

信息隐藏的层次安全性^{*}

郭艳卿¹, 何德全¹, 尤新刚^{1,2}, 孔祥维¹

(1. 大连理工大学信息安全研究中心, 辽宁 大连 116023;

2. 北京电子技术应用研究所, 北京 100091)

摘要: 近年来, 信息隐藏作为一门新兴学科得到了迅速的发展。但人们对信息隐藏的本质仍缺乏深刻的认识。以分析现有的信息隐藏性能评价方法为基础, 将信息隐藏与物理学进行类比, 提出信息隐藏的“层次性”概念, 并从层次性角度探讨了信息隐藏的安全性。

关键词: 层次性; 信息隐藏; 理论框架

中图分类号: TN918.91 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0105-04

信息隐藏 (information hiding) 是利用人类感觉器官的不敏感性 (感觉冗余), 以及多媒体数字信号本身存在的冗余 (数据特性冗余), 将秘密信息隐藏于一个宿主信号 (掩护体) 中而不被觉察。它对外表现的只是宿主信号的外部特征, 并不改变其基本特性及使用价值^[1]。数字图像的广泛应用为信息隐藏提供了极好的载体, 利用数字化图像信号相对于人类视觉的冗余, 可以进行各种时 (空) 域和变换域的信息隐藏, 从而实现一种“非加密”方式的隐蔽通信。

近年来, 信息隐藏技术方法研究得到了飞速发展, 涌现出很多高水平的信息隐藏及分析算法。与此同时, 很多学者正致力于图像信息隐藏理论框架的研究。如, Cachin^[2]、Mittelholzer^[3]、Zollner^[4]等试图将密码学中的信息论模型推广到信息隐藏技术中来; 林代茂通过对数字图像的熵和视觉冗余的定量分析阐述了熵和感觉冗余概念对信息隐藏技术的重要意义^[5]。然而, 这些理论研究仍然是零散的, 他们并没有准确地阐述图像信息隐藏的理论安全性^[6]。如, Cachin 基于自己的信息隐藏系统安全性定义得出: 如果一个信息隐藏系统嵌入一个秘密信息到载体中去的过程不改变原图像的概率分布, 则该系统是 (理论上) 绝对安全的。但他的安全性定义的前提是假设已知载体图像的统计信息, 而信息隐藏及分析常常是在样本很少情况下进行的, 在这种条件下, 很难抓住稳定的统计规律, 因此这个假设在实际中常常是无法满足的。即使已知某种图像的统计分布, 由于隐藏信息操作是在不可感知条件

下进行的微小变化, 这样, 由统计分布产生的误差很有可能远远大于嵌入秘密信息引入的误差, 统计分布所产生的如此大的误差使得统计分布对图像信息隐藏来说变得毫无意义^[7]。

本文以分析现有的信息隐藏性能评价方法为基础, 将信息隐藏与物理学进行类比, 寻求它们的共性, 并提出信息隐藏的“层次性”概念, 在分析了产生这种“层次性”的根本原因之后, 又从层次性角度探讨了信息隐藏的安全性。

1 图像信息隐藏性能评价方法

在对图像信息隐藏技术方法和理论框架研究不断深入的同时, 迫切需要对信息隐藏系统的性能评估和基准测试等进行研究, 以便指导信息隐藏及分析系统的建立^[7]。从公开的文献上看, 对于信息隐藏性能评价 (测试) 主要包括主观失真评价、对掩密后掩密图像质量 (不可感知性) 的客观评价, 以及针对通用分析算法的抗分析能力评价。

(1) 主观失真评价是图像信息隐藏性能评价方法的最初阶段。它包括两个步骤: 第一步, 将失真的数据集按照从最好到最坏的次序排序; 第二步, 挑选测试人员按照一定准则 (如 ITU—R Rec. 500), 描述所处理对象的级别和相应的可感知性以及质量, 对每个数据集进行评定, 已得出所处理对象针对原对象的不可感知性。这种评价方法的结果对最终的图像信息隐藏性能评价和测试是有实用价值的, 但由于它受观察者背景知识、观测环境等其他因素的限制和影响, 评价结果的一致性较差, 而且

* 收稿日期: 2004—09—11

基金项目: 国家“863”高技术研究发展计划资助项目 (2002AA054010); 国家自然科学基金资助项目 (60372083)

作者简介: 郭艳卿 (1980年生), 男, 博士生; E-mail: sagat823@yahoo.com.cn.

