



高保真的 可逆信息隐藏

► 欧博 赵耀 倪蓉蓉 著



北京交通大学出版社
<http://www.bjtu.cn>

高保真的可逆信息隐藏

欧 博 赵 耀 倪蓉蓉 著

北京交通大学出版社

• 北京 •

内 容 简 介

可逆信息隐藏技术能够将特定信息嵌入到载体中,并允许合法用户在提取该信息后无失真地恢复出原始载体,因而在军事、医学、司法等对图像内容敏感的领域受到了广泛关注。本书以高保真的可逆信息隐藏技术为主要研究内容,探讨在给定嵌入容量的情况下如何更有效地减小嵌入失真,提升图像视觉质量。

版权所有,侵权必究。

图书在版编目(CIP)数据

高保真的可逆信息隐藏 / 欧博, 赵耀, 倪蓉蓉著. —北京: 北京交通大学出版社, 2019.1

ISBN 978-7-5121-3782-0

I. ① 高… II. ① 欧… ② 赵… ③ 倪… III. ① 计算机图形学—研究 IV. ① TP391.411

中国版本图书馆 CIP 数据核字 (2018) 第 258022 号

高保真的可逆信息隐藏

GAOBAOZHEN DE KENI XINXI YINCANG

责任编辑: 陈建峰

出版发行: 北京交通大学出版社

地 址: 北京市海淀区高粱桥斜街 44 号 邮编: 100044

印 刷 者: 艺堂印刷(天津)有限公司

经 销: 全国新华书店

开 本: 140 mm×203 mm 印张: 5.6 字数: 161 千字

版 次: 2019 年 1 月第 1 版 2019 年 1 月第 1 次印刷

书 号: ISBN 978-7-5121-3782-0/TP·869

印 数: 1~600 册 定价: 36.00 元



本书如有质量问题, 请向北京交通大学出版社质监组反映。

投诉电话: 010-51686043, 51686008; E-mail: press@bjtu.edu.cn。

前 言

随着因特网和多媒体信息技术的发展,存储、修改和传播多媒体信息(文本、音频、图像、视频等)变得越来越容易。人们可以很容易地下载这些多媒体信息,并对其进行修改和发布。这不仅损害了版权所有者的合法权益,也会引发关乎国家安全、企业机密和个人隐私等的一系列信息安全问题。信息隐藏是一种隐蔽通信、版权保护和内容完整性认证的有效技术手段。近年来提出的可逆信息隐藏技术能够将特定信息嵌入到载体中,并允许合法用户在提取该信息后无失真地恢复出原始载体,因而在军事、医学、司法等对图像内容敏感的领域受到了广泛关注。

本书以高保真的可逆信息隐藏技术为主要研究内容,探讨在给定嵌入容量的情况下如何更有效地减小嵌入失真,提升图像视觉质量。本书取得的主要创新性研究成果包括以下几方面。

1. 提出了一种基于可自适应选择预测误差直方图的高容量可逆信息隐藏方法。该方法设计了两种预测器,通过参数调节得到不同的预测误差直方图。对比上层嵌入,自适应地

得到当前嵌入层的最优预测误差直方图，使得像素补偿的收益最大化。实验结果表明该方法在高嵌入率情况下的图像质量明显优于基于直方图移位的传统方法。

2. 提出了一种基于偏微分方程预测器的可逆信息隐藏方法。偏微分方程预测器能够根据图像的局部相关性迭代更新得到最优预测值。在每一次迭代中，该方法通过计算当前预测值在上下左右四个方向上的梯度，来自适应地分配权重，因而预测更准确。实验结果表明在同等嵌入率下该方法带来的失真更小。

3. 提出了一种基于非局部均值预测的可逆信息隐藏方法。通过全局地利用图像的自相似性来提升像素预测的准确性，不仅能在图像平滑区准确预测，也能在纹理区取得较好效果。实验结果表明，该方法对于自然图像尤其是纹理图像可取得更好的嵌入性能。

