# 广义信息隐藏技术的安全问题*

林代茂, 胡 岚, 郭云彪, 周琳娜
(北京电子技术应用研究所, 北京 100091)

摘 要: 对信息隐藏的安全性问题进行了深入讨论, 给出了不同应用模式下的信息隐藏安全性定义, 结合广义信息隐藏有关理论给出了广义信息隐藏安全性条件, 并利用感知系统空间理论加以精确描述, 在分析理论安全的基础上, 对广义信息隐藏的现实安全给出了解释。

关键词: 信息隐藏; 安全性; 信息隐藏分析
中图分类号: TP391.1 文献标识码: A 文章编号: 0529-6579 (2004) S2-0014-03

信息隐藏技术的安全性问题是一个热门话题, 有些研究者借鉴了密码学的研究成果[1,2], 有些研究者用传统信息论的方法[3,4]得到了重要的结论。然而信息隐藏技术毕竟是一个新的学科, 需要针对其自身特点导出更直观的结果。另一方面, 这些结果必须与信息隐藏技术的机理相匹配。我们可以从认识论的角度解释信息隐藏技术的机理, 在此基础上定义广义信息隐藏, 通过分析可以得出, 掩盖信息的存在并不是实现广义信息隐藏的必要条件。在这篇文章中, 我们将依据这些基本概念对广义信息隐藏技术的安全问题作进一步的研究。

## 1 信息隐藏安全性的含义

信息隐藏技术之所以受到许多研究者的关注并得到较快的发展, 是由于它具有广泛的应用前景。虽然不同应用场合对信息隐藏技术的要求不同, 但是都涉及一个共同的问题, 即信息隐藏技术的安全性问题。

安全性的定义取决于信息隐藏技术的应用目的, 或者说取决于它所面临的威胁。嵌入信息量与通信安全的矛盾、声像质量与水印鲁棒性的矛盾以及文件可信性与水印完好性的关系是讨论信息隐藏技术安全性的出发点。

### 1.1 隐蔽通信应用

Alice 与 Bob 之间的秘密通信可能受到 Wendy 的 4 种威胁: ①发现或有依据的怀疑他们在传递秘密消息; ②不仅发现了 Alice 和 Bob 在进行秘密通信, 而且提取了秘密信息; ③Wendy 无论是否怀疑 Alice 在与 Bob 进行秘密通信, 都要修改通信内容; ④完全禁止 Alice 与 Bob 的任何通信。其中第 2 种威胁是以第 1 种威胁为前提的, 而第 4 种威胁已经超出了讨论的范围, 因此针对另两种威胁来定义信息隐藏的安全性。

定义 1 用于隐蔽通信的信息隐藏技术是 S1 类安全的, 是指攻击者没有合理的理由证明经过传输信道的通信信息 $S'$ (经过传输信道后的 Stego message) 中隐藏有秘密信息 $M$。

定义 2 用于隐蔽通信的信息隐藏技术是 S2 类安全的, 是指攻击者无法损坏经过传输信道的通信信息 $S'$ 中所隐藏的秘密信息 $M$。

不能把这两类安全性定义理解为递进关系, 这是因为两种攻击可能独立进行。

### 1.2 版权保护应用

信息隐藏技术的第 2 种典型应用是保护声像产品版权的数字水印技术, 它所面临的攻击是盗版者消除水印的企图, 因此, 人们希望水印信息具有鲁棒性, 在这里, 鲁棒性和安全性是同意语。

定义 3 用于版权保护的信息隐藏技术是 R 类安全的, 是指攻击者对含有水印的信息 $S$ 的任何攻击都不能彻底消除水印的痕迹。

### 1.3 文件可信性应用

和鲁棒性水印相反, 当人们用脆弱性水印来防止别人恶意篡改文件内容时, 不是担心水印被删除或破坏, 而是担心攻击者在不影响水印的情况下篡改了文件的内容。要求二者一全皆全、一损皆损。因此关于安全性的第 4 个定义是:

定义 4 用于保护文件可信度的信息隐藏技术是类 $T$ 安全的, 是指攻击者不可能在不损坏水印

* 收稿日期: 2004-09-11
基金项目: 国家 863 高科技资助项目 (2002AA145010); 国家 973 计划资助项目 (TG1999035804)
作者简介: 林代茂 (1945 年生), 男, 研究员, 博士生导师; E-mail: daimaolin@hotmail.com

的情况下对含有水印的信息 $S$ 作任何的篡改。

## 2　广义信息隐藏技术的安全性条件

### 2.1　广义信息隐藏技术机理的回顾

基于广义信息隐藏的机理，为了对下面的讨论有共同的术语，有必要对这一机理作一个简要的回顾。

信息记录系统可以记录多维信息空间 $V$ 中部分区域 $V_r \subset V$ 的信息，信息感知系统能够感知的信息也属于信息空间中的一个区域 $V_d \subset V$。需要隐藏的秘密信息 $M$ 本来位于 $V_d$ 之中，但是经过映射作用后，成为可以记录而不可感知的 $M'$，$M' = F(M) \in V_d \text{Ⅳ}_r$ 从而实现了信息隐藏。

### 2.2　广义信息隐藏技术的安全性条件

在具体讨论安全性之前，需要对下面的情况作一个约定。即攻击行为可能破坏了原来的隐藏信息，使映射 $M'$ 变成了 $M''$(见图 1)，这时，信息隐藏的实现者无法从 $F'(M')$ 和 $F'(M'')$ 得到隐藏的信息 $M$，从而无法有效地保护声像产品的版权或者不能达到隐蔽通信的目的。可以认为 $M' \in V_r$ 已不再成立，虽然可能存在一种反向映射，使得 $G(M'') = M$，但这是实现者和攻击者都不知晓的，没有实际的意义。

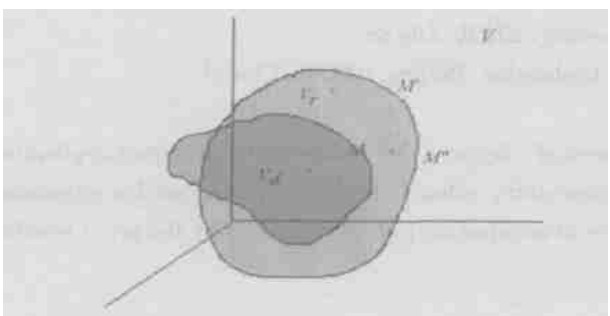

图 1　信息空间示意图

Fig. 1　Illustration of infomation space

S1 类安全要求攻击者没有合理的理由证明经过传输信道的通信信息 $S'$ 中隐藏有秘密信息 $M$。不能把信息隐藏的安全性依赖于传输信道的特性，因此，S1 类安全实质上要求攻击者没有足够的理由证明 $S$ (stego message) 中隐藏有秘密信息 $M$。这只要 $M'$ 不会落入攻击者的感知范围就可以了，即 S1 安全的充要条件是：

$$M' \notin V_d^a \tag{1}$$

始终成立。

其中，上标 $a$ 表示感知系统的主体是攻击者。

S2 类安全的定义是攻击者无法破坏隐藏的秘密信息 $M'$，不管他是否怀疑有隐藏信息的存在。也就是说，无论实施了哪种攻击行为，$M'$ 可以被隐藏实现者所感知的性质始终不能遭到破坏，即 S2 类安全的充要条件是：

$$M' \in V_d^m \subset V_r \tag{2}$$

始终成立。

其中，上标 $m$ 表示感知系统的主体是信息隐藏的制造者。值得注意的是，此时应有 $V_d^m \supset V_d^a$。

R 类安全要求无论受到何种攻击都不能彻底消除水印的痕迹，前已提到，R 类安全与 S2 类安全含义相同，因此 R 类安全的充要条件同样是：

$$M' \in V_d^m \subset V_r \tag{3}$$

始终成立。

T 类安全强调水印的脆弱性，要求水印信息 $M$ 始终与被保护文件 $C$ 联系在一起。可以考虑建立 $C$ 与 $M$ 之间的某种联系作为安全性条件，但是与其它安全条件相一致的表述还是要求在信息记录区域中保留完整的 $M'$。至于在不修改 $C$ 的情况下完全消除水印的问题不是脆弱水印关心的主要内容，因为接收者理应收到带有水印的文件，如果水印被消除，他完全有理由相信文件可能已被修改。这样，T 类安全的必要条件可表示为：

