数据冗余空间中的掩密术安全性*

宋 辉[1], 孔祥维[1], 尤新刚[1,2], 胡 岚[2]
(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: 分析了目前掩密术的研究的理论和掩密术安全性评估理论, 指出了目前掩密术研究框架的部分局限性和现有掩密术安全性理论的不足。在视觉冗余的基础上提出了基于数据冗余性的掩密术定义和掩密术安全评估准则。

关键词: 掩密术安全性; 数据冗余性; 掩密术安全评估
中图分类号: TP391 文献标识码: A 文章编号: 0529-6579 (2004) S2-0087-04

信息隐藏技术自 20 世纪 90 年代中期公开以来, 已备受有关专家和机构的重视。早期人们主要尝试各种信息隐藏的方法研究, 目前信息隐藏的研究正在建立符合信息隐藏自身特点的理论框架。信息隐藏从发展初期到现在, 并没有建立符合自身特点的理论基础, 在理论框架上主要借用了其他学科的思想和基础理论, 如通信科学、图像处理、检测与估值、密码学等。

作为信息隐藏在隐蔽通信应用的掩密术, 同样也存在着理论的构建问题。掩密术的研究包括掩密技术和掩密分析技术这两个相互对抗的分支, 目前这两个分支的理论研究基础主要可归类为信息论模型[1]、通信模型[2]、博弈论[3]模型和噪声模型。信息论模型试图用信息论的相关原理来量化统计上的差异, 从而鉴别掩密算法安全性; 通信模型的视点聚焦于秘密的信道选择、信道利用、信道容量的大小和掩密术嵌入容量的问题; 博弈论模型的分析侧重于掩密同掩密分析的对抗; 噪声模型则是将噪声的数学模型按照其统计分布的规律叠加到载体上。总体来说这些模型的基础都是统计学, 主要围绕着载体和载密体的统计分布进行的, 进而更一般地认为掩密术的研究是围绕载体的统计特征进行的, 因此载体的统计特征的研究对掩密术的发展起到了很大的推动作用[4]。

但是统计学的一些先天不足, 使掩密术的研究有可能陷入某种误区。这是由于统计性命题与概率性命题呈现的矛盾性, 使现有的掩密分析方法的科学性受到挑战, 即整个观测空间与单个观测样本的矛盾。其一, 统计学描述的是观察空间整体的概率分布, 然而对单个样本来说, 这一概率分布的描述是没有意义的。如对一个确定的图像样本, 讨论它的像素分布应该是一个概率性命题, 而概率性命题本身的特性为篡改留下了空间。但当我们试图用多样本来联合检验时, 这样又回到统计命题的范畴, 但掩密通信的秘密性否定了对手或分析方得到多样本的可能性, 这样根本上否定了联合检测的可行性。这是因为秘密通信双方会使秘密通信的存在次数尽量可能的少, 而搭线检测者仅能实现对整体样本的抽样分析。其二, "系统的一些详细信息会由于统计描述而丢失"[5], 即统计描述不能体现个体术正是利用不同个体样本的多样性, 在保持统计学意义不变性的基础上对个性化信息进行目的性篡改以达到表达密信的目的。例如, 一个图像集合的各图像元素是经过一个固定扫描设备对一幅原始图像分别进行扫描得到的, 虽然它们的视觉效果相同, 但是这个图像集合的所有样本的像素值在空间上的分布不可能完全相同, 而统计意义上表述是无法全部表示出这种差异。

早期的囚犯模型适用于秘密通信的过程描述, 为早期的掩密术研究规定了一个较为宽泛的框架。但就目前掩密术的发展来看, 这一框架的某些约束条件需要重新进行考虑。例如, 囚犯模型的通信双方是囚徒这一假设有过强的约束性, 在实际中秘密通信双方会将本人的信息白化, 淹没在整个通讯群体中, 所以 "一定存在秘密通信" 的假设不成立。主动看守与被动看守的假设变得适用性很小, 在通信双方背景白化的前提下, 搭线窃听的监视者 (也就是被动看守) 的存在是普遍的, 也是盲目的; 但

* 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: 宋辉 (1980 年生), 男, 研究生; E-mail: song8008@student.dlut.edu.cn

是主动看守的存在应该重新考虑，因为如果主动看守是普遍存在的，通讯内容全部被替换或篡改，则掩密术的存在价值就必须重新考虑。本文根据图像视觉冗余，提出数字图像普遍具有的数据冗余性，定义了冗余空间的掩密术概念，并试图摆脱以前各种模型的局限性，构建一个更为普遍的掩密术研究框架，进而探索掩密术安全性的研究和评估。