4. 提出了一种基于像素值排序的可逆信息隐藏方法。以像素块为基本嵌入单元，利用块内像素值的大小顺序在信息嵌入前后保持不变这一特性，将图像的嵌入划分了多个层级。通过容量划分和像素选择技术，根据容量自适应地在不同类型的像素块嵌入信息，得到最优的嵌入效果。实验结果表明该方法在小嵌入容量下对图像的改变更小。

5. 提出了一种基于二维预测误差直方图的可逆信息隐藏框架。利用预测误差间的相关性，将邻近的两个预测误差作为嵌入单元来设计一种二维的可逆嵌入方案，并给出了多

个新的、更有效的二维可逆映射，理论证明了该方法的优越性。实验结果表明该方法明显优于当前主流的可逆信息隐藏方法。

著 者

2018 年 10 月

缩 略 语

RDH	可逆信息隐藏 (reversible data hiding)
PEE	预测误差扩展 (prediction-error expansion)
HS	直方图移位 (histogram shifting)
MSE	均方误差 (mean square error)
PSNR	峰值信噪比 (peak signal to noise ratio)
PDE	偏微分方程 (partial differential equation)
NLM	非局部均值 (non-local mean)
LSB	最低有效位 (least significant bit)
bpp	位每像素 (bit per pixel)

目 录

1	绪论	1
1.1	研究背景和意义	1
1.2	可逆信息隐藏技术	3
1.2.1	可逆信息隐藏的研究现状	7
1.2.2	可逆信息隐藏的应用	16
1.3	本书的主要贡献和组织结构	20
2	基于可调节的预测误差直方图的可逆信息隐藏方法	25
2.1	引言	25
2.2	预测误差直方图可调的 RDH 算法	26
2.2.1	像素补偿	28
2.2.2	信息的可逆嵌入和提取	31
2.2.3	嵌入提取流程	32
2.3	实验结果	34
2.4	结论	42

3	基于偏微分方程预测器的可逆信息隐藏方法	43
3.1	引言	43
3.2	基于 PDE 预测器的可逆嵌入提取算法	44
3.2.1	PDE 预测器	45
3.2.2	溢出问题处理	50
3.2.3	嵌入流程	52
3.2.4	提取流程	54
3.3	实验结果	55
3.4	总结	65
4	基于非局部均值预测的可逆信息隐藏方法	66
4.1	引言	66
4.2	PEE 算法的基本原理	68
4.3	非局部均值预测	70
4.4	基于非局部均值预测的可逆方案	74
4.5	实验结果	80
4.6	总结	86
5	广义的利用像素值排序的可逆信息隐藏方法	87
5.1	引言	87
5.2	广义的 PVO 可逆嵌入算法	89
5.2.1	PVO 嵌入方法	89
5.2.2	PVO- k 嵌入算法	90
5.2.3	最优混合嵌入	94

5.3	自适应的混合 PVO- k 算法的实现	99
5.3.1	修改最大值和最小值像素的 PVO- k 嵌入的扩展 方法	99
5.3.2	混合嵌入的最优阈值选择	103
5.3.3	嵌入和提取流程	105
5.4	实验结果	107
5.5	结论	113
6	基于预测误差对扩展的可逆信息隐藏	114
6.1	引言	114
6.2	基于 pairwise PEE 的可逆信息隐藏框架	115
6.2.1	传统的预测误差扩展技术	115
6.2.2	二维预测误差直方图	118
6.2.3	pairwise PEE 技术	122
6.3	pairwise PEE 技术的实现	126
6.4	实验结果	131
6.5	结论	147
7	总结与展望	149
7.1	总结	149
7.2	展望	151
	参考文献	154

