信息隐写与隐写分析研究框架探讨

钮心忻, 杨义先
(北京邮电大学信息安全中心, 北京 100876; 北京邮电大学网络与交换技术国家重点实验室, 北京 100876)

摘 要: 文章分析了广义信息隐藏研究中存在的问题, 提出引入全信息理论和模糊信息处理的思想进行研究. 对信息空间从三个层面上进行了分类, 将隐写和隐写分析问题放在信息空间中进行研究, 建立了隐写分析研究框架.

关键词: 信息隐写; 隐写分析; 全信息理论; 模糊信息处理
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2006) 12A-2421-04

Study on the Frame of Information Steganography and Steganalysis

NIU Xin-xin, YANG Yi-xian
(*Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;*
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: The main problems in the field of information steganography are indicated. In order to solve these problems, the ideas of comprehensive information theory and the methods of fuzzy information processing are introduced. Upon these, the information space is proposed and classified in three aspects. In the information space, the research of steganography and steganalysis can be done accordingly. The framework of steganalysis is then proposed.

Key words: steganography; steganalysis; comprehensive information theory; fuzzy information processing

1 引言

信息隐藏与数字水印方面的研究已经发展了十多年, 到目前为止, 一直存在两个并行发展的应用分支, 一个是用于隐蔽通信的"信息隐藏"(或称"信息隐写"), 另一个是用于版权保护的"数字水印", 这两方面的研究应用环境不同, 导致研究的侧重点和要求不同, 但是它们有一个共同的特点, 都是将一些数据嵌入到载体数据中去, 同时不对载体数据产生较明显的破坏. 因此"信息隐写"与"数字水印"的核心是一致的, 我们统称为"广义信息隐藏".

本文针对广义信息隐藏的研究历程进行了简要的回顾, 指出了目前研究中存在的一些问题, 在信息隐写与隐写分析方面提出了一些新的想法.

2 广义信息隐藏研究的简要回顾

从信息隐藏领域十多年来研究重点的发展变化情况看, 它经历了一个由浅入深、由应用推动理论的发展过程. 从二十世纪90年代中期最早的LSB(最低比特位)隐藏方法, 逐步发展为包括各种变换域调制技术在内的多种隐藏方法, 同时更加强调盲检测和算法的鲁棒性. 隐藏信息的载体也从最早期的图像, 扩展到音频、文本、视频等各种类型的数据, 信息隐藏空间也从空间、时间域, 扩展到DCT域、小波域、DFT域、以及信号复数倒频谱域等等. 在各种算法不断涌现的同时, 人们注意到有很多基础性的问题制约了算法的深入发展, 例如信息隐藏的模型问题、容量问题、透明度问题、对载体的影响问题等等, 很多问题没有一个有效的测度. 换句话说, 人们注意到信息隐藏研究缺乏象通信系统中仙农信息论这样坚实的理论基础.

从2000年开始, 研究者开始关注信息隐藏的模型, 以及信息隐藏的容量等问题. 此后, 掀起了理论研究的热潮. 信息隐藏模型及容量研究影响比较大及有代表性的是Moulin等人提出的基于信息论的信息隐藏理论框架[1], 将信息隐藏过程抽象化, 认为隐藏过程相当于隐蔽信息的通信过程, 用通信模型表示信息隐藏, 隐蔽信息作为通信输入, 隐蔽载体作为信道, 攻击行为也描述为信道, 隐蔽密钥和隐蔽载体(如果必要)作为通信的边信息存在; 信息检测则认为是一种假设检验模型. 还有其他一些模型, 例如Costa dirty paper模型[2]、Cohen与Lapidoth模型[3]、Somekh-Baruck模型[4]、并行高斯信道模型[5]等. 这些模型的共同点都是把信息隐藏类比于一个通信模型, 其差别在于对攻击行为及信道的描述或假设不同. 信息隐藏的容量被认为是上述通信模型下最大可靠传输率.