1 图像视觉冗余与数字图像的数据冗余性

图像视觉冗余[6]：是人视觉观察的受限性和人脑处理的受限性（也可称为心理冗余）。视觉观察的局限性体现在肉眼的生理结构限制，如由于肉眼的生理特征（锥细胞与柱细胞的数量及位置的分布特征及锥细胞和柱细胞自身的生理构造特性）决定了视场中心的高采样和高处理能力和中心外围的低采样和低处理能力，这一生理现象简称为视场的中心化效应；人脑处理能力的受限性表现在对简单背景的信息搜索、对复杂环境的信息屏蔽以及动态信息的视觉吸引（可以称为主角效应——即对心理对主观敏感信息的加权）等。由于以上原因产生了图像视觉冗余，使的人们仅能感知图像在感知阈值之上的内容，而难以察觉图像在感知阈值之下的变化。

若将人的感知信息量定义为视觉信息量，将图像区域的纹理及色彩复杂程度定义为图像区域信息量。由人的感知特性而知，视觉信息量并不与图像区域信息量呈线性的关系，本文粗略地将它们之间的定性关系用曲线（图 1）来表示：

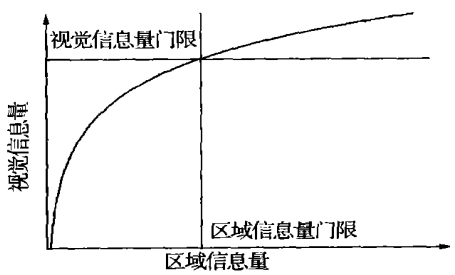

图 1 区域信息量与视觉信息量定性关系曲线

Fig. 1 The qualitative relation curve between image information and view information

通过这一关系，将视觉感知与图像表示结合起来。而视觉冗余便体现在区域信息量门限以上的区域信息量的变化由于视觉信息量的上限效应而变得不易被感知。若用 I_{view} 表示视觉感知信息量的大小，用 I_{image} 表示区域信息量的大小，用 $I_{view} = V(I_{image})$ 这一函数描述视觉信息量与区域信息量的关系。则在区域信息量的递增方向上有：$V' \geqslant 0$ 及 $V'' \leqslant 0$。这一关系在视觉上的表现在视觉信息量随着区域信息量的增加而增加，在超过区域信息量门限的区域信息量的增加与其引起的视觉信息量的增加是非线性的，视觉信息量会随着区域信息量的增加而趋于饱和，即视觉不能完全感知区域的信息量的全部信息。这一性质是图像掩密学的视觉上可行的根本原因。同时由于视觉冗余的存在使有损压缩技术变得可行，即保持视觉信息量不变的情况下去掉视觉冗余。

随着图像有压缩技术逐步完善，压缩后的数字图像的视觉冗余被去除了大部分，由于冗余空间的缩小甚至消失，掩密的空间变得更加困难乃至不可能实现。但是损失了的视觉冗余，使原始信息本身变成了一个未知的空间集合，有可能损坏图像中的非冗余部分，这样判断一个数字图像是否是原始图像的正常表示就变得更加困难，秘密通信者只要选出一个最接近正常图像的掩密信息来实现秘密通信。这与文献 [7] 中提到的压缩不同，该文中的压缩聚焦于数据量的压缩，即去除数据之间的冗余，而非视觉冗余。

对于数字图像来说，在采集和压缩过程中引入由于不同阶段和不同目的的量化引入量化误差，这样导致了观测者对于样本的先验知识的缺乏，使原始信息具有本质上的未知性。这时原始样本的数字表示实际上是唯一的，即它的数字表示允许一定程度上的变化，这种数字图像本质上的特性是图像本身和图像格式所允许的，本文将数字图像的这种可变化的特性定义为数字图像的数据“数据冗余性”——即视觉感知和图像格式引起的噪声的特征性分布，这一性质是在图像视觉冗余下派生出来的，是图像视觉冗余在数字图像上的表现形式。将某一样本数据冗余性的程度定义为这个样本的“冗余度”。

当然，目前的有损压缩技术并不能完全不损失视觉信息量，当损失视觉信息量的时候，其数据冗余性就不包含在视觉冗余中了，但是我们认为这种损失是不正常的，是一种不正常的、奇异的表现。故将格式允许但是不属于视觉冗余的可变性不归类为数据冗余性。

根据对数字图像的观测空间的数据冗余性可以分为：采样数据冗余性（permissibility sampled redundancies，简记为 P_S），压缩数据冗余性（permissibility compression redundancies，简记为 P_C）。同样，样本可以有相对应的定义：采样冗余度 D_{P_S}，压缩冗余度 D_{P_C}。采样数据冗余性定义是针