1 绪 论

1.1 研究背景和意义

因特网的普及和多媒体技术的发展,使得多媒体信息的应用达到了前所未有的广度和深度。人们不仅可以方便地通过网络下载和拷贝数字媒体信息,还能凭借功能强大的多媒体工具对原始数据内容加以修改,甚至以所有者的身份加以发布和进行网络贸易。然而,这些方便、容易的拷贝和修改也带来了一系列潜在的信息安全问题,如版权保护、信息完整性认证、真实性认证、未授权拷贝等。图 1.1 给出了数字媒体信息发布的基本模型。如图所示,供应商是版权所有者,他们希望通过网络发布数字媒体信息 X ,而信息接收者,即消费者,则希望通过网络接收到 X 。盗版者是非版权所有者,他们未经许可拷贝原有信息,然后重新以所有者的身份发送 X 或者修改部分信息后发送不可信版本(篡改信息) $\tilde{X}$ 。在这种情况下,消费者不可避免地会受到盗版拷贝的副本或者不可信版本的影响。这不仅损害了消费者权益,也极大地破坏了市场秩序,打击了合法供应商的积极性。实际上,信息安

全问题不仅仅是经济层面的问题，更关乎个人信息安全甚至国家安全。因此，对于信息安全的保护不仅仅需要立法上的支持，给予盗版者法律上的惩罚，更需要技术上提供一种有效的手段去增加盗版的难度，并检测和跟踪盗版源。

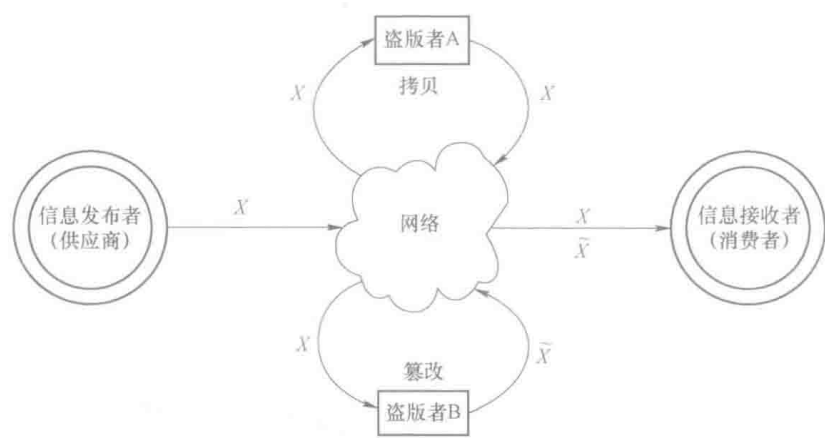


图 1.1 数字媒体信息发布的基本模型

为了从技术上解决信息安全问题，传统的方法是采用加密和数字签名等技术。但是这些技术对数字媒体内容的保护有一定的局限性。加密的信息变成无法理解的密文信息，使得信息无法通过公共网络让他人获得。同时，一旦信息被解密，就难以证明数据是否被非法拷贝和分发。而数字签名虽然能够为数据的传输提供有效的保护，但是往往需要往原始数据中加入大量签名，在实际应用中也并不方便，并且随着具有并行计算能力的破解技术的发展，数字签名的安全性已经受到质疑。为了弥补传统技术上的缺陷，研究者开始寻求一种新的技术来保护数字媒体信息，使得对原始数据解密后

依然能够对媒体内容提供保护, 实现其真实性和完整性认证。所谓信息隐藏, 是指利用数字媒体信息的冗余性, 把版权信息嵌入作品本身, 从而保护版权的一种隐蔽通信技术。信息隐藏将隐秘信息以检查者难以察觉的方式隐藏于公开的载体中, 然后通过公开的载体的传输来实现隐秘信息的传递。隐秘信息之所以能隐藏在多媒体数据中是因为载体信息本身存在很大的冗余性, 人眼对信息的变化存在掩蔽效应, 当合理控制嵌入的强度而不引起剧烈变化时, 嵌入信息便不易使人察觉, 也不会影响原始载体本身的传输和使用。到目前为止, 信息隐藏主要包含隐写、数字水印、数字指纹等几个分支。信息隐藏是近二十年来兴起的一个前沿研究领域, 它涉及网络技术、通信技术、计算机科学、密码技术、信息论等多种学科, 与信息安全、数据加密等均有密切的关系, 受到了国内外工业界和学术界的广泛关注, 特别是在网络技术及其应用迅速发展的今天, 信息隐藏的研究更具有现实意义。

