文章编号:1004-1478(2012)03-0005-06

流媒体信息隐藏的安全性界定及安全容量模型

田晖[1], 卢璟[2], 陈永红[1]

(1. 华侨大学 计算机科学与技术学院,福建 厦门 361021;
2. 华侨大学 信息处,福建 厦门 361021)

摘要: 针对目前流媒体信息隐藏尚无具有普遍意义的理论模型问题,从流媒体的载体特性出发,借鉴信息论和最优化技术,在阐述流媒体信息隐藏的安全性原理的基础上,给出了其不可感知性和不可检测性的定义. 分析了隐藏容量的相对性和安全容量问题,进而提出一种流媒体多隐藏信道安全容量模型,指出多隐秘信道的并行使用将有助于获得最佳的隐藏性能.

关键词: 信息隐藏; 隐蔽通信; 流媒体; 安全隐藏容量
中图分类号: TP309.2; TP309.7 **文献标志码:** A

Secure definition and secure capacity model of streaming-media information hiding

TIAN Hui[1], LU Jing[2], CHEN Yong-hong[1]
(1. *College of Comp. Sci. and Tech., Huaqiao Univ., Xiamen* 361021, *China*;
2. *Dept. of Infor., Huaqiao Univ., Xiamen* 361021, *China*)

Abstract: Aiming at the problem that the streaming-media information hiding has no universal theory model until now, the formal definition of perceptive transparency and statistical security were given based on elaborating secure principle of streaming-media information hiding using information theory and optimization techniques from the carrier of streaming-media characteristic. The relativity of hiding capacity and secure capacity were investigated, a secure capacity model of multi-hiding information channel based on streaming-media was proposed, the covert multi-channel of streaming-media can be employed in parallel to achieve a nice hiding performance.

Key words: information hiding; covert communication; streaming-media; secure hiding capacity

0 引言

信息隐藏是1990年代末提出的一种新的信息安全技术. 它通过把隐秘信息藏匿于可公开的载体(数字媒体)中以实现隐蔽通信及版权保护等目的. 与传统加密技术相比,它不仅关注隐秘信息实质内容的隐藏,更强调要掩盖其存在的事实,从而为隐秘信息提供更好的安全保护. 因此,信息隐藏从提

收稿日期:2011-11-29
基金项目:福建省自然科学基金计划资助项目(2011J05151);华侨大学科研基金资助项目(11BS210);华侨大学"中央高校基本科研业务费"(JB—ZR1131,JB—ZR1148);福建省重大科技计划专项(2011H6016)
作者简介:田晖(1982—),男,湖北省赤壁市人,华侨大学讲师,博士,主要研究方向为计算机网络与信息安全、智能信息处理.

出开始就一直受到研究者们的广泛关注[1].

近年来,基于流媒体的信息隐藏研究逐渐成为新的研究热点. 相比于静态的存储型媒体(如图像、文本等),动态流媒体能够为隐秘信息提供更为庞大的载体空间和更为安全的存在环境. 目前,基于流媒体的信息隐藏技术研究已取得了一些显著成果,如基于 P2P 的信息隐藏[2]、基于 IPTV 的信息隐藏[3]以及基于 VoIP 的信息隐藏[4-11]等;研究内容主要包括信息隐藏方法、信息隐藏编码算法和隐蔽通信系统的实现技术等. 然而,迄今为止流媒体信息隐藏尚无具有普遍意义的理论模型.

为此,本文在前期研究基础上,借鉴信息论和最优化理论的思想,从流媒体的载体特性出发,提出一种流媒体信息隐藏的安全容量模型.

1 流媒体信息隐藏的一般应用模型

流媒体信息隐藏的一般应用模型如图 1 所示.

图 1 流媒体信息隐藏的一般应用模型

图 1 中的场景表述如下:发送者和接收者打算通过流媒体信息隐藏经由公共的网络信道传输隐秘信息. 为此,通信双方首先建立了一个看似正常的流媒体通信. 与此同时,发送者利用某种安全的隐藏算法,在保证透明性(不对流媒体的正常通信产生影响)的前提下把隐秘信息嵌入到流媒体数据包中. 另一方面,接收者在载密数据包到达后,通过相应的解析算法准确提取对方所隐藏的隐秘信息. 通常,还假设在上述通信过程中存在着非法窃听者他一直希望探测到通信双方会话过程中可能存在的隐藏行为,并试图获得隐秘信息. 为了抵制非法窃听者的攻击,上述隐秘通信还需引入某个密钥来对隐藏过程及隐秘信息进行控制和保护. 不失一般性,基于流媒体的信息隐藏系统的定义可形式化描述如下.

