安全性限制下的隐写容量分析*

曹 佳, 刘文芬, 张卫明
(信息工程大学信息工程学院, 河南 郑州 450002)

摘 要: 运用网络信息论中率失真及随机编码等理论对安全性限制下的隐写容量进行了研究, 利用强联合典型序列方法得到了隐写容量的下界, 并在特定条件下给出了隐写容量的上界。研究结果表明: 在没有安全性限制下, 与 Moulin 关于一般信息隐藏系统容量的研究结果一致; 而 Moulin 关于绝对安全条件下的隐写容量分析结果只是在此情形下的特例。此外, 还对当前较流行的一种基于图像的隐写算法——LSB 随机嵌入算法的信息传输率及隐写容量进行了研究, 发现二者之间存在着一定的差距。

关键词: 信息隐藏; 网络信息论; 随机编码; 率失真理论; 隐写术; 隐写容量
中图分类号: TN911.2 文献标识码: A 文章编号: 0529-6579(2004)S2-0164-05

隐写术是信息隐藏的一个重要分支, 它将秘密信息隐藏在其他载体中, 通过载密对象的传输, 实现秘密信息的传递。隐写术的出现改变了传统隐秘通信的旧观念, 它与密码术的主要区别在于密码术旨在隐藏信息的内容, 而隐写术的目的在于隐藏信息的存在。

隐写术的容量, 即隐写容量, 是隐写术理论研究的一个重要问题, 同时也是隐写术应用的一项重要指标。从信息论角度而言, 隐写容量是指载体所能隐藏的最大消息率。Moulin 和 O'Sullivan[1] 在这方面的工作最为突出, 他们建立了信息隐藏系统的通信模型, 从信息论角度研究了一般信息隐藏系统的隐藏容量, 并把研究结果初步应用到隐写术上。而文献 [1] 中假设隐写系统的接收(译码)者已知攻击信道并且假设此信道是无记忆或分块无记忆信道, 因此, Somekh-Baruch 和 Merhav[2] 减弱了上述假设条件, 证明了类似于文献 [1] 中隐藏容量的一般表达式。另一方面, 由于文献 [1] 和 [2] 是在无失真译码前提下对隐藏容量进行研究, 而实际上平均错误译码概率可以大于 0。针对上述信息隐藏系统实际存在的鲁棒性, 伍宏涛[3] 等扩展了文献 [1] 中的结果, 得出了无主动攻击情况下平均错译概率不超过信息隐藏系统的容量。然而, 与一般信息隐藏系统不同, 隐写术对安全性(即不可检测性)有其特殊的要求, 故隐写容量也应具有一定的安全性要求。Cachin[4] 提出用载体与载密对象之间的相对熵来度量隐写系统的安全性, 他定义了安全隐写系统, 这种度量被多篇文献和专著所引用。于是, Moulin 和 Wang[5] 在文献 [1] 和 [4] 的基础上, 得到了 Cachin 定义的绝对安全(即)条件下隐写系统的容量表达式, 这对于隐写容量的研究又推进了一步。此外, 张卫明[6] 等利用载体与载密对象之间的变化距离定义了隐写系统的安全性, 并在此安全性度量下推导出文献 [1] 中隐藏容量与此安全性之间的制约关系。

本文在文献 [1]、[4] 和 [5] 的基础上, 对安全性限制下的隐写容量作进一步的研究。文献 [5] 仅考虑了绝对安全(即 $\varepsilon=1$)条件下的隐写容量, 对于一般 ε-安全($\varepsilon\geqslant 0$)条件下的隐写容量未曾给出相应的研究结果。绝对安全其实是要求载体与载密对象的概率密度相同, 而一般安全却要求载体和载密对象之间的相对熵$\leqslant\varepsilon$($\varepsilon\geqslant 0$), 这无疑大大增加了研究的难度。针对上述问题, 本文运用网络信息论中率失真及随机编码等理论对一般 ε 安全($\varepsilon\geqslant 0$)条件下的隐写容量进行研究, 利用强联合典型序列方法得到了隐写容量的下界, 并在特定条件下给出了隐写容量的上界。在没有安全性限制下, 本文的结果与文献 [1] 中的研究结果一致; 而文献 [5] 的结果仅仅只是我们在绝对安全条件下的特例。此外, 本文还对当前较流行的一种基于图像的隐写算法——LSB 随机嵌入算法的信息传输率及隐写容量进行了研究, 发现二者之间存在着一定的差距。本文所得结论对隐写算法的设计和安全性分析具有一定的指导意义。

