基于 K-L 差异的隐密术安全性理论研究

宋　辉[①]　　孔祥维[①]　　尤新刚[①②]
[①](大连理工大学电信学院　大连　116023)
[②](北京电子技术应用研究所　北京　100091)

摘　要：隐密术安全性理论研究一直是被广泛关注的研究重点和难点。该文通过对 K-L 差异的回顾及隐密术安全性的定性分析，指出 Cachin 给出的安全性定义缺乏一般性。同时注意到除概率分布的差异外，隐密信息的样本量和状态集合的势对隐密信息的安全性也有重要影响。结合对隐密信息安全性的定性分析，给出了一个基于 K-L 差异及假设检验的隐密术安全性定义，并推导出修改率对于隐密术安全性的影响。最后结合现有的隐密算法和隐密分析算法设计了一组对比试验，以验证该文理论分析的有效性。

关键词：隐密术；安全性度量；K-L 差异；样本量
中图分类号：TP391　　**文献标识码**：A　　**文章编号**：1009-5896(2010)02-0439-05
DOI: 10.3724/SP.J.1146.2009.00142

The Study of Security in Steganography Based on K-L Divergence

Song Hui[①]　　Kong Xiang-wei[①]　　You Xin-gang[①②]
[①](*School of Electronic and Information Engineering*, *Dalian University of Technology*, *Dalian* 116024, *China*)
[②](*Beijing Institute of Electronic Technology and Application*, *Beijing* 100091, *China*)

Abstract: This paper presents a universality method for measure of security in steganography. According to the definition of K-L divergence and the properties of security in steganography, some limitations in Cachin's definition of security are shown in the beginning. Besides the divergence of probability distributions between stego and cover, the sample size and the cardinality of the state set of random variable have great effect on security in steganography. Based on K-L divergence and hypothesis testing, an amended measure of security and a useful illation are presented. The result of examination can prove that the new measure of security is reasonable.

Key words: Steganography; Measure of security; K-L divergence; Sample size

1　引言

隐密术是一种通过隐藏秘密信息存在性的保密通信技术[1]，隐密术主要以 Simmons 的“囚徒问题”[2]为应用模型进行研究。如图 1 所示，Bob 和 Alice 的通信内容被第三方 Willie 审查。为了躲避审查，Bob 和 Alice 通过有目的地修改多媒体信息中不具有“使用价值”的随机变量来表示秘密信息。图 1 中 m 表示秘密信息，c 表示掩护信息，k 表示共享的密钥，s 表示隐密信息。

安全性和容量问题是隐密术研究中的核心问题。在文献[3–5]中，学者尝试通过度量因嵌入秘密信息而引起失真来描述隐密信息安全性，然后用信道编码理论或博弈论阐述容量问题，同时文献[5]证明了在隐密术中秘密信息具有密码学意义上的安全性。但是上述基于失真理论或密码学意义上的安全性并不是隐密术所最终追求的，对秘密信息存在性的隐藏才是隐密术安全性的独特体现，因此隐密术安全性是指在各种测度下无法区分隐密信息集合与掩护信息集合。文献[6]提出用掩护信息的概率分布 P_C 相对于隐密信息的概率分布 P_S 的 K-L 差异 $D_{KL}(P_C \,||\, P_S)$ 度量隐密系统的安全性。信息的本质是对随机事件的记录，因此从概率描述的角度对信息属性进行区分是必要的。在实际算法设计中往往采用减少修改量的方法在安全性和容量上进行折衷，如 QIM[7]、MM[8]或 PQ[9]等算法，但是理论上缺少修改量与安全性关系的度量。最新的研究[10–12]显示：在同等安全性下，隐密术的容量并非与图像的大小成正比，因此隐密术安全性非仅与 P_S 同 P_C 的差异有关。本文首先介绍 K-L 差异的定义及性质；随后将隐密术安全性的定性分析与 K-L 差异结合，