费时费力,不具有真正意义的实用性。

(2) 从本质上说,对掩密后掩密图像质量(不可感知性)的客观评价是对主观失真评价的客观化。在信息隐藏方法的视觉失真度度量中,许多学者将图像嵌入隐藏信息前后的峰值信噪比(PSNR)作为信息隐藏技术中感知性评价的一个重要的甚至唯一的客观评价指标。但由于峰值信噪比是对整幅图像数据变化情况的平均统计,因此只能反映图像在信息隐藏前后的总体统计差别,并不能完整客观地表达人类的视觉特性(如不能表达局部视觉感受严重破坏所引起的信息隐藏性能的差别)^[8]。张婷等^[9]提出的分块峰值信噪比(BPSNR)虽然在一定程度上能较好地衡量图像信息隐藏所造成的感知性能和数据特性的改变,但这种评价方法的本质(基于峰值信噪比)仍未改变,因而,不能从根本上解决如何定量客观评价掩密后掩密图像视觉变化这一问题。

(3) 针对通用分析算法的抗分析能力评价方法是评价信息隐藏技术优劣的主要手段,它选用公认具有较好分析能力的分析算法来评价一种隐藏算法的性能。如一种空域掩密算法抵抗RS方法分析的能力,抵抗小波方法分析的能力等。由于上述分析算法具有很强的代表性,它们从时(空)域及变换域的统计特征变化等多方面因素评价“安全性”,因此能较全面地反映隐藏算法的性能。

上述几类评价方法是按照信息隐藏不同发展阶段的目标划分的:最初,图像信息隐藏的目的是在嵌入秘密信息后人眼无法察觉到掩密图像与原图像的区别;而后,又希望能通过算法定量计算掩密图像与原图像的差别大小;目前,绝大多数的隐藏算法都能保证掩密的视觉“不可见性”,于是人们对隐藏算法的性能又有了更高的要求,进而定义了各种信息隐藏的理论安全性^[2-3]。表面上看,很多问题都已经或正在得到解决,但事实上,又出现了更多的疑问:视觉不可见性与现有的很多统计意义上的“安全性”有着怎样的关系?在图像信息隐藏的博弈过程中,基于统计特性的安全性定义是否存在合理性?什么是真正意义上的安全性定义?

总体来说,虽然人们在信息隐藏的理论框架研究方面已取得了卓越的成就,然而我们却不能满足于现有的理解,还必须进一步去寻求更合理、更科学和更有实际意义的理论框架,以便更好地研究和解决现实世界已经提出的诸多新问题。

2 跨越不同层次的图像信息隐藏

从视觉“不可见”到统计“不可见”是人们对

图像信息隐藏最直观的认识。在这里我们试图沿着另一种分析思路来思考图像信息隐藏问题,希望这种对图像信息隐藏不同角度的分析能够使我们对其本质有更深入的理解。

我们可以用热力学理论和图像信息隐藏之间的类比作进一步解释:考虑密闭容器内的气体,为简单起见,我们仅将气体分子的速度作为描述气体微观层次上的唯一变量,密闭容器的外部环境确定了内部气体分子唯一的的状态空间(分子速度所可能取到的值)。如果我们把图像中的一个像素的像素值看成是一个微观变量,将图像获取、量化、保存等所有操作定义为“图像的环境”,那么此“环境”同样确定了图像的微观变量(如同气体分子一样)的状态空间(这个状态空间是图像格式可容空间的子空间,例如,灰度图像的格式容许每个像素都可以取0~255的整数值,但这显然容许了很多无意义的“噪声”图像的存在,而前述定义的状态空间的确定是有“图像获取”这一条件限制的,所以在这个状态空间中不存在无意义的“噪声”图像)。

我们可以看到所描述的图像信息隐藏与热力学系统的相似之处:

(1) 层次性

从某种意义上讲,我们的掩密算法仅局限在微观层次上(如同为具体的某个气体分子在状态空间中选择一个代表秘密信息的速度),掩密算法的最基本要求是将图像的宏观变量——图像视觉质量限制在原值附近一个很小的邻域内变化(相当于保持气体的某一宏观变量基本保持不变,如温度或压强基本保持不变)。迄今为止,掩密算法仍未完全脱离微观层次,而分析掩密图像时所提取的特征量是跨越不同层次的,不仅包含在有原始图像情况下的宏观变量——“图像视觉质量”,还包含空域及各变换域中的各阶统计量等(相当于提取气体变量中的宏观温度或压强,还提取了气体分子速度分布的各阶统计量等)。

(2) 跨越不同层次的复杂性

图像信息隐藏的层次性产生的根本原因是数字图像的层次性。图像中的一些问题并不像看似的那么简单,比如我们很容易判断一块 $M \times N$ 的像素区域表示的视觉含义,但要让计算机(即我们的算法)从这 $M \times N$ 个数据中辨别此区域表示的视觉含义是相当困难的,这个问题的难度在于它要求我们的算法必须从微观(像素数据)层次跨越到宏观(视觉)层次,从微观(像素数据)层次去描述大量微观变量(像素级数据)涌现出来的宏观视觉特性。

同样, 热力学系统理想气体中所含分子数在 10^{23} 数量级, 讨论理想气体单个分子的状态用动能(e)、动量(p) 等来描述; 而在整体层次上, 我们选择温度(T)、体积(V) 等物理量来描述系统的状态。整体层次物理量与分子层次物理量完全不同, 而且不能用简单的叠加原理来建立它们之间的联系。温度、体积这些物理量是系统整体涌现出来的量。

综上所述, 层次性是图像信息隐藏的一个基本属性, 正确认识图像信息隐藏的不同层次及层次之间的关系是建立理论框架的关键所在。

3 不同层次的安全性研究

跨层次的解释需要一个理论框架, 在这个框架中, 一个组织层次上系统的行为、较低层次上组分的行为, 以及两层次间的关系都要得到解释。这就是欧阳莹之^[10] 提出的综合微观分析的框架, 这个框架可以联系系统的描述层次和组分的描述层次, 但它没有抛弃系统概念, 而是在解释组合作用时把系统概念纳入到组分概念中, 从而允许有多种视角。

物理学中, 人们建立了微观层次的分子动力学、宏观层次的热力学, 并且在这两个层次之间建立了统计力学以揭示它们之间的联系, 所有这些工作作为物理学提供了近乎完善的理论框架。类比来看, 图像信息隐藏同样需要先在不同层次建立比较完善的理论, 进而建立各个层次之间的联系, 最终揭示图像信息隐藏的本质。

我们可以借鉴这个思路, 在建立图像信息隐藏整体理论框架之前, 从不同层次入手, 建立不同层次下的图像信息隐藏安全性定义, 展开不同层次下的工作。在对图像信息隐藏不同层次有比较透彻的研究之后或有阶段性研究成果的同时, 再对层次之间的联系进行深入探索。

掩密前后视觉质量的变化可以作为宏观层次的研究对象之一, 视觉不能分辨的情况(在视觉门限以下的问题) 属于另一层次的问题, 这些问题我们不能指望在宏观这一层次得到完美的解决。

在像素级的微观层次上可以进行局部特性的研究, 如在设计算法时考虑改变量所造成的空域影响、F5 方法引入的矩阵编码等问题的研究, 以及某些图像格式和压缩方法对图像中局部像素的状态空间的影响问题(如 Jpeg 图像的块不连续性问题) 的研究, 都应该属于这一微观层次的研究范围。

值得注意的是, 在微观层次与宏观层次之间的联系尚未清楚之前, 不应该盲目地跨越层次进行分析, 这样做只能使问题复杂化。比如, 目前我们设

计掩密算法的准则通常是以微观层次上最小改动为目标的(如 LSB 方法是以空域的最小改动为目的), 而评价这些掩密算法的时候, 我们通常又跨越到了宏观层次, 我们试图用宏观上的视觉质量变化来评价它们。这好像是在改动了一团气体部分分子的速度(改变量很小), 然后问这种改变对气体的压强或温度造成了怎样的影响呢? 虽然我们不知道气体温度与气体分子的平均动能之间的关系(分子的动能与其速度的平方成正比), 但“平均动能”这一概念显然不是一个微观概念。