* 收稿日期: 2004-09-11
作者简介: 曹佳(1981 年生), 男, 硕士; E-mail: caojia_cj@yahoo.com.cn

1　问题陈述

符号说明：本文用大写字母表示随机变量（如 X），用小写字母表示其实际取值（如 X），用花写字母表示其取值集合（如 X），N 维随机向量用带上标 N 表示（如 $X^N = X_1, X_2, L, X_N$，其取值集合为 X^N）。随机变量 $X \in X$ 的概率密度函数记为 $p_x(x)$，$x \in X$，在不引起混淆的情况下，我们直接用 $p(x)$，$x \in X$ 表示。特定字母 A 和 Q 在本文中用来表示条件概率密度函数。又对于给定的随机变量 X, Y, Z，$H(X)$ 表示 X 的熵，$I(X;Y)$ 表示 X 和 Y 之间的互信息，$I(X;Y|Z$ 表示已知 Z 的条件下，X 和 Y 之间的互信息。下面我们首先对隐写系统进行简要的介绍，隐写系统的通信框图如图 1 所示。

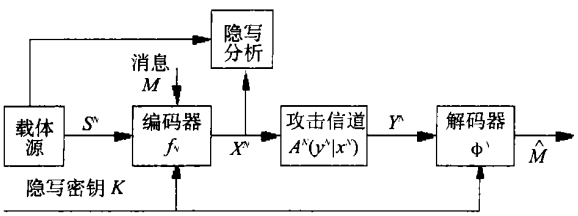

图 1　隐写系统的通信框图

Fig. 1　Communication-theoretic view of steganography

载体源随机发送载体数据

$$S^2 = (S_1, S_2, L, S_N) \in S^N$$

其中，S_1，S_2，L，S_N 独立同分布，且概率密度函数为 $p_s(s)$，$s \in S$。消息源发送消息 M，由于消息在隐藏之前通常需要压缩，因此，可假设消息 M 为消息集 M 上服从均匀分布的随机变量。隐写密钥 K 的概率密度函数为 $p_k(k)$，$k \in K$，且载体 S^N、消息 M、密钥 K 三者相互独立。编码器将载体数据 S^N 和消息 M 通过隐写密钥 K 加密编码成载密数据

$$X^N = f_N(S^N, M, K) \in X^N$$

一般情况下，X^N 和 S^N 之间存在一定的失真。隐写分析者（被动攻击者）会对载密数据进行检测，判断数据中是否藏有秘密信息，故 X^N 需要满足一定的安全性要求。此外，主动攻击者为了避免接收者解码出秘密消息，通常会利用一个攻击信道 $A^N(y^N|x^N)$ 对载密数据 X^N 进行攻击，生成数据 $Y^N \in Y^N$。隐写系统的接收者接收到数据，并通过解码器和隐写密钥 K 将其解码，得到消息的估计值

$$M = \phi_N(Y^N, K) \in M$$

为了分析的方便，不妨假设 $S = X = Y$，且 $|S| < +\infty$。

下面将对隐写容量问题进行数学描述：

定义 1　隐写失真函数定义为一个非负有界函数 $d: S \times X \to R^+ \cup \{0\}$，$N$ 维隐写平均失真函数定义为

$$d^N: S^N \times X^N \to R^U\{0\},$$
$$d^N(s^N, x^N) = \frac{1}{N}\sum_{i=1}^{N} d(s_i, x_i)$$

定义 2　取值于集合上的 2 个概率密度函数 p 和 q 之间的相对熵定义为：

$$D(p \| q) = \sum_{x \in X} p(x) \log \frac{p(x)}{q(x)}$$

其中，约定 $0 \log 0 = 0 \log \frac{0}{0} = 0$，当 $p > 0$ 时，$p \log \frac{p}{0} = +\infty$。