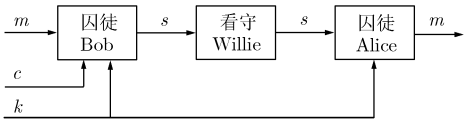

图 1 “囚徒问题”示意图

2009-02-04 收到，2009-07-21 改回
国家自然科学基金(60572111)资助课题
通信作者：宋辉　song8008@mail.com

指出文献[6]中安全性定义缺乏一般性；进而结合K-L 差异的意义和性质，考虑概率度量下的隐密术安全性的特点，将相对样本量纳入到安全性度量中，给出了一种新的隐密术安全性度量方法，并依据新的安全性度量方法推导出相对修改量与安全性的关系；最后为验证本文所提出的安全性度量的合理性，结合现有的隐密算法及隐密分析算法设计出相应的试验，并给出试验结果和相应的分析。

2 K-L 差异的简介

K-L 差异(Kullback-Leibler divergence)是一种重要的概率分布差异的非对称性度量方法。在文献[13]中被提出，$D_{\mathrm{KL}}(P\,||\,Q)$用来度量当用一个依据$Q$分布设计的熵编码器来编码一个来源于$P$分布的样本的平均的比特差异。当$P$和$Q$是离散随机变量的概率分布时，K-L 差异被定义为

$$D_{\mathrm{KL}}(P\,||\,Q)=\sum_i P(i)\log\frac{P(i)}{Q(i)} \tag{1}$$

将式(1)展开可得

$$\begin{aligned}D_{\mathrm{KL}}(P\,||\,Q)&=\sum_i P(i)\log\frac{P(i)}{Q(i)}\\&=\sum_i P(i)(\log Q(i)^{-1}-\log P(i)^{-1})\end{aligned} \tag{2}$$

式(2)中$\log Q(i)^{-1}$的意义是状态i在基于Q分布的熵编码器输出的码长，$\log P(i)^{-1}$的意义是状态i在基于P分布的熵编码器输出的码长，$(\log Q(i)^{-1}-\log P(i)^{-1})$表示状态$i$在此种情况下的编码比特差异，然后对上述编码比特差异在P分布上求编码差异的期望。令$\mathcal{P}$和$\mathcal{Q}$分别表示P和Q的状态空间，由此可知$P(i)>0\ (i\in\mathcal{P})$，$P(i)=0\ (i\notin\mathcal{P})$，对概率分布$Q$也有同样的结果。将式(1)按照$P$和$Q$的概率分布的状态空间展开可得

$$\begin{aligned}D_{\mathrm{KL}}(P\,||\,Q)&=\sum_i P(i)\log\frac{P(i)}{Q(i)}=\sum_{i\in\mathcal{P}\cup\mathcal{Q}}P(i)\log\frac{P(i)}{Q(i)}\\&=\sum_{i\in\mathcal{P}\cap\mathcal{Q}}P(i)\log\frac{P(i)}{Q(i)}+\sum_{i\in\overline{\mathcal{P}}\cap\mathcal{Q}}P(i)\log\frac{P(i)}{Q(i)}\\&\quad+\sum_{i\in\mathcal{P}\cap\overline{\mathcal{Q}}}P(i)\log\frac{P(i)}{Q(i)}=\sum_{i\in\mathcal{P}\cap\mathcal{Q}}P(i)\log\frac{P(i)}{Q(i)}\\&\quad+\sum_{i\in\overline{\mathcal{P}}\cap\mathcal{Q}}0\log\frac{0}{Q(i)}+\sum_{i\in\mathcal{P}\cap\overline{\mathcal{Q}}}P(i)\log\frac{P(i)}{0}\\&=\sum_{i\in\mathcal{P}\cap\mathcal{Q}}P(i)\log\frac{P(i)}{Q(i)}+\sum_{i\in\overline{\mathcal{P}}\cap\mathcal{Q}}0+\sum_{i\in\mathcal{P}\cap\overline{\mathcal{Q}}}+\infty\end{aligned} \tag{3}$$