3 存在的问题

尽管在信息隐藏的理论方面提出了各种模型, 也根据各

收稿日期: 2006-10-27; 修回日期: 2006-12-11
基金项目: 国家自然科学基金(No. 60473016, No. 90604022)

种模型提出了隐藏容量的计算公式,但是这些理论结果始终无法指导算法的设计,或者说现在还无法充分验证理论模型的准确性,以及为达到隐藏容量的上界该如何设计隐藏算法.换句话说,理论研究结果与具体载体、具体算法设计之间存在比较大的鸿沟.我们提出以下问题:

3.1 基于信息论的通信模型是否能最准确地描述信息隐藏问题?

首先来比较一下信息隐藏问题和通信问题.信息隐藏(隐写)是设法在多媒体信息中嵌入一些额外信息,嵌入的信息应该不影响载体的使用,甚至不能产生"载体携带了秘密信息"的怀疑,一旦载体被怀疑携带了秘密信息,则信息隐藏就失败了.信息隐藏的对立面——隐写分析,就是试图在一些看似正常的多媒体载体中,区分出哪些是正常的载体,哪些是携带了秘密信息的载体,一旦能够准确识别出来,则信息隐写就失败了.

而 Shannon 信息论面向通信工程,决定了它在理论上具有强烈的通信特色.Shannon 在"通信数学理论"[6]一文中明确指出:"通信系统的基本问题是,在统计噪声背景下,在信息接收端近似地或精确地复制发送端发出的信号波形",Shannon 在构建他的"通信数学理论"的时候,通过深入分析,明确地抓住了"噪声背景下复制信号波形"这个核心.为了研究在"随机噪声背景下"的信号波形复制,就需要引入概率论和随机过程一类数学方法作为信号波形分析的基本工具.这样,就使"通信数学理论"本质上成为了"统计型的通信理论".Shannon 的这些思想完全符合通信工程的实际需要,切中了通信技术的要害,对现代通信技术的发展做出了不朽的贡献.

但是把"通信模型"应用到信息隐藏领域是否合适呢?首先,信息隐藏的载体是多媒体信号,它们本身不是"随机噪声",而是有实际"信息内容"含义的信号,或者对于每一个具体的多媒体载体,可以说它是"确定型"信号,而不是"统计型"信号,因此目前的很多参考文献中估算隐藏容量时,需要假设载体、攻击信道等是高斯白噪声,这一点在具体算法设计时是不成立的,或者只能假设近似成立.第二,信息隐藏是人与人的智力较量,信息隐藏者要尽可能隐蔽地将信息传递出去,攻击者要尽可能从大量貌似正常的载体中找出那些非正常的载体,并且根据载体内容进行有针对性的破坏.可以说,信息隐藏的攻击者是人,而且攻击手段是有"智能"的,从目前信息隐藏或数字水印的应用情况也说明了这一点.而通信系统的目的是将发送端的信号精确地传递到接收端,信道所能产生的破坏就是提高噪声强度,而信道噪声是无"智能"的.目前研究信息隐藏的通信模型中,将攻击者模拟为信道的噪声干扰,没有考虑攻击者的主动攻击,即智能性攻击.

3.2 信息隐藏的最直接约束条件是"不引起载体的可察觉改变",这一点的度量是否准确?

要研究信息隐藏的最大容量,必然要涉及的一个最直接的约束条件是"不引起载体的可察觉改变",在目前的各类研究文献中,主要都是采用失真度量的方法,即嵌入信息后的载体与原始载体的失真度量小于某个门限,信道攻击产生的失真度量小于某个门限.当然有多种失真度量,例如载体对应元素的失真度量、载体某些重要特征参数的失真度量等.所有这些失真度量,都是载体信号本身差异的失真度量,没有从载体内容的角度考虑.正常的载体压缩、信号处理等,都会引起载体的失真,如何区分载体是由于正常的压缩引起的失真、还是由于嵌入秘密信息引起的失真?要知道,信息隐藏的攻守双方都是有极高智力的人,如何更加准确地描述"不引起载体的可察觉改变"这一较为"主观"的约束条件?

基于以上分析,我们认为,要想把信息隐写与隐写分析的研究推向更深入,需要一个更加合适的研究方法和模型.同时,要研究安全的信息隐写,必须详细了解隐写分析.隐写与隐写分析,是一个对立统一体,它们之间是相互促进的.