定义 3　满足失真限制 D 的 N 长 ε 安全隐写码定义为一个三元组 (M, f_N, ϕ_N)，其中，

（1）M 是消息集，其势为 $|M|$；

（2）$f_N: S^N \times M \times K \to X^N$ 是编码映射，发送者利用此映射和隐写密钥 k 将秘密消息 m 嵌入到载体 s^N 中，生成载密对象 x^N，并且 f_N 满足如下失真限制：

$$\sum_{s^N \in S^N} \sum_{k \in K} \sum_{m \in M} \frac{1}{|M|} p(s^N) p(k) d^N(s^N, f^N(s^N, m, k)) \leqslant D \quad (1)$$

和安全性限制：

$$\frac{1}{N} D(p_{S^N} \| p_{X^N}) \leqslant \varepsilon \quad (2)$$

（3）$\phi_N: Y^N \times K \to M$ 是解码映射，接收者利用此映射和密钥 k 从 y^N 中提取出消息 $\hat{m} = \phi_N(y^N, k)$。

注 1　由于假设 S^N，M，K 三者相互独立，且 M 服从均匀分布，故

$$p(s^N, m, k) = \frac{1}{|M|} p(s^N) p(k)$$

从而隐写平均失真限制如（1）式；

注 2　Cachin 在文献 [4] 中对于一般随机过程定义了平均安全隐写系统，若

$$\lim_{n \to \infty} \frac{1}{n} D(p_{S^n} \| p_{X^n}) \leqslant \varepsilon$$

则称此系统平均 ε-安全，特别，当 $\varepsilon = 0$ 时，则称此系统平均绝对安全。而对于上述定义的 N 长隐写码，

$$\lim_{n \to \infty} \frac{1}{n} D(p_{S^n} \| p_{X^n}) = \frac{1}{N} D(p_{S^N} \| p_{X^N})$$

故（2）式表明了隐写码的 ε-安全限制。

主动攻击者通常利用某些攻击信道对载密数据 X^N 进行攻击，得到 Y^N，从而使接收者难于从中提取出秘密消息 M。

定义 4 N 维攻击信道定义为 X^N 到 Y^N 上的条件概率密度函数 $A^N(y^N|x^N)$，而主动攻击者可能采用的 N 维攻击信道全体所组成的集合记为 $\mathcal{A}^N$。

由于消息 M 服从均匀分布，故定义 3 中隐写码的码率 $R=\frac{1}{N}\log|M|$，且平均错误译码概率为：

$$P_{e,N}=\frac{1}{|M|}\sum_{m\in M}P\{\phi_N(Y^N,K)\neq m\mid M=m\} \tag{3}$$

定义 5 称率 R 关于失真 D，ε-安全及一类攻击信道 $\{A^N,\ N\geqslant 1\}$ 可达，若存在一列满足失真限制 D 的 N 长 ε-安全隐写码 $(M,\ f_N,\ \phi_N)$，$N\geqslant 1$，其码率为 R，且满足当 $N\to+\infty$ 时，

$$\sup_{A^N\in\mathcal{A}^N}P_{e,N}(A^N)\to 0$$

定义 6 隐写容量 $C^{STEG}(D,\ \varepsilon,\ \{A^N,\ N\geqslant 1\})$ 定义为所有关于失真 D，ε-安全及攻击信道类 $\{A^N,\ N\geqslant 1\}$ 可达率的上确界。

2 隐写容量

为了分析简便，本节假设攻击信道为无记忆信道，这与文献 [1] 中的假设是相符的。

定义 7 满足失真限制 D 的 ε 安全无记忆隐写信道定义为 S 到 $X\times U$ 上的条件概率密度函数 $Q(x,\ u|s)$，且 $Q(x,\ u|s)$ 满足：

$$\sum_{u,\ s,\ x}Q(x,u\mid s)p(s)d(s,x)\leqslant D \tag{4}$$

和

$$D(p_S\|p_X)\leqslant\varepsilon \tag{5}$$

上述信道的 N 维无记忆扩展信道定义为 S^N 到 $X^N\times U^N$ 上的条件概率密度函数 $Q^N(x^N,\ u^N|s^N)$：

$$Q^N(x^N,u^N\mid s^N)=\prod_{i=1}^{N}Q(x_i,u_i\mid s_i) \tag{6}$$

注 定义 7 中 U 为任意有限集，U 为 U 上的一辅助随机变量。

定义 8 集合 Q 定义为所有满足失真限制 D 的 ε-安全无记忆隐写信道全体所组成的集合。

定义 9 无记忆攻击信道定义为 X 到 Y 上的条件概率密度函数 $A(y|x)$，且上述信道的 N 维无记忆扩展信道定义为 X^N 到 Y^N 上的条件概率密度函数 $A^N(y^N|x^N)$：