在式(3)中，$i\in\mathcal{P}\cap\mathcal{Q}$表示对于$P$和$Q$都存在的状态，这部分编码差异有上界；$i\in\overline{\mathcal{P}}\cap\mathcal{Q}$表示对于$P$中不存在的状态但在基于$Q$分布的编码器中存在的状态，这部分对于编码差异的表面贡献为 0，但因为$\sum_{i\in\mathcal{Q}}Q(i)=1$，当$\overline{\mathcal{P}}\cap\mathcal{Q}\neq\phi$时，$\sum_{i\in\mathcal{P}\cap\mathcal{Q}}Q(i)<1$，这使$\mathcal{P}\cap\mathcal{Q}$上的编码差异的下界增加，因此这部分对整体编码差异也有直接影响；$i\in\mathcal{P}\cap\overline{\mathcal{Q}}$表示$P$分布中存在但基于$Q$分布的编码器不能表示的状态，此时编码器将失效，因此编码差异为无穷大。由上述分析可以看出，K-L 差异对于描述编码比特差异问题具有一般性，不会因为状态空间的差异而失效。

$D_{\mathrm{KL}}(P\,||\,Q)$在表示用$Q$分布代替真实的$P$分布进行编码时的编码差异时，也被称为相对熵(relative entropy)。同时$D_{\mathrm{KL}}(P\,||\,Q)$也被称为用$P$分布代替实际$Q$分布时的信息获得(information gain)。因此应用 K-L 差异度量非对称差异时，在不同应用环境下需要谨慎考虑P和Q的含义。K-L 差异对于任意的概率分布P_1、P_2、Q_1和Q_2都有如下的性质：

$$D_{\mathrm{KL}}(P_1\,||\,Q_1)\neq D_{\mathrm{KL}}(Q_1\,||\,P_1),\ P_1\neq Q_1 \tag{4a}$$

$$D_{\mathrm{KL}}(P_1\,||\,Q_1)\geq 0,\text{当且仅当}P_1=Q_1\text{时取等号} \tag{4b}$$

$$\begin{aligned}D_{\mathrm{KL}}(\lambda P_1+(1-\lambda)P_2\,||\,Q_1)&\leq\lambda D_{\mathrm{KL}}(P_1\,||\,Q_1)\\&\quad+(1-\lambda)D_{\mathrm{KL}}(P_2\,||\,Q_1)\end{aligned} \tag{4c}$$

$$\begin{aligned}D_{\mathrm{KL}}(P_1\,||\,\lambda Q_1+(1-\lambda)Q_2)&\leq\lambda D_{\mathrm{KL}}(P_1\,||\,Q_1)\\&\quad+(1-\lambda)D_{\mathrm{KL}}(P_1\,||\,Q_2)\end{aligned} \tag{4d}$$

式(4a)表示 K-L 差异的非对称性，由于不满足对称性，并且也不满足三角不等式，因此 K-L 差异不应该不认为是一种“距离”；式(4b)表示 K-L 差异的非负性；式(4c)和(4d)表示 K-L 差异对于两个变量都是凸函数。这些性质为研究隐密系统的安全性提供了很好的工具。

3 基于 K-L 差异的隐密术安全性分析

隐密术的安全性的度量包含两个层次：逻辑关系的验证和统计关系的检验。前者针对信息记录中各种已知的逻辑关系进行验证以鉴别样本的属性；后者针对信息记录中独立同分布的随机变量进行假设检验，接受较大置信度的假设，拒绝较小置信度假设，本文将针对统计关系的检验进行讨论。本节首先对基于统计关系验证的隐密术安全性问题进行定性的分析，然后结合定性分析结果阐述文献[6]中安全性定义不具备一般性的原因，最后结合定性分析结果和 K-L 差异给出隐密术安全性的度量定义并做进一步有意义的推导。