4 研究的思路

本文重点关注信息隐写与隐写分析的研究.信息隐写的目的是,以网络上传输的多媒体数据为载体,将秘密信息携带在多媒体载体中,同时,携带了秘密信息的多媒体载体与其他正常的多媒体数据一般人无法区分,只有秘密通信的双方已知隐写算法和密钥,才能够从中提取出秘密信息.隐写分析的目的是,对于一般人无法区分的多媒体载体,通过扩展隐写分析系统的"感知"能力,即抓住隐写产生的特征,区分出正常载体和非正常载体.

本文融合智能信息理论、模糊数学等思想,提出建立适合于隐写与隐写分析研究的工具与模型.

4.1 信息空间的描述

国内学者曾提出广义信息隐藏的模型[7],把信息描述为一个感知空间和记录空间,这两个空间是不完全重叠的,既有可感知但未被记录的信息,也有记录下来但无法感知的信息.

用空间的概念描述上述问题,我们可以假设全信息空间是 n 维的,即 $V^n=(v_1, v_2, \cdots, v_n)$,其中一个 r_1 维子空间是感知空间,表示为 $W^1=(v_{s_1}, v_{s_2}, \cdots, v_{s_{r_1}})$,另一个 r_2 维子空间是记录空间,表示为 $W^2=(v_{t_1}, v_{t_2}, \cdots, v_{t_{r_2}})$,$W^1$ 与 W^2 不完全重叠.因此属于 W^1 但不属于 W^2 的信息就是可以感知但未记录下的信息,而属于 W^2 但不属于 W^1 的信息就是可以记录但不可感知的信息.信息隐藏就是将感知空间里的信息想办法映射到一个可以记录但无法感知的空间中,而合法接收者具有逆映射和密钥,能够再正确映射回感知空间.而隐写分析就是在未知逆映射的情况下,将不可感知的信息感知出来.

4.2 全信息理论

在信息科学原理中,把信息分为本体论信息和认识论信息[8].本体论信息的定义是"事务运动状态及其变化方式的自我表述/自我显示",本体论信息是一种客观的存在,不与主体是否存在有关.主体关于某事务的认识论层次信息定义是"主体所感知或表述的关于该事务的运动状态及其变化方式,包括状态及其变化方式的形式、含义和效用".由于引入了主体,认识论层次的信息概念具有了比本体论层次信息概念丰富得多的内涵,既包含了信息的表现形式,又包含了主体对信息内在含义的理解,还包含了主体对事务价值的判断.因此,在信息科学理论中,把同时考虑事务运动状态及其变化方式的外

在形式、内在含义和效用价值的认识论层次信息称为“全信息”. 把只计及形式因素的信息称为“语法信息”, 把计及含义因素的信息称为“语义信息”, 把计及效用因素的信息称为“语用信息”.

对应全信息理论, 我们认为信息隐写与隐写分析不只涉及到信息的表现形式, 还涉及到信息的含义和效用. 因此我们将全信息理论的概念引入到信息隐写分析研究中. 把隐写分析按这三个层次划分, 目前隐写分析的研究可以认为在“语法”层次和“语义”层次上.

目前网络上有上百种公开的隐写软件, 不少隐写软件生成的隐写载体具有软件的特殊标记, 利用这些特征码匹配的方法, 可以识别经过特定软件隐写的载体. 我们可以把这类隐写分析定义为语法信息层次的隐写分析.

目前很多隐写分析算法研究, 是针对隐写载体数据(或内容)中出现的统计特征差异进行分析的, 例如针对 LSB 隐写的直方图分析、卡方分析、隐藏容量分析、RS 分析等, 针对 JPEG 图像的分析等, 都属于针对载体内容的隐写分析. 可以把这类隐写分析定义为语义信息层次的隐写分析.

再高一层的隐写分析, 可以定义为针对多媒体载体的使用所进行的隐写分析. 例如, 针对特定被监视对象之间的通信数据、大量数据的异常流量、流向, 用户的异常行为和状态等. 可以把这类隐写分析定义为语用信息层次的隐写分析.

