特征保持隐写的博弈分析

高瞻瞻 汤光明 张伟伟

(解放军信息工程大学 郑州 450001)

摘 要 为了分析基于统计特征保持的隐写算法的安全性,将隐写对抗分为以特征子集作为策略和以隐写、隐写分析算法作为策略两种情况建立了两种隐写博弈模型。模型将隐写分析方的检测率作为支付函数,用隐写对抗双方特征子集间的差异反映算法抗统计分析的能力。通过对模型进行均衡分析,给出了各种情况下基于统计特征保持的方式提高隐写系统安全性的最优策略,并得到了均衡局势下的期望支付。

关键词 隐写,统计特征保持,博弈分析,安全性

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.07.043

Game Analysis on Statistical Characteristics Preserving Steganography

GAO Zhan-zhan TANG Guang-ming ZHANG Wei-wei

(PLA Information Engineering University, Zhengzhou 450001, China)

Abstract In order to analyze security of statistical characteristics preserving steganography, two game models were established. They are different in strategies. One takes feature subsets as its strategies while the other's strategies are steganography or steganalysis algorithms. In these two game models, payoff is the detection rate of steganalysis, and the divergence between feature subsets of two confrontation sides is used to reflect steganography algorithm's ability to resist statistical analysis. By equilibrium analysis on the models, optimal strategies to improve steganography system security were given in each case, and the expected payoff in equilibrium situations was also proposed.

Keywords Steganography, Statistical characteristics preserving, Game analysis, Security

1 引言

信息隐藏是互联网时代信息安全领域的重要研究内容之一,数字隐写和隐写分析是信息隐藏两个相互促进、共同发展的方向[1]。近年来,隐写分析技术特别是通用盲检测技术的发展对隐写算法的统计安全性提出了更高的要求。但是,目前基于图像统计特征的隐写往往仅考虑图像某一方面的特征而忽略其他特征,这使其安全性无法得到保证。如 Agaian[2] 提出的方法和 Lou 等[3] 提出的基于局部复杂度的自适应隐写算法虽然能够抵御针对一阶直方图的攻击,但高阶统计失真明显。张湛等[4] 基于隐写编码和图像 Markov 链模型的隐写方法也只做到了二阶统计特性的保持。此外,文献[5]利用 DCT 系数块内块间相关性设计失真函数,基于编码嵌入机制设计的隐写算法针对的也只是 CC-PEV 特征隐写检测方法。

关于特征保持隐写算法安全性,已有文献从实验的角度进行了探讨。文献[6]指出,按照某一模型过度优化的自适应隐写虽然可以有效抵抗该模型范围内的特征检测,但攻击者采用模型外的特征就可能得到非常准确的检测方法。文献[7]则表明,目前对于各类检测普适能力较强的 JPEG 隐写方法依然是早期的非自适应隐写方法 nsF5[8]。

博弈论可以很好地描述隐写与隐写分析动态对抗的过程。刘春庆等[9] 以隐写和隐写分析算法作为隐写双方的策略,以二人零和对策建立了对抗模型。文献[10]提出用期望安全数据传输率作为支付函数建立隐写博弈模型。Schottle 等[11] 则利用博弈论研究了基于图像复杂度的自适应隐写如何选择嵌入位置的问题。这些研究普遍局限于隐写博弈的理论建模,虽然理论价值高,但对隐写算法的设计指导性不强。

本文在以上博弈隐写研究的基础上,依据不同的策略类型建立了两种针对特征保持隐写的博弈模型。基于这些模型研究了特征保持隐写的安全性,探讨了提高隐写算法的安全性的方式,所得结论对特征保持隐写算法的设计和应用具有一定参考意义。

2 博弈问题描述

目前,隐写分析领域以通用盲检测技术的研究为主。通用隐写分析方法认为秘密信息的嵌入必然引起载体轻微的改动,图像的空域统计特性、频域统计特性、像素的空间相关性等都可能发生不同程度的变化[12]。基于这些变化的统计特性,通用隐写分析方法将隐写分析归结为模式识别中的二元分类问题,从而实现对载密体的正确区分。

针对这一现状,隐写方提出了统计特征保持的隐写思想,即将特定统计特征的变化限制在较小的范围内,从而使通用

到稿日期:2013-09-07 返修日期:2013-12-22 本文受国家自然科学基金项目(61101112),河南省科技攻关项目(122102210047)资助。