3.1 隐密术安全性的定性分析

设掩护信息中的独立随机变量X服从概率分布P_C，其状态集合为$\mathcal{C}$，掩护信息经过隐密算法得到隐密信息，隐密信息中独立随机变量X服从概率分

布 P_S，其状态集合为 $\mathcal{S}$。隐密术中探讨样本量为 n 的隐密信息样本 $\boldsymbol{x}=(x_1,\cdots,x_n)\sim P_S$ 的安全性问题等价于检验假设：$H_0:\boldsymbol{x}=(x_1,\cdots,x_n)\sim P_C$ 的置信度。首先根据 $\boldsymbol{x}$ 确定其状态集合 $\mathcal{X}$（$\mathcal{X}\subseteq\mathcal{S}$），此时需要对 $\mathcal{X}$ 是否属于 $\mathcal{C}$ 进行验证，如果 $\mathcal{X}\not\subset\mathcal{C}$ 则接受 H_0 的置信度为 0。如果 $\mathcal{X}\subseteq\mathcal{C}$，首先统计样本的 k 阶经验分布 $P_{\boldsymbol{x}}^k$，然后判断 $P_{\boldsymbol{x}}^k$ 与掩护信息的 k 阶联合分布 P_C^k 的差异在该样本量下的置信度。值得注意的是：对于 k 阶联合分布，实际有效样本量会减小到 $\lfloor n/k\rfloor$（$\lfloor\bullet\rfloor$ 表示向下取整），同时 k 阶联合分布的状态集合的势与 k 呈幂级数关系为 $|\mathcal{X}^k|=|\mathcal{X}|^k$，此时检验的置信度随 k 的增加而迅速下降，因此对于有限样本量只具有判断有限阶联合分布的能力。当样本量为 n 无限大时，根据 Borel 强大数率对于任意 k 阶联合分布都有：$\lim\limits_{n\to\infty}P(P_{\boldsymbol{x}}^k=P_S^k)=1$，因此当样本量趋近于无穷时当且仅当 $P_{\boldsymbol{x}}^k=P_C^k$ 才能接受假设 H_0。基于上述分析，可以得到如下的结论：

(1)当 $\mathcal{S}\not\subset\mathcal{C}$ 时，隐密系统是绝对不安全的，此时概率分布差异应为无穷大；

(2)当 $\mathcal{S}\subseteq\mathcal{C}$ 时，隐密系统的安全性取决于样本量 n 以及概率分布差异，且概率分布差异只能起有限作用，即当 $\mathcal{S}\subseteq\mathcal{C}$ 时概率差异的度量有上界；

(3)当样本量 n 有限时，只能度量有限阶联合分布的差异；

(4)当 $n\to+\infty$ 时，当且仅当对于任意的 k 都有 $P_{\boldsymbol{x}}^k=P_C^k$ 时，隐密信息才是安全的。

由上述结论可知，隐密术安全性与样本量、状态集合的势以及概率分布的差异都有关系，并且在隐密术安全性研究中，掩护信息与隐密信息的概率分布差异度量需要满足非对称性。

3.2 对 Cachin 隐密安全性定义的分析

文献[6]给出了一个基于 K-L 差异的隐密系统的安全性定义：当 $D_{\mathrm{KL}}(P_C\,||\,P_S)=0$ 时，隐密系统是绝对安全的；当 $D_{\mathrm{KL}}(P_C\,||\,P_S)\le\varepsilon$ 时，隐密系统是 ε 级安全的，其中 P_C 和 P_S 分别代表掩护信息和隐密信息中独立同分布随机变量的概率分布，其中 P_C 和 P_S 分别定义在状态集合 $\mathcal{C}$ 和 $\mathcal{S}$ 上。如果将这一定义用如同式(3)的形式展开可得

$$\begin{aligned}D_{\mathrm{KL}}(P_C\,||\,P_S)&=\sum_i P_C(i)\log\frac{P_C(i)}{P_S(i)}\\&=\sum_{i\in\mathcal{C}\cap\mathcal{S}}P_C(i)\log\frac{P_C(i)}{P_S(i)}+\sum_{i\in\overline{\mathcal{C}}\cap\mathcal{S}}0\log\frac{0}{P_S(i)}\\&\quad+\sum_{i\in\mathcal{C}\cap\overline{\mathcal{S}}}P_C(i)\log\frac{P_C(i)}{0}\\&=\sum_{i\in\mathcal{C}_C\cap\mathcal{S}}P_C(i)\log\frac{P_C(i)}{P_S(i)}+\sum_{i\in\overline{\mathcal{C}}\cap\mathcal{S}}0+\sum_{i\in\mathcal{C}\cap\overline{\mathcal{S}}}+\infty\end{aligned}\quad(5)$$