对数字图像的采样量化数据空间；压缩数据冗余性是针对不同压缩格式的有损压缩数据空间。

采样数据冗余性：其本质是媒体采集过程中的量化误差使得确定的媒体信息在空间表示上隐含着微观的随机性，先前针对图像空域 LSB 进行改变的掩密算法的理论基础就在于此。但是应该注意到，对于确知的媒体采集系统，其量化误差不是完全不可测的，其局部的量化误差的与该区域的图像的纹理复杂程度、局部梯度等可观测量是相关的。所以非压缩媒体是可以进行掩密操作的，但是这一掩密过程必需考虑载体本身的数据冗余性和载体局部的冗余度等因素相关。

压缩数据冗余性：即是在视觉允许条件下由有损压缩带来的数字图像数据冗余性，这一空间的存储形式在受到压缩准则的影响较大。所以压缩准则对这一空间的存在形式起到了决定性的作用。不同的压缩准则，其压缩数据冗余性是不同的，不同的有损压缩数字图像格式有不同的数据冗余性，所以对这一空间的分析显得尤为重要。

图像视觉冗余（image redundancies in view）是定义在肉眼感觉这个观测空间下，其量化表示为图像冗余度（degree of image redundancies in view，简记为 D_R）；按照图像掩密术的一般要求有：

$$D_R \geqslant D_{P_C} \tag{1}$$

$$D_{P_C} \geqslant D_{P_Q} \tag{2}$$

其中对于某一样本当且仅当该样本被压缩时，(1) 式取等号，因此 (1) 式可以理解为图像可压缩的原因；(2) 式当且仅当样本为无损存储时取等号，(2) 式应该理解为压缩使允许冗余空间变化。

2　数据冗余空间上的掩密术概念

掩密术的定义大都在数字图像的感知性质和密码通信的模型的基础上衍生的，以统计为数学工具和先验知识。掩密术的目的是进行秘密通信，对手不能发现通信的存在，因此安全性是掩密术最重要的性质。

在 Christain Cachin 的信息论模型[1] 中的安全性是以信息论为基础，这就要求对载体信息 C 的先验知识已知[8]，这一约束条件在实际应用中很难实现。即使已知 C 的概率分布，跟据概率论和统计学的一般理解，对于单个待检样本的判决是一个概率性命题，即作为样本在集合的统计先验知识确定的情况下也具有可变性。根据上文，载体集合 C 作为一个系统，它的一些信息会因为统计描述而丢失，即视觉条件下的一致的样本集合的元素在个体表现上是多样的，并且这个集合不只有一个符合统计规律。这样概率性判决在掩密术研究中是否有价值必须做研究。

同时，Christain Cachin 的信息论模型[1] 是以假设检验为前提，由 Neyman-Pearson 算法得鉴别函数到最优的解。在这一推导过程中需要已知 C 和 S 的存在先验概率，但是在实际运用中由于通讯群体的背景信息白化，检测方是无法得到这一条件的，并且错误判决并不是像该文中提到的无代价的，因为判决失误导致的错误决策会暴露搭线检测者的存在，并且干扰了正常通信活动进行。

在文献 [8] 中，作者将自己陷入了矛盾之中，即含密样本 s 是否属于载体集合 C。该文作者在没有讨论检测空间的情况下便假设 $s \in C$，一般认为属于载体集合的 s 是安全的。在 s 具有绝对安全性的前提下讨论它的安全性，就失去了理论基础。

部分相关文献[2,8] 在探讨掩密术的安全性时，往往陷入讨论密信 M 的安全性或者水印抵抗联合攻击的强度这类的误区中，这对于掩密术的研究是没有意义的。掩密术的意义在于最大可能的隐藏秘密通信的存在性。如果密信的存在性被很好的（乃至绝对的）隐藏，那么在这个基础上讨论 M 的安全性是没有意义的。

本文认为：通常意义下的掩密术是数据冗余空间内进行表达秘密信息来进行通信。这一过程的本质是由于冗余空间的存在，使样本信息对于接收者和检测者具有可变性，即在样本的宏观表现不变的前提下还存在微观变化。这一微观变化不能被统计学所描述，样本信息的可变性可以称为样本所具有的熵[9]，它与最大熵原理中的熵的含义相类似，也是对于系统不可测部分的不确定性的一种度量。“合法”噪声的存在，使量化空间（包括采样量化和压缩量化）上的变化成为一种被普遍采用的掩密术。基于以上对数字图像的分析，本文对掩密科学赋予一系列新的定义。