高瞻瞻(1988—),男,硕士生,主要研究方向为信息隐藏,E-mail:gaozhandyx@126.com;汤光明(1963—),女,博士,教授,主要研究方向为图像处理、信息隐藏等;张伟伟(1989—),男,硕士生,主要研究方向为图像识别等。

隐秘分析无所作为。在这一过程中，隐写方的目标是尽可能地降低被发现的概率，而分析方的目标则是尽可能多地发现并阻止秘密信息的传送。双方的利益完全对立，隐写方的支付就是分析方的收益，其行为符合二人零和博弈问题。

现实中隐写双方的对抗较为复杂，本文将其简化为两种基本情况。在此基础上分别建立博弈模型，以实现对特征保持隐写算法的安全性分析。

3 以特征子集作为策略的博弈模型

3.1 博弈双方的策略

在第一种对抗情况下，考虑隐写方仅使用统计特征保持的隐写方法，分析方也仅使用基于统计特性的盲检测方法。此时双方进行博弈时需要确定的仅是具体选择哪些特征来进行保持或检测。

用于隐写分析的特征多种多样，常见的有：图像质量指标(IQM)、子带系数的高阶 PDF 矩、直方图统计特征、子带直方图的 CF 矩、关于经验矩阵及共生矩阵的统计分析、SPAM 特征[13]等等。所有这些特征共同构成集合 Z^n，它是隐写双方特征选择的空间，属于博弈双方共享的知识。

对于隐写方，其策略是先从 Z^n 中选择一个 m_a 维的特征子集，然后在嵌入秘密信息的过程中保持该集合内的特征不变或仅发生无法分辨的变化。相似地，隐写分析方的策略是从 Z^n 中选择 m_c 个统计特征用于检测。根据 Kerckhoffs 原则，隐秘通信系统不对算法保密，因此在接下来的论述中认为隐写对抗双方了解对方选择的策略，即选择了哪个特征子集。

3.2 博弈模型的建立

固定隐写对抗双方特征子集的大小 m_a、m_c，则隐写方的策略共有 $C_n^{m_a}$ 个，记此时隐写方的策略集为 $A=\{A_1,A_2,\cdots,A_{C_n^{m_a}}\}$；相应地，攻击方的策略集为 $C=\{C_1,C_2,\cdots,C_{C_n^{m_c}}\}$。隐写双方的零和博弈模型可以表示为：

$$G=(A,C,Q) \tag{1}$$

式中，Q 为隐写者的支付矩阵，这是一个 $C_n^{m_a}\times C_n^{m_c}$ 的矩阵。Q 中元素 q_{ij} 表示在博弈局势 (A_i,C_j) 下分析方检测成功的概率。

定义 1 称两个特征子集 A_i、C_j 中相同元素的个数为两集合的关联度 k，$k=g(A_i,C_j)=|A_i\cap C_j|$。

现实中，检测算法特征子集内各个特征对特定隐写算法检测成功的贡献不尽相同。早期的通用隐写检测算法总是尽量寻找最有效的那些特征来实施检测，但这些算法往往只对个别隐写算法有较好的检测表现，在应用时有很大局限；最近提出的 SRM、PSRM 等检测方法说明特征集维数的增大更有利于隐写的判断。因此，对于一般的隐写算法，具体特征对检测概率的影响可以忽略。进一步地，可以认为隐写对抗双方所选子集的差异程度唯一衡量了隐写检测成功的概率，即认为 q_{ij} 的取值仅与 A_i、C_j 间的关联度 k 有关。故有

$$q_{ij}=f(k)=f(g(A_i,C_j)) \tag{2}$$

$f(k)$ 应有如下性质：(1)当 $k=0$ 时，隐写对抗双方特征子集间的关联度最小，这有利于分析方成功实施样本检测，故此时 $f(k)$ 取最大值；(2)随着 k 的增大，隐写检测的特征子集越来越多地与隐写方所保持的特征相重合，所以检测成功的概率将不断下降。

因此，$f(k)$ 是一个单调递减的函数，$f(k):\{0,1,\cdots,\min(m_a,m_c)\}\to[0.5,1]$。

3.3 模型的均衡分析

在上述博弈模型下，任意一方固定选择某一策略时，对方都可以通过调整自身策略来增大或减小关联度 k，进而实现自身收益的最大化。即不存在 i^*、j^* 使得

$$\min_{1\leqslant i\leqslant C_n^{m_a}}\max_{1\leqslant j\leqslant C_n^{m_c}} q_{ij}=q_{i^*j^*}=\max_{1\leqslant j\leqslant C_n^{m_c}}\min_{1\leqslant i\leqslant C_n^{m_a}} q_{ij} \tag{3}$$

