的 RDH 算法的有效性。

由图 3 的嵌入容量-失真曲线可以较明显地看到: 本文算法在宿主纹理较丰富时, 容量-失真性能具有较大优势, 这得益于 FCGAP 预测算子的有效性; 当作用在较为平滑的宿主

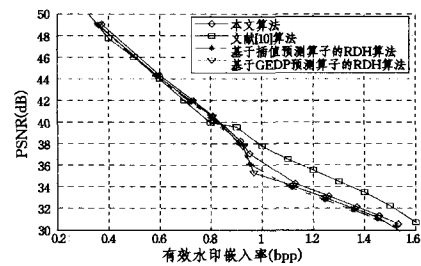
上时, 本文算法与基于曾等^[12]、Yang 等^[14]预测算子的 RDH 算法性能没有明显差别, 原因是三者的预测算子此时都比较有效, FCGAP 优势不明显。基于半方向上下文预测算子的 Li 等^[10]算法相比 3 个基于全方向上下文预测算子算法的性能, 在图 3(a)、(b)、(d) 中表现出明显的不足, 这是由其预测算子相对不足导致的, 虽然该算法采用了提高局部特征利用率的自适应方法; 在图 3(c) 中, Li 等^[10]算法性能相对更优, 这是因局部特征利用带来的性能改善大于预测算子不足的影响。



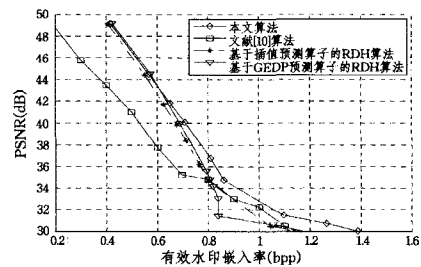
(a) Lena



(b) Baboon



(c) Plane



(d) Barbara

图 3 基于 FCGAP 的本文算法与 Li 等^[10]、基于的插值预测算子和基于 GEDP 预测算子的 RDH 算法的性能对比

图 3(a)、(c)、(d) 中, 文中实现的 3 种算法的容量-失真曲线存在一个不同程度的突变区, 这是因 2 次(层)嵌入引起的, 图 3(b)各算法仅进行了一层嵌入, 没有出现曲线突变现象。执行多层嵌入时, 优化每层的嵌入参数 Δ 可进一步提高容量-失真性能, 改善性能突变程度, 参数 Δ 如何优化是一个不小的挑战, 有待于后续的研究。

结束语 PEE 图像 RDH 算法能有效挖掘宿主像素间的

冗余信息,因而一般能获得较好的容量-失真性能。在此类 RDH 算法中,算法性能在很大程度上决定于预测算子的预测精度。图像的基本理论告诉我们,距离目标像素越近的近邻与目标像素相关度越高,文中提出的 FCGAP,基于 12 最近邻进行像素值预测处理,有利于充分挖掘目标像素的相关信息,获得比现有仅基于部分最近邻像素的预测算子更好的预测精度。实验结果表明,文中基于 FCGAP 的图像 RDH 较现有可逆数据隐藏算法具有更理想的容量-失真性能,FCGAP 适用于 RDH 算法,基于完整上下文的预测算子用于 RDH 是可行的。

参 考 文 献

[1] Cox I J, Miller M L, Bloom J A, et al. Digital watermarking and steganography (2nd ed) [M]. Burlington: Morgan Kaufman, 2008: 385-395

[2] 罗剑高, 韩国强, 沃焱, 等. 篡改定位精度可动态调整的无损图像认证算法[J]. 华南理工大学学报: 自然科学版, 2011, 39(7): 121-126

[3] 罗剑高, 韩国强, 沃焱, 等. 基于自适应图像块组合的无损图像认证算法[J]. 通信学报, 2012, 33(6): 64-72

[4] Yu Y H, Chang C C. A high capacity reversible data hiding scheme for annotation [A] // Second International Symposium on Intelligent Information Technology Application [C]. Shanghai, China, 2008: 940-944