$$A^N(y^N\mid x^N)=\prod_{i=1}^{N}A(y_i\mid x_i) \tag{7}$$

定义 10 集合 A 定义为主动攻击者可能采用的所有无记忆攻击信道全体所组成的集合。

在分析容量之前，我们首先假设 A 为有限集或紧集，而文献 [1] 中给出的所有满足失真限制的攻击信道全体组成的集合 A 其实也为一紧集，这里我们扩展了文献 [1] 的条件。

引理 1 对于给定的无记忆攻击信道 $A(y|x)$，令隐写信道 $Q(x,\ u|s)\in\mathcal{Q}$，且 $Q(x,\ u|s)$ 使得

$$J(Q,A)=I(U;Y)-I(U;S) \tag{8}$$

在 Q 上取得最大值，即 $J(Q,A)=\max_{Q\in\mathcal{Q}}J(Q,A)$，则对于任意给定的 $\varepsilon_1>0$ 及 $0<\delta\ll\varepsilon$，存在充分大的正整数 N 和一个满足失真限制 $D+\delta$ 的 N 长 $(\varepsilon+\delta)$ 安全隐写码 (M,f_N,ϕ_N)，使得 $P_{e,N}<\varepsilon_1$，且 $|M|\geqslant 2^{N[J(Q,A]-\varepsilon_1}$。

引理 2 设 (M,f_N,ϕ_N) 为一满足失真限制 D 的 N 长 ε-安全隐写码，其码率为 $R=\frac{1}{N}\log|M|$，$A(y|x)$ 为一给定攻击信道，若此隐写码满足条件

$$D(p_{S^N}\|p_{X^N})\geqslant\sum_{i=1}^{N}(p_{S_i}\|p_{X_i})$$

且当 $N\to+\infty$ 时，有 $P_{e,N}\to 0$，则对于任意给定的 $\varepsilon_1>0$，存在有限集 U 及隐写信道 $Q(x,u|s)\in\mathcal{Q}$，使得 $R<J(Q,A)+\varepsilon_1$。

定理 1 假设攻击者已知隐写信道，译码者已知隐写信道和攻击信道，令

$$\underline{C}(D,\varepsilon,A)=\max_{Q\in\mathcal{Q}}\min_{A\in\mathcal{A}}J(Q,A) \tag{9}$$

其中，$J(Q,A)=I(U;Y)-I(U;S)$，U 为定义在任意有限集 U 上的随机变量，且 $(U,S)\to X\to Y$ 形成马氏链，则隐写容量

$$C^{STEG}(D,\varepsilon,\{A^N,N\geqslant 1\})\geqslant\underline{C}(D,\varepsilon,A)$$

当限制隐写码满足条件

$$D(p_{S^N}\|p_{X^N}\geqslant\sum_{i=1}^{N}D(p_{S_i}\|p_{X_i})$$

时，隐写容量

$$C^{STEG}(D,\varepsilon,\{A^N,N\geqslant 1\})\geqslant\underline{C}(D,\varepsilon,A)$$

注 1 由于 $S_1,S_2,\cdots,S_N$ 相互独立，故当 $X_1,X_2,\cdots,X_N$ 相互独立时，有

$$D(p_{S^N}\|p_{X^N}=\sum_{i=1}^{N}D(p_{S_i}\|p_{X_i})$$

又当 $D(p_{S^N}=p_{X^N}$ 时，有

$$D(p_{S^N}\|p_{X^N}=\sum_{i=1}^{N}D(p_{S_i}\|p_{X_i})=0$$

注 2 在没有安全性限制下，定理 1 的结论与文献 [1] 中的研究结果一致，而在绝对安全条件下，结论又与文献 [5] 的结果相符。

定理 2 当 $Y=X$（即不存在主动攻击）时，$\underline{C}(D,\varepsilon)=\max_{Q\in\mathcal{Q}}H(X|S)$，其中，