1.2 可逆信息隐藏技术

可逆信息隐藏是近几年新兴的热点研究。相比于传统的信息隐藏技术, 可逆信息隐藏^[1-6] 允许人们在提取嵌入信息后无失真地恢复出原始内容, 在诸如军事、医学、法律等对图像内容敏感的领域, 有着重要应用价值。图 1.2 给出了可逆信息隐藏的系统模型。从图中可以看出, 在经过无损信道传

输后，当用户经过授权拿到相同密钥后即能从含密载体中无损地恢复出原始载体和隐秘信息。

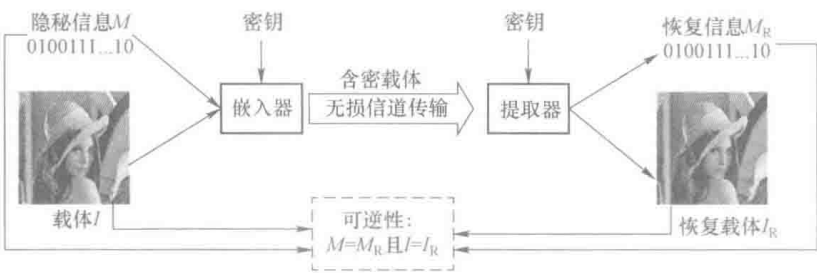


图 1.2 可逆信息隐藏的系统模型

需要指出的是，本书讨论的是以图像为载体的信息隐藏，其他载体如音频和视频的信息隐藏方法不在本书的讨论范围内。

严格来说，可逆信息隐藏是一种脆弱水印，即对于含密图像的任何修改都会影响信息的准确提取和恢复，因而它对传输环境有着特殊的要求。图 1.3 给出了可逆信息隐藏与传统鲁棒水印的嵌入提取的比较。

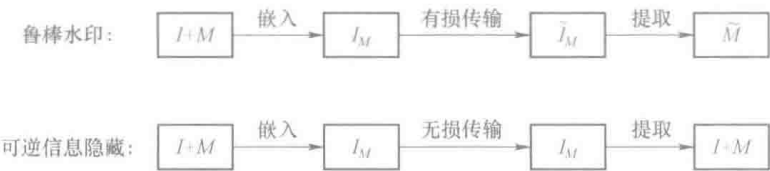


图 1.3 鲁棒水印和可逆信息隐藏的比较

图中 I 是原始图像， M 是需要嵌入的隐秘信息， I_M 是嵌入隐秘信息后的含密图像， $\tilde{I}_M$ 指经过有损信道传输后受损的含密图像。如图 1.3 所示，鲁棒水印的目的在于最大限度地从

受损载体中提取出隐秘信息 M ，更加强调水印信息的稳健性，要求算法能够抵抗一定程度的攻击，因而可以允许载体在有损信道中传输，在实际的版权保护和认证中应用广泛。不同于鲁棒水印，在可逆信息隐藏中，载体必须在无损信道中传输，在保证含密图像没有受到任何修改后，用户才能无损地恢复出原始图像 I 和嵌入的隐秘信息 M 。因此，鲁棒性一般不作为可逆信息隐藏算法（以下简称可逆算法）的考虑范畴。在评价一个可逆算法的性能时，通常考虑以下两个方面：

(1) 不可见性 (imperceptibility)：经过信息隐藏操作后，隐藏载体在视觉质量上没有明显的降质现象，嵌入信息无法被人察觉和分辨出来。对于可逆信息隐藏而言，目前学术界主要采用客观评价标准——峰值信噪比 (PSNR) 评判含密图像的视觉质量。对于大小为 $H \times W$ 的 8 位灰度图像而言，PSNR 的计算公式为

$$\text{PSNR} = 10 \cdot \lg \frac{255^2}{\text{MSE}} \quad (1.1)$$

其中 MSE 为均方误差，它计算对应像素在嵌入前后的差的平方，表示为

$$\text{MSE} = \frac{\sum_{i=1}^H \sum_{j=1}^W (p_{i,j} - p'_{i,j})^2}{H \times W} \quad (1.2)$$