当 $\mathcal{S}=\mathcal{C}$ 时，由于 K-L 差异是定义域上的凸函数，且在 $P_C=P_S$ 时取得最小值，此时文献[6]给出的定义基本上可以适用于安全性描述。但是容易证明对于任意给定的 P_C，以定义在 $\mathcal{S}=\mathcal{C}$ 上的 P_S 为变量的 $D_{\mathrm{KL}}(P_C\,||\,P_S)$ 是无上界的，即存在 P_S 相对于给定的 P_C 是绝对不安全的，这与定性分析的结论(2)不符，因为此时隐密信息的安全性与样本量有密切关系。当时 $\mathcal{S}\ne\mathcal{C}$，可以发现文献[6]给出的安全性定义与安全性的定性分析相悖。$\mathcal{C}\cap\overline{\mathcal{S}}$ 部分对安全性的影响取决于样本量，小样本量下该部分对安全性的负面影响十分有限，但是在式(5)中该部分的影响总是无穷大；$\overline{\mathcal{C}}\cap\mathcal{S}$ 部分对安全性的影响是显著的，一旦 $\overline{\mathcal{C}}\cap\mathcal{S}$ 不是空集，隐密系统是绝对不安全的，但是在式(5)中该部分对安全性度量的直接影响是 0，这都与上一节给出的隐密术安全性定性分析不符。因此可知文献[6]中的定义不具有一般性。

3.3 基于 K-L 差异的隐密术安全性度量

依据上文的分析，影响隐密术安全性的因素有：样本量 n、掩护信息状态集合的势 $|\mathcal{C}|$ 和隐密信息与掩护信息的概率分布的差异的非对称度量。隐密信息的安全性会随着 P_C 与 P_S 的差异越大而变差；样本量 n 相对于掩护信息状态集合的势 $|\mathcal{C}|$ 的值越大，相同概率差异的情况下，隐密术的安全性越差；相同概率差异的情况下，掩护信息的熵越大，同等条件下隐密术的安全性越高。隐密信息安全性度量可以分如下几个步骤：

(1)度量单个状态的概率差异对安全性的影响 $d(i)=f(P_S(i)\,||\,P_C(i))$；

(2)求隐密信息中各状态的概率差异对安全性影响的期望 $E(d)=\sum\limits_{i\in\mathcal{S}}P_S(i)d(i)$；

(3)用掩护信息的熵对差异度量的期望进行归一化，得到归一化的差异度量(Normalized Measure of Divergence，NMoD) $\mathrm{NMoD}=E(d)/H(P_C)$；

(4) $g(n,|\mathcal{C}|)$ 描述势为 $|\mathcal{C}|$ 的状态集合当样本量为 n 时，概率估计的相对准确度；

(5) $g(n,|\mathcal{C}|)$ 乘以 NMoD，得到隐密信息的安全性度量(Measure of Security，MoS)，即 $\mathrm{MoS}=g(n,|\mathcal{C}|)\times\mathrm{NMoD}$。

考虑到用安全性度量的非交换性，尤其是状态集合上表现出的非交换性，如果令步骤(1)中的 $f(P_S(i)\,||\,P_C(i))=\log(P_S(i)/P_C(i))=\log P_S(i)-\log P_C(i)$，即用同一状态在两个不同分布中的信息量的差异衡量这个状态对于安全性的影响。此时求 $d(i)$ 在 P_S 上的期望则有 $E(d)=\sum P_S(i)\log(P_S(i)/P_C(i))=D_{\mathrm{KL}}(P_S\,||\,P_C)$。