因此，不存在纯策略纳什均衡，那么此博弈模型一定存在混合策略下的均衡局势[14]。所谓混合策略，是指博弈参与者按照一定的概率选择一种纯策略作为实际的行动。所有纯策略被选中的概率和为 1。本模型中，隐写方混合策略的行动空间是在 $C_n^{m_a}$ 个特征子集上的概率分布，分析方则是在 $C_n^{m_c}$ 个特征子集上的概率分布。

定理 1 此博弈模型下，隐写方的最佳混合策略是 $(\frac{1}{C_n^{m_a}},\frac{1}{C_n^{m_a}},\cdots,\frac{1}{C_n^{m_a}})$，即以相同概率选择子集 A_i。

证明：给定隐写方的混合策略 $(a_1,a_2,\cdots,a_{C_n^{m_a}})$，则隐写分析方在纯策略 C_j 下的期望收益为 $\sum_{i=1}^{C_n^{m_a}}a_iQ_{ij}=\sum_{i=1}^{C_n^{m_a}}a_if(g(A_i,C_j))$。如果 $(a_1,a_2,\cdots,a_{C_n^{m_a}})$ 是隐写方的最优选择，那一定意味着分析方在各个纯策略间是无差异的，即：

$$\sum_{i=1}^{C_n^{m_a}}a_if(g(A_i,C_1))=\sum_{i=1}^{C_n^{m_a}}a_if(g(A_i,C_2))=\cdots=\sum_{i=1}^{C_n^{m_a}}a_if(g(A_i,C_{C_n^{m_c}}))$$

解此方程组得 $a_1=a_2=\cdots=a_{C_n^{m_a}}$。

又 $\sum_{i=1}^{C_n^{m_a}}a_i=1$，故此均衡局势下隐写方的混合策略为 $(a_1,a_2,\cdots,a_{C_n^{m_a}})=(\frac{1}{C_n^{m_a}},\frac{1}{C_n^{m_a}},\cdots,\frac{1}{C_n^{m_a}})$，同理可得分析方的混合策略 $(c_1,c_2,\cdots,c_{C_n^{m_c}})=(\frac{1}{C_n^{m_c}},\frac{1}{C_n^{m_c}},\cdots,\frac{1}{C_n^{m_c}})$。

定理 2 均衡局势下，隐写对抗双方的期望支付仅与特征集的维数 m_a、m_c 有关，隐写方的期望支付为

$$\sum_{k=0}^{m}\frac{C_{m_a}^{k}\cdot C_{n-m_a}^{m_c-k}}{C_n^{m_c}}f(m-k),m=\min(m_a,m_c) \tag{4}$$

证明：根据定理 1，在均衡局势下，分析方选择各个策略的概率均匀分布。因此，对于隐写方任意一次决策 A_i，关联度 $g(A_i,C_j)=k$ 的概率仅与 m_a 和 m_c 的大小有关，可以记为 $p(k,m_a,m_c)$。由基本的组合数学知识可得：

$$p(k,m_a,m_c)=\frac{C_{m_a}^{k}\cdot C_{n-m_a}^{m_c-k}}{C_n^{m_c}},k=(0,1,\cdots,\min(m_a,m_c)) \tag{5}$$

因此，在该博弈模型的均衡局势下，隐写方的期望支付为

$$\begin{aligned}F=F(A,C)&=\sum_{i=1}^{C_n^{m_a}}\sum_{j=1}^{C_n^{m_c}}a_ic_iq_{ij}\\&=\sum_{k=0}^{m}p(k,m_a,m_c)f(m-k)\\&=\sum_{k=0}^{m}\frac{C_{m_a}^{k}\cdot C_{n-m_a}^{m_c-k}}{C_n^{m_c}}f(m-k),m=\min(m_a,m_c)\end{aligned} \tag{6}$$