定义 1 对于给定的六元组 $\Omega = <C, M, K, C^*, \Phi, \Psi>$,其中,$C$ 表示载体流媒体信息的集合,M 表示隐秘信息的集合,C 必须能够完全地隐藏 M,即 $|C| \geqslant |M|$;K 表示密钥集合;C^* 表示载密流媒体信息的集合;Φ: $C \times M \times K \rightarrow C^*$ 代表嵌入函数;Ψ: $C^* \times K \rightarrow M$ 代表提取函数. 如果某系统 $\forall c \in C, m \in M$ 和 $k \in K$,满足 $\Psi(\Phi(c, m, k), k) = \Psi(c^*, k) = m$,则该系统称为基于流媒体的信息隐藏系统.

2 流媒体信息隐藏的安全性界定

2.1 流媒体信息隐藏的安全性证明

流媒体信息隐藏系统中,发送方可通过载体信息 C、隐秘信息 M 和密钥 K 唯一地得到载密信息 C^*,即 $H(C^* | (C, M, K)) = 0$;而接收方准确提取 M 的充要条件是 $I(M; C^* | K) = H(M)$. 进一步展开该式可得到 $I(M: C^* | K) = H(M | K) - H(M | C^*, K) = H(M) - H(M | C^*, K) = H(M)$. 从而,$H(M | C^*, K) = 0$,含义是在“已知 C^* 和 K 后可唯一地确定 M”.

如前所述,被动攻击者的目标是截获 C^*,并试图提取 M. 因此,对应存在条件熵 $H(M | C^*)$,其含义是“在给定 C^* 后,M 尚存在的不确定性”. 为抵制攻击,隐藏过程的设计者同样依据 $H(M | C^*)$ 拟定隐藏方法,即隐藏系统的安全性取决于已知 C^* 后 M 尚存在的不确定性. $H(M | C^*)$ 值越趋近于 $H(M)$,该隐藏系统就越安全. 特别地,当 $H(M | C^*) = H(M)$,即 $I(M; C^*) = H(M) - H(M | C^*) = 0$ 时,该系统具有绝对安全性,因为此时被截获的 C^* 不能为攻击者提供任何额外信息. 不过,尽管此系统在攻击者只获得 C^* 时是安全的,但并不能确保攻击者同时获得 C 时的安全性. 换言之,如果攻击者能够同时获得 C^* 和 C,那么该系统是不安全的. 这一判断可通过反证法证明[12].

要使攻击者在获得 C 和 C^* 之后,仍然不能提取 M,需满足 $I(M; (C^*, C)) = H(M) - H(M | (C^*; C)) = 0$,即必须满足安全条件 $H(M | (C^*, C)) = H(M)$,也就是说必须有 M 与 C 和 C^* 相互独立. 不妨假设 $H(C) = H(C^*)$,当 C^* 中没有嵌入信息时,$H(C^* | C) = H(C | C^*) = 0$. 当 C^* 中嵌入信息后,$H(C^* | C) = H(C | C^*) > 0$. 根据不确定性与熵的关系可知,已知 C^* 后对 C 的不确定性等价于对 C 和 C^* 的观察所能获得的 M 的信息. 因而,在 C^* 中嵌入信息后,$I(M; (C^*, C)) = H(M) - H(M | (C^*; C)) > 0$,即 $H(M | (C^*, C)) < H(M)$,这意味着

$H(C^*|C)=H(C|C^*)>0$ 时,并不能满足上述安全条件. 只有当 $H(C^*|C)=H(C|C^*)=0$ 时才能让上述安全条件成立,而这又表示载体中不隐藏任何信息,这又与信息隐藏的初衷相悖. 由此可得出结论,攻击者能够同时获得 C 和 C^* 的信息隐藏系统是不安全的. 换言之,任何信息隐藏系统必须避免原始载体信息的泄漏.

从信息论的角度出发,安全信息隐藏系统必须使得攻击者对于 C 的不确定性应该不小于对于 M 的不确定性,即必须满足 $H(C)\geqslant H(M)$. 在流媒体信息隐藏系统中,载密流媒体样本具有不可再生性,其内容在通信开始之前并未生成,而通信结束后就会予以丢弃,因而流媒体信息隐藏系统从根源上排除了攻击者获得 C 的可能,也就是 $H(C)\geqslant H(M)$ 恒成立. 因此,较之基于存储型媒体的信息隐藏系统,流媒体信息隐藏系统能够提供更好的安全性能.