令 $g(n,|\mathcal{C}|)=\dfrac{\log(n+1)}{\log|\mathcal{C}|}=\log_{|\mathcal{C}|}(n+1)$，对于 k 阶联合分布则有 $g_k(n,|\mathcal{C}|)=g(n/k,|\mathcal{C}^k|)$，需要说明的是这只是一个满足需要的近似描述。$g_k(n,|\mathcal{C}|)=\log_{|\mathcal{C}^k|}(n/k+1)$ 是 n 的增函数，表明样本量越大差异的置信度越高；$g(0,|\mathcal{C}|)=0$，说明样本量为 0 时不存在安全问题；当 $1\le n/k<|\mathcal{C}^k|$ 时，$|\mathcal{X}|\le|\mathcal{C}|$ 导致差异的度量的准确性很低，因此 $0<g(n/k,|\mathcal{C}^k|)\le 1$ 是合理的；当 $n\to\infty$ 时，根据 Borel 强大数律可以得到准确的概率分布，此时概率分布差异的度量是绝对可信的，因此 $g(\infty,|\mathcal{C}^k|)=\infty$ 也是合理的；同时 $g(n,|\mathcal{C}|)=\log_{|\mathcal{C}|}(n+1)$ 对于 $|\mathcal{C}|$ 和 k 是减函数，因为对于 k 阶联合分布，样本量递减会为 $\lfloor n/k\rfloor$，同时状态集合的势增长为 $|\mathcal{C}^k|=|\mathcal{C}|^k$，对于有限样本必然使概率估计得准确度下降，导致差异度量的准确度下降，因此对于有限样本量只能度量有限阶联合分布的差异。因此 $g(n,|\mathcal{C}|)=\log(n+1)/\log(|\mathcal{C}|)$ 是一种满足需求的近似表示。基于上述分析，本文对隐密术安全性作如下定义：

隐密术安全性定义 当 $\log_{|\mathcal{C}^k|}\left(\dfrac{n}{k}+1\right)\times\dfrac{D_{\mathrm{KL}}(P_{S^k}\,||\,P_{C^k})}{H(P_{C^k})}\le\varepsilon$ 时，则该隐密系统对于样本量 n 在 k 阶联合分布下具有 ε 级安全性。当且仅当 $\varepsilon=0$ 时，隐密系统是在此情况下是绝对安全的。

下面将应用所给出的隐密术安全性定义分析修改率对于隐密信息安全性的影响。当相对修改率为 $\lambda\in[0,1]$ 时，用 P_λ 表示此时样本的概率分布。若采用的是均匀修改方式，则 $P_\lambda=\lambda P_S+(1-\lambda)P_C$，其状态空间为 $\mathcal{C}\cup\mathcal{S}$。当样本量保持不变时，只有归一化的 k 阶 K-L 差异影响隐密信息的安全性。如果认为样本值之间是独立的，即放弃独立性检验，那么可以推导出 k 阶联合概率分布。则有

$$\frac{D_{\mathrm{KL}}(P_\lambda^k\,||\,P_C^k)}{H(P_C^k)}=\frac{D_{\mathrm{KL}}(P_\lambda\,||\,P_C)}{H(P_C)}\tag{6}$$

对于固定的掩护信息类型 $H(P_C)$ 保持不变，此时唯一影响安全性的因素是 $D_{\mathrm{KL}}(P_\lambda\,||\,P_C)$。将 $P_\lambda=\lambda P_S+(1-\lambda)P_C$ 代入 K-L 差异的定义式可得

$$\begin{aligned}D_{\mathrm{KL}}(P_\lambda\,||\,P_C)&=\sum_{i\in\mathcal{S}\cup\mathcal{C}}P_\lambda(i)\log\frac{P_\lambda(i)}{P_C(i)}\\&=\sum_{i\in\mathcal{S}\cup\mathcal{C}}(\lambda P_S(i)+(1-\lambda)P_C(i))\\&\quad\cdot\log\frac{\lambda P_S(i)+(1-\lambda)P_C(i)}{P_C(i)}\end{aligned}\tag{7}$$

将式(7)对 λ 求导可得

$$\frac{dD_{\mathrm{KL}}(P_\lambda\,||\,P_C)}{d\lambda}=\frac{D_{\mathrm{KL}}(P_\lambda\,||\,P_C)}{\lambda}+\frac{D_{\mathrm{KL}}(P_C\,||\,P_\lambda)}{\lambda}\tag{8}$$

因为 K-L 差异的非负性，因此可得

$$\frac{dD_{\mathrm{KL}}(P_\lambda\,||\,P_C)}{d\lambda}=\frac{D_{\mathrm{KL}}(P_\lambda\,||\,P_C)}{\lambda}+\frac{D_{\mathrm{KL}}(P_C\,||\,P_\lambda)}{\lambda}\ge 0\tag{9}$$