应该说, 语用信息层次的隐写分析是隐写分析应用中的第一步, 它可以使“大海捞针”式的搜索变成有针对性的、集中目标的搜索. 具体应用中其实也是这样做的.

4.3 模糊信息处理理论

通过对隐写分析的研究我们注意到, 隐写分析能否成功, 与具体的隐写算法以及信息隐藏量的大小有直接的关系, 如果隐藏数据量很大, 产生了非常明显的特征, 则很容易(或很有把握)识别出非正常的载体. 如果在一个很大的载体中, 只嵌入 1 比特的数据, 则再好的隐写分析方法也无法识别出来. 因此隐写分析的结果不适合用二值逻辑描述(即: 有隐写、还是没有隐写), 而是采用隐写的“可疑度”来描述. 同时, “可疑度”应该与隐藏量和隐藏强度直接相关, 隐藏容量与隐写算法和载体直接相关. 而计算隐藏容量时又需要“不引起载体的可察觉改变”这一约束条件.

我们认为, 模糊信息处理是一个比较合适的研究方法[9]. 利用模糊集合的概念, 将所有可能的多媒体载体对象作为一个集合 U, 有两类模糊集合 A 和 B, A 代表正常载体集合, B 代表非正常载体(有隐写载体)集合. 对任意一个多媒体载体 x, 需要识别它属于集合 A 还是集合 B. 识别过程有两个重要的步骤: (1) 特征抽取: 从载体对象中提取反映其某些特征的数据; (2) 识别判决: 根据抽取的数据, 按某种分类规则对所给的载体对象进行判决, 指出载体对象归属于哪一个集合. 在模糊数学中, 某个载体对象归属于某一个集合是以隶属度来计算的. 隐写分析成功的标志是能正确区分正常载体和非正常载体. 而是否能以正确的隶属度将载体对象归类到集合 A 或集合 B 中, 关键在于特征的提取, 以及建立特征与隶属度之间的函数关系.

5 隐写分析研究框架

综合上述三方面的分析, 本文对信息空间从三个角度进行了分类(图 1).

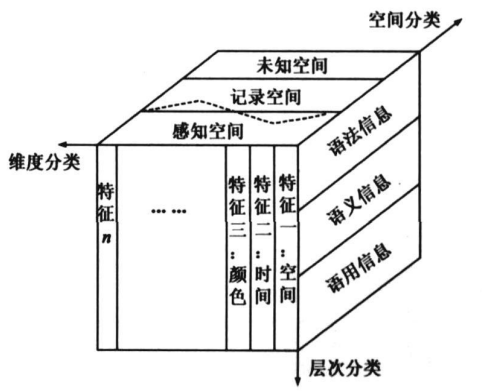

图 1　信息空间分类

从信息的层次分类, 可以分为语法信息、语义信息和语用信息. 这是从全信息的概念进行的分类.

从信息空间上分类, 可以分为感知空间、记录空间和未知空间. 其中感知空间与记录空间有重叠, 但不一定完全重合(图中虚线表示互相交叉重叠), 而未知空间则属于既无法感知也无法记录的空间, 当然, 随着技术的发展, 无论是记录空间还是感知空间都会逐步向未知空间扩展.

从信息空间的维度上分类, n 维信息空间的每一维就是信息的一个特征, 例如信息的时间、空间、方向、亮度、颜色、情感、统计特征、直方图特征、各种变换域系数的特征等等.

上述三种分类是对信息空间不同层面上的分类, 每个特征会归属于不同的信息层次, 每个特征也会分别是一些子空间(感知空间、记录空间和未知空间)的维度. 例如图像信号的空间特征、音频信号的时间特征都属于语法信息层次, 并且都会是记录空间的维度. 而情感特征则属于语用信息的层次, 情感信息的研究还不成熟, 目前所研究的记录空间和感知空间都不会包含情感这一特征, 因此目前把它归于未知空间的维度.

隐写分析的研究, 就是将原来不可感知的信息变成可以感知的, 也就是说原来不属于感知空间, 将感知空间扩充维数, 包含了信息的感知特征, 则信息变成可以感知的. 从隐写分析的研究看, 最初的 LSB 隐写是不可感知的, 自从人们发现了它的直方图异常特征之后, 它变成可以被感知的, 也就是感知空间扩充了“直方图特征”这一维. 随着隐写与隐写分析的算法不断在对抗中完善, 感知空间的维度会不断增加.