2.2　流媒体信息隐藏安全性的界定

流媒体信息隐藏的安全性通常包括不可感知性和不可检测性. 不可感知性,是指对于用户而言,隐藏过程在感官上是不可分辨的,因此要求隐藏过程必须维护流媒体感官效果和使用价值,这也正是"隐"的前提; 不可检测性是指载体的统计特性不能发生明显改变,也就是统计上须具有不可分辨性,因此要求隐藏过程尽可能维护流媒体被修改前后具有一致的统计特性.

下面分别就不可感知性和不可检测性进行分析.

1) 不可感知性分析. 不可感知性是一切信息隐藏的前提. 载体感官效果的评价方式大致可分为主观评价和客观评价. 前者以人的主观判断为基础; 后者则是通过某些参数来衡量载体的质量或信息隐藏后的失真程度. 常见感官效果的评价方法可参阅文献[13]. 尽管评价方法侧重点不同,却有一个一致的目标,也就是给出一个载体失真的度量. 不失一般性,将隐藏前后的载体失真记为 $T(C,C^*)$; 根据密钥选择的不同,记给定隐藏方法失真度的数学期望为 $E(T(C,C^*))$. 不难看出,当 $E(T(C,C^*))$ 的值足够小时,可满足不可感知性. 由此,流媒体信息隐藏系统的不可感知性可描述如下.

定义 2　在流媒体信息隐藏系统 Ω 中,$T(C,C^*)$ 为隐藏前后的失真函数. 当 $E(T(C,C^*))\leqslant\delta$,则称系统 Ω 是 δ 即不可感知的; 特别地,当 $E(T(C,C^*))=0$ 时,则称系统 Ω 是绝对不可感知的.

据此定义可知,不同隐藏方法不可感知性的比较等价于这些方法所能达到的最小 δ 值的比较. 需要指出的是,失真函数选取将是该环节的关键,针对不同载体可能会有不同的失真函数. 其中,均方差函数是一种普遍采用的失真评价方式[14],其计算方式为

$$T(\boldsymbol{X},\boldsymbol{Y})=\frac{1}{n}\sum_{i=1}^{n}(x_i-y_i)^2$$

式中,$\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 均为 n 维向量.

2) 不可检测性分析. 信息论中,互熵常用于衡量 2 个概率分布的差异性. 给定 χ 上的 2 个概率分布 $p(x)$ 和 $q(x)$,其互熵可定义为

$$D(p\parallel q)=\sum_{x\in\chi}p(x)\log\frac{p(x)}{q(x)}$$

式中,当 $p(x)=q(x)=0$ 时,取 $D(p\parallel q)=0$; 当 $p(x)=0$ 而 $q(x)>0$ 时,$D(p\parallel q)=\infty$. 对于任意的 $p(x)$ 和 $q(x)$,有 $D(p\parallel q)\geqslant 0$,且当 $p(x)=q(x)$ 时 $D(p\parallel q)=0$. 由于互熵也常被看做 2 个概率分布的某种"距离"差异,因而也被称为 Kullback Leibler 距离.

文献[15]最先采用互熵来衡量信息隐藏系统中载体信息和载密信息的概率分布差异. 当两者差异足够小时,隐藏过程对于攻击者而言是不可检测的. 以此为基础,流媒体信息隐藏系统的不可检测性可以描述如下.

定义 3　在流媒体信息隐藏系统 Ω 中,载体信息 C 的概率分布记作 P_C,载密信息 C^* 的概率分布记作 P_{C^*}. 当 $D(P_C\parallel P_{C^*})\leqslant\varepsilon$,则称系统 Ω 是不可检测的; 特别地,当 $D(P_C\parallel P_{C^*})=0$ 时,则称系统 Ω 是绝对不可检测的.

值得强调的是,在流媒体信息隐藏过程之中,攻击者往往是难以获得原始载体及其确切统计特征的. 不过,也不可排除攻击者通过对正常流媒体通信进行细致观察,总结出某些流媒体分布特征. 这些公共特征也正是隐藏算法的设计者们应密切注意的. 攻击者不断地发掘新的载体特征以达到其攻击目的,而设计者们也必须不断地改进相应的隐藏算法以维护这些载体特征不发生显著变化. 这是一个典型的博弈过程,从而也注定了隐藏方法和隐

藏分析(攻击)方法的有效性都具有阶段性特点,并且也正是在这种对抗中互相促进并交替发展.