并根据 K-L 差异是凸函数的性质可得

$$\begin{aligned}\frac{dD_{\mathrm{KL}}(P_\lambda\,||\,P_C)}{d\lambda}&=\frac{D_{\mathrm{KL}}(P_\lambda\,||\,P_C)}{\lambda}+\frac{D_{\mathrm{KL}}(P_C\,||\,P_\lambda)}{\lambda}\\&\le\frac{\lambda D_{\mathrm{KL}}(P_S\,||\,P_C)+(1-\lambda)D_{\mathrm{KL}}(P_S\,||\,P_C)}{\lambda}\\&\quad+\frac{\lambda D_{\mathrm{KL}}(P_C\,||\,P_S)+(1-\lambda)D_{\mathrm{KL}}(P_C\,||\,P_C)}{\lambda}\\&=D_{\mathrm{KL}}(P_S\,||\,P_C)+D_{\mathrm{KL}}(P_C\,||\,P_S)\end{aligned}\tag{10}$$

根据式(8)的结果，对 $D_{\mathrm{KL}}(P_\lambda\,||\,P_C)$ 求 λ 的二阶导可得

$$\frac{d^2D_{\mathrm{KL}}(P_\lambda\,||\,P_C)}{d\lambda^2}=\sum_{i\in\mathcal{S}\cup\mathcal{C}}\frac{(P_S(i)-P_C(i))^2}{\lambda P_S(i)+(1-\lambda)P_C(i)}\ge 0\tag{11}$$

由上述推导可知：在其它条件保持不变的情况下，当隐密算法使 $P_S\ne P_C$ 时，由式(9)和式(11)可知 $D_{\mathrm{KL}}(P_\lambda\,||\,P_C)$ 对于 λ 的一阶导数和二阶导数均大于零，这意味着随着 λ 的增加，隐密信息的安全性将加速下降。并且根据式(10)可知，$D_{\mathrm{KL}}(P_\lambda\,||\,P_C)$ 对于 λ 得一阶导数的上界是 $D_{\mathrm{KL}}(P_S\,||\,P_C)+D_{\mathrm{KL}}(P_C\,||\,P_S)$。由此当隐密算法不能保证 $P_S=P_C$ 时，保证 P_S 尽量接近 P_C 会获得更大的相对修改量。

4 实验分析与讨论

本文主要研究的是保持概率分布对于隐密信息安全性的影响，因此本文选择隐密算法 MB 与 JSteg 算法进行同等状况下的安全性比较。从隐密算法原理上看，MB 算法与 JSteg 算法在改动量化后 DCT 系数时采用的是相同的方法，但是 MB 算法在嵌入过程中保持了一阶直方图的不变性，虽然对于图像来说保持一阶直方图并不等于保持概率分布，但是二者同等条件下的安全性比较是能够反映保持概率分布对隐密算法安全性的影响的。

本文采用文献[14]给出的 JPEG 图像隐密分析方法作为标准，比较两个隐密算法在不同改动率以及不同图像尺寸下的安全性。根据公开发表的文献及对比试验显示，文献[12]给出的这种隐密分析算法性能在目前是最优的，因此基于这种隐密分析方法的安全性比较具有很强说服力的。

本试验采用 1000 幅来自 Sony F828 相机拍摄的自然图像作为试验数据，用裁减的方法得到不同尺寸的图像，在裁减过程中保持压缩质量及 DCT 系数 8×8 块的不变性。分别用上述两种隐密方法，在修改量为 5%nac(nac: non-zero AC DCT coefficient，即非零交流 DCT 系数)，10%nac，

15%nac 和 20%nac 4 种修改率生成隐密图像。这里采用修改率而非一般采用的嵌入率作为衡量标准，是为了验证修改率、图像尺寸及保持部分概率分布对安全性的影响。对上述来源图像每组分别采用 500 幅原始图像和 500 幅隐密图像作为训练样本，对剩下的 1000 幅图像进行分类并记录结果，随后重新随机挑选训练样本和测试样本重复上述试验，如此反复共 4 次得到平均正确率。两种算法在对应情况下的分类情况如表 1 和表 2 所示。

表 1 MB 算法在不同情况下的分类正确率(%)