$$M' \in V_r \tag{4}$$

始终成立。

比较上述几个条件，我们发现尽管信息隐藏技术的不同应用领域给出不同的安全性定义，但是它们成立的条件却相当一致。无论在哪个应用领域，信息隐藏技术的实现都建立在信息可以记录的基础上。S1 类安全取决于双方感知能力的竞争，其它类的安全要求不破坏信息记录。显然，这个结果非常自然合理，而且很直观。

## 3　广义信息隐藏技术的现实安全

在密码学中，人们建立了理论安全和现实安全的不同定义，二者之间的差别是由于计算时间和存储空间的限制造成的。而我们在上一节里仅仅讨论了广义信息隐藏的理论安全，有必要对其现实安全作进一步的解释。

一般来说，信息记录系统对信息隐藏的实现者和攻击者是一样的，而信息感知系统却因人而异(盲人的视觉区域可能为零的例子明显地说明了这个问题)。

信息感知系统是时变的、不连续的系统，广义信息隐藏技术的实现和被攻击过程就是双方增强感知能力、扩大感知区域的过程。

对于广义信息隐藏技术的实现者来说，他的感知范围除了原来的 $V_d$ 以外，又增加了 $M'$ 点，形成

了不连续的信息感知区域。而对于攻击者来说，信息感知系统可能仍是 $V_d$ 未变。为了实现有效的攻击，攻击者会不断地变换攻击方法，力图扩大自己的感知能力，使隐藏的信息落在他的感知区域之中，从而断定隐藏信息的存在，或者通过破坏 $M'$，使实现者的感知区域回归为 $V_d$。

因此，广义信息隐藏技术的现实安全取决于二者的竞争。正如加密算法是否安全实际取决于破密者的攻击能力，未必由穷举空间决定一样，广义信息隐藏的现实安全决定于攻击方法的有效性。

## 4 结 论

本文对信息隐藏的安全性问题进行了深入讨论，给出了不同应用模式下的信息隐藏安全性定义，结合广义信息隐藏有关理论给出了广义信息隐藏安全性条件，并利用感知系统空间理论加以精确描述：信息隐藏技术的实现是建立在隐藏信息可记录的基础上，信息隐藏的安全取决于攻防双方感知能力的竞争。在分析理论安全的基础上，对广义信息隐藏的现实安全给出了进一步解释，本文尽管没有能够精确定量地给出信息隐藏安全与感知系统之间的关系，没有形成自成体系的完备理论模型，但研究结果对我们设计安全高效的信息隐藏系统有着极为积极的指导意义。

参考文献：

[1] 胡岚, 周琳娜, 郭云彪. 信息隐藏分析与攻击∥信息隐藏第四届全国学术研讨会(CIHW2002)论文集[C]. 北京: 机械工业出版社, 2002: 34－41.

[2] 尤新刚, 周琳娜, 郭云彪. 信息隐藏学科的主要分支及术语∥信息隐藏第三届全国学术研讨会(CIHW2001)论文集[C]. 西安: 西安电子科技大学出版社, 2001: 43－50.

[3] SMITH J R, COMISKEY B O. Modulation and information hiding in images, workshop on information hiding[M]. University of Cambridge, UK, 1996.

[4] Ramkumar Mahalingam, Akansu Ali N. Theoretical capacity measures for data hiding in compressed images[C]. The International Society for Optical Engineering 1999, 3528: 482－492.

# The Security of Generalized Information Hiding

*LIN Dai-mao, HU Lan, GUO Yun-biao, ZHOU Lin-na*

(Beijing Institute of Electronic Technology and Application, Beijing 100091, China)

**Abstract**: A deep analysis of security on information hiding is presented. Security definitions for the different application are also proposed here. Based on the concept of the generalized information hiding, this paper put forward a interesting issue about how to deal with the security problem. The secure theory of information hiding is verified by the given feasible settlement

**Key words**: information hiding; security; steganalysis