3 流媒体信息隐藏的安全容量模型

3.1 安全隐藏容量问题

使得载体信息和载密信息在统计上不可分辨是安全的信息隐藏系统的目标之一,也是抵抗各种可能攻击的前提. 如果某个概率分布模型能够准确地描述载体信息的部分统计特性,那么该模型可以用于指导设计一个相对安全的信息隐藏系统. 换言之,倘若该模型囊括了攻击者所知的所有统计特性,那么以该模型为基础而构建的信息隐藏系统对于攻击者来说是不可检测的. 因此,信息隐藏的安全性也就取决于模型所能描述统计特性的能力.

模型描述的概率特性越精确,那么隐藏系统的安全性能越佳. 此外,给定的概率模型要能够测度信息隐藏系统的安全容量,即最大隐秘信息长度. P. Sallee [16] 首先提出了这种基于模型的信息隐藏设计思路.

根据之前的分析,当某一类载体的集合 C 上的确切概率分布模型 P_C 确定后,依据该模型嵌入生成的载密信息与对应载体信息是统计上不可分辨的. 然而,在现实应用中,得到这种确切模型是很困难的,隐藏算法的设计只能以观察到的近似模型 $\hat{P}_C$ 为基础. 基于模型的隐藏编码算法如图 2 所示.

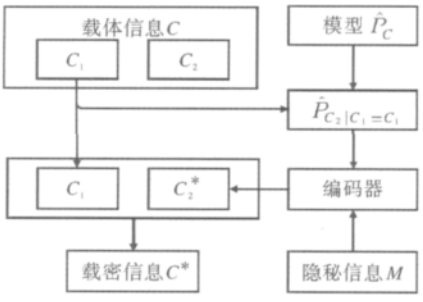

图 2 基于载体特性模型的隐藏编码算法

图 2 可描述如下:

1) 将载体信息 C 划分为 C_1 和 C_2 两部分. 隐藏过程主要替换 C_2 部分而对 C_1 不作修改. C_1 的作用在于确定适合 C 的条件概率分布 $\hat{P}_{C_2|C_1=C_1}$;

2) 按概率分布 $\hat{P}_{C_2|C_1=C_1}$ 将隐秘信息进行编码得到 C_2^*;

3) 将 C 中的 C_2 替换为 C_2^*,即生成载密信息 C^*.

图 3 描述了基于载体特性模型的隐藏解码算法一般流程:

1) 将载密信息 C^* 划分为 C_1 和 C_2^* 两部分;

2) 将 C_1 代入模型 $\hat{P}_C$ 得到条件概率分布 $\hat{P}_{C_2|C_1=C_1}$;

3) 按概率分布 $\hat{P}_{C_2|C_1=C_1}$ 从 C_2^* 中解析出隐秘信息 M.

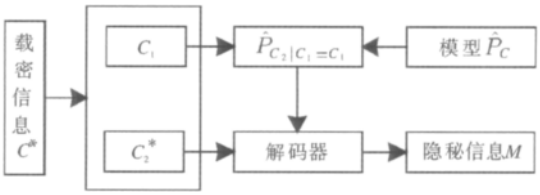

图 3 基于载体特性模型的隐藏解码算法

由以上编解码流程不难得知: 隐藏系统设计者确保信息隐藏系统安全性的前提是获得理想的模型 $\hat{P}_C$; 攻击者能够检测出以 $\hat{P}_{C_2|C_1}$ 为模型的信息隐藏过程的前提是获悉较之 $\hat{P}_{C_2|C_1}$ 更为精确或拥有更多统计特性的概率分布模型. 除此以外,还可以引入密钥 K 对编解码过程进行保护和控制以进一步增强安全性. 此时,密钥就成了正确提取隐秘信息的关键.

安全隐藏容量等价于在不被检测出的前提下载体信息所能隐藏的隐秘信息最大长度. 以模型 $\hat{P}_C$ 为基础构建的信息隐藏系统安全容量是可测度的. 从信息论的角度来看,C_2 等价于隐藏过程的信道,其安全容量可以用 $\hat{P}_{C_2|C_1}$ 的熵来测度. 换言之,安全隐藏容量可形式化描述如下.