由式(6)可知，隐写方的期望支付仅与特征集的维数 m_a、m_c 有关。

4 以算法作为策略的博弈模型

另一种接近实际的博弈对抗过程是：隐写算法提出后，会出现针对该算法效果较好的检测方法；隐写方针对该检测方法利用的特征集对隐写算法进行改进，保持这些特征在隐写前后不变以提高隐写的安全性；之后分析方又发掘并利用其它特征来检测新算法。针对这类博弈过程，我们引入以隐写和隐写分析算法为策略的博弈模型。

4.1 博弈双方的策略

将隐写对抗双方的策略归为两类算法，分别记为 naive，sophisticated。naive 隐写强调嵌入的随机性，不利用任何边信息自适应地保持图像特定的隐写特征。而 sophisticated 隐写方案清楚地认识到在嵌入信息时可以利用统计特征的不可区分来提高隐写的抗检测性，采取特征保持的隐写思想。

隐写分析方的策略是对隐写策略的反应。naive 策略下的隐写分析者选取的是区分原隐写算法最有效的一些特征，却未考虑隐写者可以在嵌入信息时尝试隐藏这些特征。sophisticated 的隐写分析者考虑到这一情况发生的可能，选取了部分其它特征构成新的特征集参与检测。

4.2 博弈模型的均衡分析

在隐写分析实践中，基于统计特征的通用隐写分析算法对不同的隐写算法往往具有不同的检测率。造成这一现象的原因很多，但很重要的一点是隐写算法在隐写前后或多或少地保持了载体图像的一部分统计特性，而这些统计特性与分析算法使用的特征子集间具有不同的关联度。用 A_n 表示隐写算法本身可保持的特征集，C_n 表示原隐写检测算法的特征集，A_s、C_s 分别表示隐写方和分析方在 sophisticated 策略下的特征集。依据上节的论述得到此博弈模型的支付关系，如表 1 所列。

表 1 （隐写方，分析方）的支付关系

		隐写分析方	
		naive	sophisticated
隐写方	naive	(f(0),1−f(0))	(f(g(A_n,C_s)),1−f(g(A_n,C_s)))
	sophisticated	(1/2,1/2)	(f(g(A_s,C_s)),1−f(g(A_s,C_s)))

naive 的分析策略是检测原隐写算法较好的方法，可以认为 $g(A_n,C_n)=0$，因此表中（naive，naive）局势的支付关系为 $(f(0),1-f(0))$。sophisticated 的隐写策略是针对 Naive 分析方法进行改进的，所以 $g(A_s,C_n)=m_c$，$f(g(A_s,C_n))=1/2$。

需要注意的是，隐写方采取 sophisticated 策略时，着重对 C_n 内的特征加以保持，却可能破坏了 A_n 中部分特征的不可检测性，因此改进后隐写算法所能保持的特征总数 $|A_s|$ 符合式(7)：

$$m_c\leqslant|A_s|\leqslant|A_n|+m_c \tag{7}$$

在隐写双方相互知悉对方策略的前提下，此模型的均衡局势有以下两种情况：

1）当 $g(A_s,C_s)\geqslant g(A_n,C_s)$ 时，$f(g(A_s,C_s))\leqslant f(g(A_n,C_s))$，为使支付最小，隐写方的最佳策略是 sophisticated。相应地，分析方应选择 sophisticated 策略。因此最终的均衡局势为（sophisticated，sophisticated），隐写方的期望支付为 $f(g(A_s,C_s))$；

2）当 $g(A_s,C_s)\leqslant g(A_n,C_s)$ 时，$f(g(A_s,C_s))\geqslant f(g(A_n,C_s))$，此时不存在最优纯策略。通过等值法可得纳什均衡下的博弈双方的混合策略，如式(8)所示，求解过程参照定理 1 证明，在此不作赘述。

$$\begin{aligned}&(a_{naive},a_{sophisticated})=\\&\left(\frac{1-2f(g(A_s,C_s))}{2(f(g(A_n,C_s))-f(g(A_s,C_s))-f(0))+1},\right.\\&\left.\frac{2(f(g(A_n,C_s))-f(0))}{2(f(g(A_n,C_s))-f(g(A_s,C_s))-f(0))+1}\right)\\&(c_{naive},c_{sophisticated})=\\&\left(\frac{2(f(g(A_n,C_s))-f(g(A_s,C_s)))}{1+2(f(g(A_n,C_s))-f(0)-f(g(A_s,C_s)))},\right.\\&\left.\frac{1-2f(0)}{1+2(f(g(A_n,C_s))-f(0)-f(g(A_s,C_s)))}\right)\end{aligned} \tag{8}$$