其中， $p_{i,j}$ 和 $p'_{i,j}$ 分别为嵌入信息前后的像素值。PSNR 的单位为 dB，PSNR 值越高，表明嵌入信息后图像相比于原始图

像的失真越小，含密图像的视觉质量也就越好，也就越不容易被人察觉。一般来说，对于 PSNR 值在 30 dB 以上的含密图像，人眼是难以分辨它和原始图像的差别的。当然，在高保真的图像处理领域，PSNR 值会要求更高，比如 48 dB 以上。

(2) 嵌入容量(embedding capacity): 简称容量(capacity)，是指在载体中能够嵌入的隐秘信息的数量，单位为比特(bit)。对一幅图像而言，容量也用嵌入率（平均每个像素嵌入的比特数）来表示，单位为 bpp (bit per pixel)。嵌入率越大，所隐藏的信息也越多。例如，1.0 bpp 表示平均每个像素嵌入了 1 比特信息。

已有的可逆算法研究主要着眼于提升含密图像的不可见性和容量。然而，不可见性和容量二者之间是相互竞争和矛盾的。增强不可见性会减小图像的嵌入容量，而容量的提高则不可避免地要对原始图像作更多的修改，降低含密图像的视觉质量。如何达到二者的最佳折中，是可逆算法在嵌入性能上考虑的主要问题。具体而言，在相同嵌入容量下，能够得到更高 PSNR 值的可逆算法更优，或者在等量失真下(PSNR 值相等)，嵌入容量更大的可逆算法更佳。在实验中，研究者常用如图 1.4 所示的可逆信息隐藏的嵌入性能曲线 (PSNR/capacity) 来描绘可逆算法的嵌入性能。图中，算法 2 (Algorithm 2) 在较低嵌入率时要优于算法 1 (Algorithm 1)，因为嵌入同样容量时所得的 PSNR 值更高；而随着嵌入率的提高，算法 1 要明显优于算法 2。

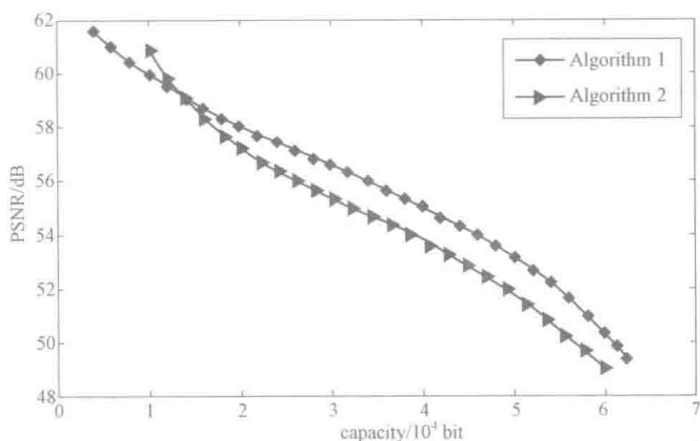


图 1.4 可逆信息隐藏的嵌入性能曲线

近年来,可逆信息隐藏也开始考虑其鲁棒性的研究,但是这里对鲁棒性的要求有所降低。即只考虑经过常规的图像操作后依然能够检测出隐秘信息的能力。这里,常规的图像操作包括 JPEG 压缩、空间滤波、打印扫描,以及旋转、缩放、平移等几何变形操作。当然,可逆信息隐藏对于鲁棒性的研究还处于起步阶段,目前的研究主要关注对于经过 JPEG 压缩后的隐秘信息的无损提取。这类研究能够在一定程度上实现隐秘信息的无损恢复(在高质量因子下有较大概率无损恢复隐秘信息,对于中低质量因子,基本无法实现可逆提取),但是原始信息的恢复依然无法实现。

1.2.1 可逆信息隐藏的研究现状

可逆信息隐藏的概念最早由美国 Honsinger 等人在 1999 年的美国专利中提出^[7]。这项专利提出了一个基于空域的可逆