定义 4 对于载体集合 C 中的某个给定实例 C,C_1 为 C 中的不变部分,C_2 为 C 中的可隐藏部分. 当以概率模型 $\hat{P}_C$ 为基础设计隐藏算法时,其安全隐藏容量为条件概率分布 $\hat{P}_{C_2|C_1}$ 的熵,即

$$r(\hat{P}_C, C_1) = H(C_2 | C_1 = C_1) =$$

$$-\sum_{C_2} \hat{P}_{C_2|C_1}(C_2 | C_1) \log_2 \hat{P}_{(C_2|C_1)}(C_2 | C_1)$$

虽然安全隐藏容量随着载体的内容不同会有所变化,但对于给定的载体 C 而言,其隐藏容量是关于 $\hat{P}_C$ 和 C_1 的函数. 尽管该定义给出了保证统计安全性前提下的隐藏容量,但这还不是流媒体信息隐藏安全容量的最终答案.

3.2　流媒体信息隐藏的安全容量模型的构建

与存储型媒体不同,流媒体是一种多通道的隐秘载体. 不仅流媒体信号而且各层的网络协议[17](如 RTP,RTCP,TCP,IP 等)也都能作为传输隐秘信息的信道. 因此,流媒体信息隐藏系统的容量问题可视做组合信道容量问题. 对于流媒体信号来说,隐藏过程需同时满足不可感知性和不可检测性; 而对网络协议而言,隐藏操作只需维护不可检测性. 将流媒体信号视做独立信道,其安全隐藏容量 V_α 可定义如下.

定义 5　设流媒体载体信号集合 C_α 的真实概率分布特征为 P_{C_α},C_α 表示该集合中的某个载体实例,C_{α_1} 表示 C_α 中的不可替换部分. 当隐藏算法以统计分布模型 $\hat{P}_{C_\alpha}$ 为基础时,流媒体载体信号的隐藏容量等价于满足不可感知性和不可检测性约束条件下函数 $r(\hat{P}_{C_\alpha}, C_{\alpha_1})$ 的最大值,即

$$\begin{cases} V_\alpha = \max r(\hat{P}_{C_\alpha}, C_{\alpha_1}) \\ s.t.\ D(P_{C_\alpha} \| \hat{P}_{C_\alpha}) \leqslant \varepsilon_\alpha \\ E(T(C_\alpha, C_\alpha^*)) \leqslant \delta_\alpha \end{cases}$$

由于网络协议的信息隐藏具有极大相似性,可将各层网络协议视做一个整体,其安全隐藏容量 V_β 可定义如下.

定义 6　设网络协议载体集合 C_β 的真实概率分布特征为 P_{C_β},C_β 为该集合中一个载体实例,C_{β_1} 表示 C_β 中的不可替换部分. 当隐藏算法以统计分布模型 $\hat{P}_{C_\beta}$ 为基础时,网络协议载体的安全隐藏容量等价于满足统计安全性约束条件下函数 $r(\hat{P}_{C_\beta}, C_{\beta_1})$ 的最大值,即

$$\begin{cases} V_\beta = \max r(\hat{P}_{C_\beta}, C_{\beta_1}) \\ s.t.\ D(P_{C_\beta} \| \hat{P}_{C_\beta}) \leqslant \varepsilon_\beta \end{cases}$$

当以上 2 个信道轮流使用时,即它们以和信道方式工作时,流媒体信息隐藏系统的安全隐藏容量 V 将满足如下关系:

$$V = p_\alpha V_\alpha = p_\beta V_\beta \leqslant \max(V_\alpha, V_\beta)$$

式中,p_α 表示流媒体信号隐藏信道的使用概率,p_β 表示网络载体隐藏信道的使用概率,且两者之和为 1,即 $p_\alpha + p_\beta = 1$. 当 $V_\alpha = V_\beta$ 时,式中等号成立. 该式表明,和信道的隐藏容量小于或等于 V_α 和 V_β 中的最大值.

当上述 2 个信道以独立并行信道的方式工作时,流媒体信息隐藏系统的安全隐藏容量 V 将满足如下关系:

$$V \leqslant V_\alpha + V_\beta$$

该式表明 2 个信道并行使用时的隐藏容量小于或等于 2 个信道单独使用时的隐藏容量之和. 从理论上分析,当 2 个信道独立使用且输入独立时上式等号成立. 然而,现实应用中,由于两信道同步的需要,将会降低总隐藏容量. 尽管如此,2 个信道并行时的隐藏容量通常大于 V_α 和 V_β 中的最大值,从而也就大于和信道的隐藏容量. 因此,把 2 个信道作为独立并行信道使用是流媒体信息隐藏系统设计中的较好选择. 值得指出的是,由于网络协议中不宜隐藏过多的隐秘信息,目前应用中主要是利用网络信道传输少量的同步比特序列,而将主体隐秘信息隐藏于流媒体信号中[4]. 其他的多隐秘信道并行方式还有待进一步研究.