$$\mathcal{Q}=\{Q(x|s):\sum_{s,x}Q(x|s)p(s)d(s,x)\leqslant D,$$

且 $D(p_s \| p_x) \leqslant \varepsilon\}$

3　LSB 随机嵌入情形

本节将对当前较流行的一种基于图像的隐写算法——LSB 随机嵌入算法的信息传输率及隐写容量进行分析。简而言之，LSB 随机嵌入算法是指在载体图像中随机选取一些像素点，然后用消息比特替换已选取像素点的最低有效比特位（即 LSB 位），从而达到隐藏的目的。下面我们首先对此算法建立简化的概率模型：

设载体序列 $S^{\infty} = \{S_1, S_2, \cdots\}$、消息序列 $M^{\infty} = \{M_1, M_2, \cdots\}$ 和密钥序列 $K^{\infty} = \{K_1, K_2, \cdots\}$ 是 3 条独立随机变量序列，满足

$$P\{S_i = 1\} = 1 - P\{S_i = 0\} = p,$$

$$P\{M_i = 1\} = P\{M_i = 0\} = \frac{1}{2},$$

$$P\{K_i = 1\} = 1 - P\{K_i = 0\} = r,\ i \geqslant 1$$

还假设 S^{∞}, M^{∞} 和 K^{∞} 三者之间也是相互独立的，又记

$$X_i = (1 - K_i)S_i + K_i M \sum_{j=1}^{i} K_j,\ i \geqslant 1$$

则 $X^{\infty} = \{X_1, X_2, \cdots\}$ 表示载密对象序列。

引理 3　$X_1, X_2, \cdots$ 是独立同分布的 0、1 随机变量序列，且

$$P\{X_i = a\} = \frac{r}{2} + (1 - r)P\{S_i = a\},$$

$$a \in \{0, 1\},\ i \geqslant 1$$

引理 4　LSB 随机嵌入算法的平均信息传输率为：

$$R \sum_{k_1, \cdots, k_n = 0\,1} P\{K_1 = k_1, \cdots, K_n = k_n\}$$

$$\frac{1}{n} H\left(M_1, M_2, L, M \sum_{j=1}^{i} K_j\right) = r$$

引理 5　设 d 为汉明失真函数，则平均失真

$$\mathrm{E}[d(S_i, X_i)] = \frac{r}{2},\ i \geqslant 1$$

以下假设失真函数均为汉明失真函数。

定理 3　对于 LSB 随机嵌入算法，其产生的隐写码满足失真限制 D 且绝对安全（即 $\varepsilon = 0$）的充分必要条件是

$$P\{S_i = 0\} = P\{S_i = 1\} = \frac{1}{2},\ i \geqslant 1$$

且当 $D \leqslant \frac{1}{2}$ 时，平均信息传输率 $R \leqslant 2D$。

注　当

$$P\{S_i = 0\} = P\{S_i = 1\} = \frac{1}{2},\ i \geqslant 1$$

时，LSB 随机嵌入算法若满足失真限制 D 且绝对安全，则其最大平均信息传输率 $R_{\max} = 2D$。

定理 4　当

$$P\{S_i = 0\} = P\{S_i = 1\} = \frac{1}{2},\ i \geqslant 1$$

且 $Y = X$（即不存在主动攻击）时，有

$$\underline{C} = \underline{C}(D, \varepsilon = 0) = \begin{cases} H(D) & \text{若 } 0 \leqslant D \leqslant 1/2 \\ 1 & \text{若 } D \geqslant 1/2 \end{cases}$$

注　定理 4 中 $\underline{C}$ 的表达式与文献 [5] 中二元汉明情形下不加安全性限制的容量表达式一致，这说明绝对安全的限制没有降低此情形下的隐写容量。