[5] Celik M U, Sharma G, Tekalp A M, et al. Lossless generalized-LSB data embedding [J]. IEEE Transactions on Image Processing, 2005, 14(2): 253-266

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

[7] Alattar A M. Reversible watermark using the difference expansion of a generalized integer transform [J]. IEEE Transactions on Image Processing, 2004, 13(8): 1147-1156

[8] 曾宪庭, 李卓, 平玲娣. 基于块参照像素的无损信息隐藏算法[J]. 计算机科学, 2012, 39(2): 47-51

[9] Thodi D M, Rodriguez J J. Expansion embedding techniques for reversible watermarking [J]. IEEE Transactions on Image Processing, 2007, 16(3): 721-730

[10] Li X L, Yang B, Zeng T Y. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection [J]. IEEE Transactions on Image Processing, 2011, 20(12): 3524-3533

[11] 曾晓, 陈真勇, 陈明, 等. 基于全方向预测与误差扩展的可逆数据隐藏 [J]. 计算机研究与发展, 2010, 47(9): 1595-1603

[12] Chen M, Chen Z Y, Zeng X, et al. Model order selection in reversible image watermarking [J]. IEEE Journal of Selected Topics in Signal Processing, 2010, 4(3): 592-604

[13] Yang W J, Chung K L, Liao H Y M, et al. Efficient reversible data hiding algorithm based on gradient-based edge direction prediction [J]. The Journal of Systems and Software, 2013, 86(2): 567-580

[14] Wu X L, Memon N. Context-based, adaptive, lossless image coding [J]. IEEE Transactions on Communication, 1997, 45(4): 437-444

[15] Signal and Image Processing Institute, University Southern California, Los Angeles. Image Database [EB/OL]. <http://sipi.usc.edu/database/>, 2012-3-26

[16] Luo L X, Chen Z Y, Chen M, et al. Reversible image watermarking using interpolation technique [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(1): 187-193

(上接第 209 页)

[10] Selvi S S D, Vivek S S, Ragan C P. Security weaknesses in two certificateless signcryption schemes[OL]. Cryptology ePrint Archive; Report 2010/092, Available from: <http://eprint.iacr.org/2010/092>

[11] Liu Z, Hu Y, Zhang X, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(3): 452-464

[12] Weng J, Yao G, Deng R H, et al. Cryptanalysis of a certificateless signcryption scheme in the standard model[J]. Information Sciences, 2011, 181(3): 661-667

[13] Chen L, Cheng Z, Smart N. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security, 2007, 6(2): 213-241

[14] Cao X, Kou W. A Pairing-free Identity-based Authenticated Key Agreement Scheme with Minimal Message Exchanges[J]. Information Sciences, 2010, 180(6): 2895-2903

[15] He D, Chen J, Hu J. An ID-based proxy signature schemes without bilinear pairings[J]. Annals of Telecommunications, 2011, 66(11/12): 657-662

[16] Barreto P, Deusajute A, Cruz E, et al. Toward efficient certifi-

cateless signcryption from (and without) bilinear pairings[OL]. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_03_artigo.pdf

[17] Selvi S S D, Vivek S S, Ragan C P. Cryptanalysis of Certificateless Signcryption Schemes and an Efficient Construction Without Pairing[C] // Inscrypt 2009, 2010: 75-92

[18] Xie W, Zhang Z. Certificateless Signcryption without Pairing", Cryptology ePrint Archive; Report 2010/187 [OL]. Available from: <http://eprint.iacr.org/2010/187>

[19] Zhu H, Li H, Wang Y. Certificateless Signcryption Scheme Without Pairing[J]. Journal of Computer Research and Development, 2010, 47(9): 1587-1594

[20] Liu W, Xu C. Certificateless Signcryption Scheme Without Bilinear Pairing[J]. Journal of Software, 2011, 22(8): 1918-1926

[21] Jing X. Provably Secure Certificateless Signcryption Scheme without Pairing[C] // 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. 2011: 4753-4756

[22] David P, Jacque S. Security Arguments for Digital Signatures and Blind Signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396