4　结语

本文以信息论和最优化理论为工具,在阐述流媒体信息隐藏的安全性原理的基础上,给出了其不可感知性和不可检测性的定义. 进而提出了一种流媒体多隐藏信道安全容量模型. 通过对流媒体信息隐藏问题的探讨,认为:

1) 流媒体样本具有不可再生和即用即弃的特点,因而基于流媒体的信息隐藏系统可从根源上避免攻击者获得原始载体的可能,较之存储型媒体具有更好的安全性能.

2) 流媒体信息隐藏系统设计中,不引起攻击者怀疑的主要手段是尽可能降低载体失真,而抵抗攻击的重要前提是隐藏过程不能显著改变载体信号的已知概率分布特性.

3) 信息隐藏系统的安全性取决于已知概率分布模型描述载体统计特性的能力. 信息隐藏容量具有相对性. 以已知模型为基础的安全隐藏容量才具有实践意义.

4) 流媒体载体是一种多通道隐秘载体,包括多种协议隐藏信道和信号隐藏信道. 这些信道可并行使用以获得信息隐藏的最佳性能.

参考文献:

[1]　Provos N,Honeyman P. Hide and seek: an introduction to steganography [J]. IEEE Security & Privacy Magazine,

2003,1(3):32.

[2] Raphael E,Thomas L,Roger W. Hidden communication in P2P networks: steganographic handshake and broadcast [C]//Proc of the 30th IEEE Int Conf on Comp Com (INFOCOM 2011),Los Alamitos: IEEE,2011:1-9.

[3] Ramirez D H. IPTV Security: Protecting High-value Digital Contents [M]. Hoboken: Wiley Press,2008.

[4] Tian H,Jiang H,Zhou K,et al. Adaptive partial-matching steganography for voice over IP using triple *m* sequences [J]. Comp Com,2011,34(18):2236.

[5] Huang Y,Tang S,Yuan J. Steganography in inactive frames of VoIP streams encoded by source codec [J]. IEEE Trans on Infor Forensics and Security,2011,6(2):296.

[6] Mazurczyk W,Lubacz J. LACK—A VoIP steganographic method [J]. Telecom Syst J,2010,45(2-3):153.

[7] Lubacz J,Mazurczyk W,Szczypiorski K. Vice over IP [J]. IEEE Spectrum,2010,47(2):42.

[8] Tian H,Zhou K,Feng D. Dynamic matrix encoding strategy for voice-over-IP steganography [J]. J of Central South Univ of Tech,2010,17(6):1285.

[9] Tian H,Zhou K,Jiang H,et al. Digital logic based encoding strategies for voice-over-IP steganography [C]//Proc of the 17th ACM Multimedia Conf, Beijing: [s. n.],2009:777-800.

[10] 肖博,黄永峰. 流媒体隐蔽通信系统模型及性能优化[J]. 西安电子科技大学学报: 自然科学版,2008,35(3):554.

[11] 袁键,黄永峰,肖博,等. 基于流媒体的隐蔽通信可靠传输机制的研究[J]. 计算机研究与发展,2009,46(S1):147.

[12] Zŏllner J,Federrath H,Klimant H,et al. Modeling the security of steganographic systems [C]//Proc of the Second Int Workshop on Infor Hiding, Berlin: Springer Press,1998:344-354.

[13] 博森,胡中豫,吴乐华,等. 通信信息隐匿技术[M]. 北京: 国防工业出版社,2005.

[14] Mittelholzer T. An information-theoretic approach to steganography and watermarking [C]//Proc of the 3rd Int Workshop on Information Hiding, Berlin: Springer Press,1999:1-16.

[15] Cachin C. An information-theoretic model for steganography [J]. Infor and Comp,2004,192(1):41.

[16] Sallee P. Model-based methods for steganography and steganalysis [J]. Int J of Image and Graphics,2005,5(1):167.

[17] Zander S, Armitage G, Branch P. Covert channels and countermeasures in computer network protocols [J]. IEEE Com Magazine,2007,45(12):136.