定义 1　数字图像掩密术是在数字图像的某个数据冗余性空间或某几个数据冗余性的联合空间中进行掩密编码调制，以达到用图像的宏观表示（如像素值，DCT 系数值）来表达秘密信息的目的。

定义 1 中所提到的掩密编码调制的目的是利用数据空间的可变性，在此空间上进行变化以实现秘密信息的表述。之所以要在某个数据冗余空间或者某几个数据冗余性的联合空间进行编码调制，是因为只有在相应的数据冗余性空间内改变才能实现在该观测空间的不可察觉，即隐藏秘密通信的存在性。也就是，掩密术的定义必须以掩密术的安全性

来描述。按照这一思路来定义某一掩密术的安全性。

定义 2 如在某一个检测空间上掩密术的掩密编码调制所引起的编码噪声强度不大于该检测空间的数据冗余度, 那么该掩密术在该检测空间下是不可见的, 具有该检测空间上的安全性。

从定义 2 来看, 掩密术或掩密系统的安全性是相对检测空间而言的, 而不是绝对的安全性, 当且仅当该掩密术或该掩密系统具有全部检测空间的安全性时, 该掩密术或该掩密系统才具有全部检测空间上的安全性。进而我们可以将安全性细化为某一观测空间下的: 视觉安全性、空域安全性、DCT 域安全性、小波域安全性或 1 阶统计量安全性、2 阶统计量安全性, 乃至某某变换域下的阶统计量和特征量的安全性等等。

针对定义 1 和定义 2 所规定的前提条件, 将掩密分析术进行一个全新的定义和解释。这样的掩密术和掩密安全性的定义更加有针对性, 避免了目前掩密术安全性的研究所存在的一些问题。

定义 3 掩密分析即是对待检样本在观察空间上, 对超过数据冗余性的奇异值进行检测并判别。

这一掩密分析定义对掩密通信方和掩密分析方都是公平的, 使掩密术和掩密分析都聚焦于数据冗余性这同一空间, 不存在假设性的限制, 并且由于数字图像的采集、编码与压缩技术都是公开的, 保证了这一系列定义与 Kerckhoffs 准则不相抵触, 并且针对性的研究也是完全可行的。下文将通过以上定义来分析影响掩密术和掩密系统安全性的部分重要因素。

3 总结与展望

本文针对目前掩密术研究存在的部分问题, 提出了数据冗余性这一概念, 并指出数据冗余性是掩密术存在的基础, 以及对数据冗余性的研究是掩密术的发展的动力。

下一步的工作应该围绕数据冗余性——这一掩密术核心课题进行更深入的研究, 这包括视觉信息量同图像区域信息量之间的量化模型的建立、无损数字图像数据冗余性研究及量化、各种有损数字图像格式的数据冗余性研究及量化和各空间联合数据冗余性的考虑等相关问题。

参考文献:

[1] CACHIN C. An information-theoretic model for steganography // Information Hiding: Second International Workshop, vol. 1525 of Lecture Notes in Computer Science[C]. Portland, Oregeon, Berlin: Springer-Verlag, 1998: 306—318.

[2] COX I J, MILLER M L, McKELLIPS A L. Watermarking as communication with side information[J]. Proceeding IEEE, 1999, 87(7): 1127—1141.

[3] ETTINGER J. Steganlysis and game equilibria[C]. Lecture Notes in Computer Science, 1998: 1525.

[4] 尤新刚, 郭云彪, 周琳娜. 信息隐藏对图像空域数据特性的影响 // 全国第二届信息隐藏学术研讨会论文集[C]. 2000: 208—214.

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

[6] 尤新刚, 周琳娜, 郭云彪. 信息隐藏学科的主要分支及术语 // 全国第三届信息隐藏学术研讨会论文集[C]. 2001: 43—50.

[7] ANDERSON R J, PETITCOLAS F A P. On the limits of steganography[J]. IEEE Selected Areas Communications, 16(4): 19.

[8] KAZENBEISSER S, PETITCOLAS F A P. Defining security in steganographic systems[C]. Proc SPIE, 2000: 4675.

[9] 林代茂. 图像的信息熵分析 // 全国第二届信息隐藏学术研讨会论文集(CIHW2000)[C]. 2000: 205—207.

Security of Steganography Based on Space of Redundancy Data

SONG Hui[1], *KONG Xiang wei*[1], *YOU Xin gang*[1,2], *HU Lan*[2]

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

Abstract: After analyzing the actual steganographic theoretics and the theoretics of evaluation of steganographic security, some localization in steganographic framework and theoretics of steganographic security are found out. Besides visual redundancies, defines of the stegangraphy and evaluation of steganographic security base on data redundancies were given out.

Key words: security; data redundancies; evaluation of steganographic security