隐写分析者要做的工作就是尽可能发现隐写产生的特征, 将它添加到感知空间中去. 而隐写研究者的目的是尽可能隐蔽地进行隐写, 不产生可能的、明显的特征.

目前的隐写分析, 基本上是针对具体隐写算法, 分析其特征, 进行隐写分析. 我们把隐写分析提高到全信息的角度, 建立了一个隐写分析研究框架(图 2). 分别从语用、语义和语法信息的层次对待检测载体进行隐写分析, 同时需要建立语用、语义和语法信息三个层次的隐写分析特征库. 每个层次的隐

写分析采用模糊信息处理的方法,建立模糊集合,提取特征,识别判决.最后,对三个层次的判决进行综合,得到总体的隐写"可疑度".

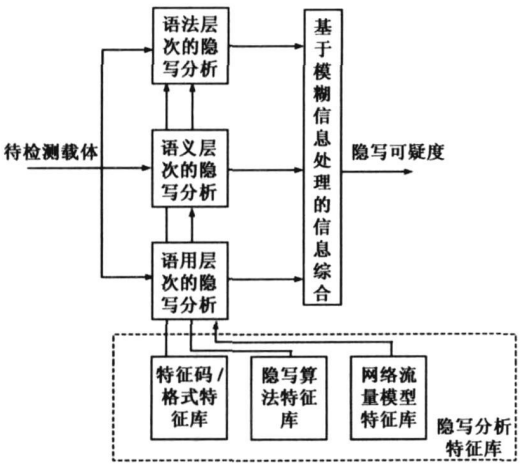

图 2 隐写分析研究框架

有了隐写分析研究框架,可以促进安全的隐写设计.即,设计新的隐写算法,使得隐写分析的可疑度降到最低.

6 结束语

本文对信息隐藏相关方面的研究进行了思考,特别对信息隐写与隐写分析的研究思路进行了探讨,提出了信息空间的分类以及隐写分析研究框架.更多的研究工作还有待继续深入.

参考文献:

[1] P Moulin, Joseph A. O' Sullivan. Information-theoretic analysis of information hiding[J]. IEEE Transactions on Information Theory, 2003, 49(3): 563- 593.

[2] M H M Costa. Writing on dirty paper[J]. IEEE Transactions on Information Theory, 1983, 29(3): 439- 441.

[3] Cohen A S, Lapidoth A. The Gaussian watermarking game[J]. IEEE Transactions on Information Theory, 2002, 48(6): 1639- 1667.

[4] A Somekh-Baruch, N Merhav. On the capacity game of public watermarking systems[A]. Proceeding of 2002 IEEE International Symposium on Information Theory[C]. Lausanne, Switzerland: IEEE, 2002. 223- 223.

[5] P Moulin, M K Mihcak. The parallel-Gaussian watermarking game[J]. IEEE Transactions on Information Theory, 2004, 50(2): 272- 289.

[6] C E Shannon. The mathematical theory of communication[J]. Bell System Technical Journal, 1948, 27: 62, 379.

[7] 林代茂, 胡岚, 郭云彪, 周琳娜. 广义信息隐藏技术的机理与模型[J]. 北京邮电大学学报, 2005, 28(1): 1- 5.

[8] 钟义信. 信息科学原理[M]. 北京: 北京邮电大学出版社, 2002.

[9] 曹谢东. 模糊信息处理及应用[M]. 北京: 科学出版社, 2003.

作者简介:

钮心忻 女, 1963 年 10 月出生于北京, 现为北京邮电大学教授、博士生导师.主要研究方向: 信息安全、信息隐藏与数字水印、数字内容安全、软件无线电等.
E-mail: xxniu@bupt.edu.cn

杨义先 男, 1961 年 3 月出生于四川绵阳, 现为北京邮电大学教授、博士生导师.主要研究方向: 网络与信息安全、密码学、编码理论等. E-mail: yxyang@bupt.edu.cn