	128×128	256×256	512×512	1280×960
5%nac	50.8	51.0	51.7	52.8
10%nac	51.0	53.3	59.7	67.2
15%nac	51.5	55.1	62.1	72.7
20%nac	52.7	57.9	65.5	76.3

表 2 JSteg 算法在不同情况下的分类正确率(%)

	128×128	256×256	512×512	1280×960
5%nac	51.1	52.4	56.8	65.3
10%nac	51.4	57.2	67.3	79.1
15%nac	52.7	59.3	71.1	81.5
20%nac	55.7	61.4	75.3	85.5

对表 1 和表 2 的结果进行比较可知，两种算法的安全性都随图像尺寸的增加而变差，随嵌入量的增加而变差，且同等情况下 MB 算法的安全性要高于 JSteg 算法。因此可知，本文的理论分析与实际情况相符。

5　结论

本文通过对 K-L 差异的回顾和对隐密信息安全性的定性分析，指出文献[6]中基于 K-L 差异的安全性度量缺乏一般性的问题。随后将样本量、状态集合的势以及概率分布的差异引入到隐密术安全性度量中，给出基于 K-L 差异的一般性的隐密术安全性度量定义。随后根据本文给出的隐密术安全性度量定义进行了一些有意义的推导，指出对于不能够保持概率分布的隐密算法，随着相对修改量的增加隐密信息的安全性会加速下降。最后设计了相应的试验对本文的理论分析加以验证。

参 考 文 献

[1] 尤新刚, 周琳娜, 郭云彪. 信息隐藏学科的主要分支及术语[C]. CIHW2001, 西安, 2001: 43–50.
You Xin-gang, Zhou Lin-na, and Guo Yun-biao. The main offshoots and terminology in information hiding [C]. CIHW2001, Xi'an, 2001: 43–50.

[2] Simmons G J. The prisoners' problem and the subliminal channel[C]. IEEE Workshop Communications Security CRYPTO, New York, 1983: 51–67.

[3] Ettinger J M. Steganalysis and game equilibria[C]. Information Hiding 1998, Oregon, USA, LNCS, 1998, 1525: 319–328.

[4] Mittelholzer T. An information-theoretic approach to steganography and watermarking[C]. Information Hiding, Dresden, Germany, LNCS, 1999, 1768: 1–16.

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

[6] Cachin C. An information-theoretic model for steganography[C]. Information Hiding 1998, Oregon, USA, LNCS, 1998, 1525: 306–318.

[7] Chen B and Wornell G. Quantization index modulation: A class of provably good method watermarking and information embedding[J]. *IEEE Transactions on Information Theory*, 2001, 48(4): 1423–1443.

[8] Kim Y, Duric Z, and Richards D. Modified matrix encoding technique for minimal distortion steganography[C]. Information Hiding 2006, VA, USA, LNCS, 2006, 4437: 314–327.

[9] Fridrich J, Pevny T, and Kodovsky K. Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities[C]. The 9th Workshop on Multimedia & Security, Dallas, Texas, USA, 2007: 3–14.

[10] Ker A. A capacity result for batch steganograph [J]. *IEEE Signal Processing Letters*, 2007, 14(8): 525–528.

[11] Ker A, Pevny T, and Kodovsky J, *et al*.. The square root law of steganographic capacity[C]. MM&Sec '08, Oxford, UK, 2008: 107–116.

[12] Pevny T and Fridrich J. Benchmarking for steganography[C]. Information Hiding 2008, Santa Barbara, CA, USA, 2008: 251–267.

[13] Leibler K. On information and sufficiency[J]. *Annals of Mathematical Statistics*, 1951, 22(1): 79–86.

[14] Pevny T and Fridrich J. Merging markov and DCT features for multi-class JPEG steganalysis[C]. Security, Steganography and Watermarking of Multimedia Contents IX, San Jose, CA, 2007: 6505.

宋　辉：男，1980 年生，博士生，研究方向为隐密术、多媒体信息安全.

孔祥维：女，1963 年生，教授，博士生导师，研究方向为多媒体信息安全、统计图像处理与模式识别.

尤新刚：男，1963 年生，研究员，天津大学博士生导师，大连理工大学兼职教授，研究方向为多媒体通信、信息安全.