对上述 $R_{\max}$ 和 $\underline{C}$ 进行比较，如图 2 所示：

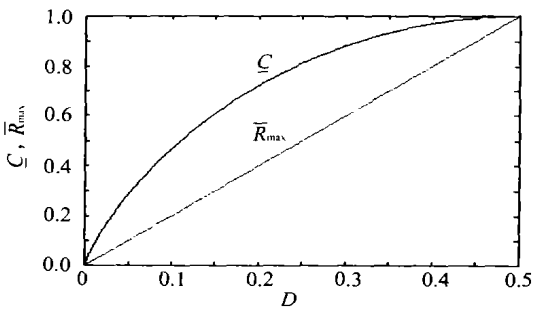

图 2　$R_{\max}$ 与 $\underline{C}$ 之间的差异

Fig 2　Difference between $R_{\max}$ and $\underline{C}$

图 2 说明了 LSB 随机嵌入算法的平均信息传输率与实际隐写容量之间存在一定的差距。LSB 随机嵌入算法的最大平均信息传输率 $R_{\max}$ 随 D 线性增长，而 $\underline{C}$ 随 D 非线性增长，且呈上凸状。

4　结　语

本文研究了安全性限制下的隐写容量。由于隐写术是通过隐藏信息的存在来达到保密通信的目的，故安全性是隐写术的一项重要指标。以往关于隐藏容量的研究中，都没有考虑安全性限制，或仅研究了特殊安全性要求下的容量，这都是不完善的。基于此，本文运用网络信息论中率失真及随机编码等理论对一般 ε-安全（$\varepsilon \geqslant 0$）条件下的隐写容量进行研究，利用强联合典型序列方法得到了隐写容量的下界，并在特定条件下给出了隐写容量的上界。此外，本文还对 LSB 随机嵌入算法的信息传输率及隐写容量进行了研究，发现二者之间存在着一定的差距。本文的研究结果不仅对于隐写术的理论研究具有一定的意义和价值，而且对于隐写算法的设计及安全性分析亦具有一定的指导作用。

研究中仍然存在一些有待解决的问题，例如：不附加特定条件下隐写容量的下界及隐写容量；介

入保密性要求后，隐写容量是否会改变；如何设计切实可行的隐写算法，使其信息传输率达到或接近隐写容量等。这些问题也是我们今后研究的重点。

参考文献：

[1] MOULIN P, O'SULLIVAN J A. Information-theoretic analysis of information hiding[J]. IEEE Trans Inform Theory, 2003, 49(3): 563—593.

[2] SOMEKH-BARUCH A, MERHAV N. On the capacity game of public watermarking systems[J]. IEEE Trans Inform Theory, 2004, 50(3): 511—524.

[3] 伍宏涛, 杨义先, 钮心忻. 改进的信息隐藏的信息论理论模型[J]. 计算机工程与应用, 2004, 6: 34—36.

[4] CACHIN C. An information-theoretic model for steganography //AUCSMITH D. Information Hiding, 2nd International Workshop, Lectures Notes in Computer Science[C]. New York: Springer, 1998, 1525: 306—318. Extended version, 2002 preprint, available at www.zurich.ibm.com/~cca/publications.html.

[5] MOULIN P, WANG Y. New results on steganographic capacity //Proc CISS 2004[C]. Princeton University, 2004: 813—818.

[6] ZHANG W M, LI S Q. Security measures of stegosystems // The Second conference of Applied Cryptography and Network Security, Lectures Notes in Computer Science[C]. New York: Springer, 2004, 3089: 194—204.

[7] COVER T M, THOMAS J A. Elements of information theory [M]. New York: Wiley, 1991.

[8] YAMAMOTO H. Information theory in cryptology[J]. IEICE Trans, 1991, E74(9): 2456—2468.

Analysis of Steganographic Capacity under the Limit of Security

CAO Jia, LIU Wen-fen, ZHANG Wei-ming

(Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China)

Abstract: The steganographic capacity under the limit of security is studied with information-theoretic methods. The lower bound of steganographic capacity is obtained by using the theory of strongly jointly typical sequences and its upper bound on a special condition is also presented. It is shown that our conclusions are same as Moulin's about capacity of information hiding systems without the limit of security and Moulin's result of steganographic capacity on the perfectly secure condition is the special case of ours. Furthermore, the information transfer rate and steganographic capacity about LSB steganographic algorithms are analyzed, and it indicates that there is some difference between them.

Key words: information hiding; network information theory; randomized codes; rate-distortion theory; Steganography; steganographic capacity