图像的统计模型及图像的某些统计量分析可以作为介于宏观与微观之间层次的研究领域。这与物理学中“统计物理学”的出现是极其相似的。这个中间层次的完备理论的建立是相当困难的。统计学面临着类似的问题^[19]。

4 结论与展望

图像信息隐藏的层次性与很多学科发展过程中面临的层次性极其相似, 但图像信息隐藏有其自身的特点: 它的层次性不像其他学科中的层次性那样清晰。在物理学中, 我们可以很清楚地划分微观层次的分子动力学、宏观层次的热力学和联系这两个层次的统计力学, 但在信息隐藏中我们很难看清楚这个层次: 当我们对图像的改变量极小时, 可以把它界定为微观层次, 可随着改变量(嵌入量) 的增加, 它连续地完成了从量变到质变、从微观到宏观的飞跃, 我们却很难界定何种程度以下属于微观层次、何种程度以上属于宏观层次、那些状态属于中间层次。图像信息隐藏的这一连续层次跨越特性是这一领域研究困难的本质所在。

参考文献:

- [1] 尤新刚, 周琳娜, 郭云彪. 信息隐藏学科的主要分支及术语 // 信息隐藏全国学术研讨会 (CIHW2000/2001) 论文集[C]. 西安: 西安电子科技大学出版社, 2001.
- [2] CACHIN C. An information-theoretic model for steganography [C]. Information Hiding: Second International Workshop, vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, U. S. A. Berlin: Springer-Verlag, 1998.
- [3] MITTERLHOIZER T. An information-theoretic approach to steganography and watermarking [C]. Fitzmann A ed. Information hiding: 3rd International workshop. Berlin: Springer-Verlag, 2000, 1768.
- [4] ZOLLNER J, FEEDERRATH H, KLIMANT H, et al. Modeling the security of steganographic systems [C]. Information Hiding: Second International Workshop, USA, Berlin: Springer-Verlag, 1998, 1525.
- [5] 林代茂. 图像的信息熵分析 // 信息隐藏全国学术研

会(CIHW2000/2001)论文集[C] . 西安: 西安电子科技大学出版社, 2001.

[6] MOSKOWITZ I S, LONGDON G E, CHANG L W. A new paradigm hidden in steganography[J] . Proceedings of New Security Paradigms Workshop, Bally cotton, Co. Cork, Ireland. 2000.

[7] 孔祥维. 信息安全中的信息隐藏理论和方法研究[D] . 大连: 大连理工大学, 2003.

[8] 尤新刚, 郭云彪, 周 琳娜. 峰值信噪比不宜用来评价信

息隐藏技术 // 信息隐藏全国学术研讨会 (CIHW2000 / 2001) 论文集[C] . 西安: 西安电子科技大学出版社, 2001.

[9] 张婷, 尤新刚, 孔 祥维. 基于像素块误差分布的信息隐藏性能测试 // 信息隐藏全国学术研讨会(CIHW2002) 论文集[C] . 北京: 电子工业出版社, 2002.

[10] 欧阳莹之. 复杂系统理论基础[M] . 田宝国, 周亚, 等译. 上海: 上海科技教育出版社, 2002.

Different Level Security of Information Hiding

GUO Yan qing¹, HE De quan¹, YOU Xin gang^{1, 2}, KONG Xiang wei¹

(1. Information Security Research Center of Dalian University of Technology, Dalian, 116023, China;
2. Beijing Institute of Electronic Technology and Application, Beijing, 100091, China)

Abstract: As a latest subject, Information Hiding has received a rapid development in recent years. But the essence of Information Hiding is still obscure. In this paper, we make an analysis of different methods for evaluating the performance of Information Hiding. Then, after finding the analogy between physics and Information Hiding, we introduce the concept level property of Information Hiding and discuss the security of Information Hiding in terms of level property .

Key words: level property; Information Hiding; theoretical framework