出现均衡局势 1 是隐写方愿意看到的，这说明特征保持算法确实带来了隐写安全性的提高。而局势 2 对应了现实中特征保持隐写算法在不完全载体模型上过度训练的情况，如 FCM 算法[15]、MOD 算法[3]。这类算法虽然对特定隐写分析方法有很高的安全性，但当分析方使用载体模型外的特征时其安全性会迅速下降，甚至不如普通的隐写算法。这种情况下，隐写方只能采取以一定概率随机使用原算法和新算法的混合策略来提高安全性。

5 模型实例

本节以一个近似的实例对以隐写和隐写分析算法作为策略的隐写博弈模型作进一步说明。

5.1 实验方案

HOS(higher order image statistics)[16] 隐写检测算法是 Lyu 和 Farid 提出的一种经典的通用盲检测算法。算法主要分两步实现：从样本图像（原图像和载密图像）中提取特征，然后基于这些特征训练分类器。

提取特征向量时，HOS 算法首先用类似于小波的正交镜像滤波器(Quadrature Mirror Filters，QMF)将图像分解为多尺度的水平、垂直、对角方向和低频分量，之后依据周边低频分量的前 4 阶统计量，借助线性预测器估算每个低频分量的均值、方差、偏态系数和峰度。估算系数与实际系数的误差数据作为最终的特征向量。

针对 HOS 检测算法，文献[17]借助 POCS 算法提出了一种特征保持的隐写方法。算法从视觉安全性、统计安全性和信息可提取性 3 方面对载密体的选择范围进行限制。如果这些限制凸集 S_i 的交集非空，由 POCS 算法生成的图像序列 $\{f_k\}_{k=0}^{\infty}$ 将按式(9)收敛于交集中的一点。

$$f_{k+1}=(P_{S_n}(P_{S_{n-1}}\cdots P_{S_1}(f_k)\cdots)),k=0,1,\cdots \tag{9}$$

式中，$P_{S_i}(x)=\arg\min_{y\in S_i}\|y-x\|$。这就保证了最终生成的载体图像不仅满足上述 3 方面要求，而且具有最小的失真。本实验选择该算法作为隐写方的 sophisticated 策略，相应的 naive策略是仅从视觉安全性和信息可提取性两方面考虑形成的隐写算法。隐写分析方的 naive 和 sophisticated 策略分别选择 HOS 和 SPAM 检测算法[13]。

实验的图像样本来自 UCID 图像库[18]，该图像库包括了

1338 幅未经压缩的 TIFF 格式的彩色图像。实验前将全部图像转换为 png 格式灰度图。其中一半用于分类器训练，另一半用于检测。

5.2 实验结果及分析

表 2 和表 3 列出了不同嵌入量下隐写方的支付情况，即隐写分析算法正确检测的概率。由表 2 和表 3 数据可以发现，在(sophisticated，naive)局势下分类器的分类效果下降明显，近乎随机猜测，说明文献[17]的算法能有效保持 HOS 检测特征，在面临 HOS 检测方法时具有很高的安全性。这一实验结果符合上节描述的以算法作为策略的博弈模型。

表 2 嵌入 3000bits 时隐写方的支付

		隐写分析方	
		naive	sophisticated
隐写方	naive	85.19%	82.57%
	sophisticated	52.58%	90.06%

表 3 嵌入 5000bits 时隐写方的支付

		隐写分析方	
		naive	sophisticated
隐写方	naive	89.49%	86.05%
	sophisticated	51.83%	96.32%

表 4 列出了 HOS 算法在不同隐写算法下检测效果的详细数据。表中前两列数据分别为经过训练的分类器在训练图像集和检测图像集上检测正确的概率。观察表 4 可知，与训练集相比，检测集下的分类器效果有明显的下降，尤其是在(sophisticated，naive)局势下，造成这一结果的主要原因是过高的漏检率，这说明分类算法已无法有效区分载密图像和原始图像。表中最后一列为检测集内 669 幅载密图像相对原图像的 *PSNR* 平均值，$PSNR=10\cdot\log(225^2/(MSE))$，其中 *MSE* 为对应图像间的均方误差。由于 sophisticated 隐写策略在载密图像生成中考虑了统计安全性，因此其 *PSNR* 相较于 naive 策略有 0.5～1dB 的下降。

表 4 HOS 在不同隐写策略下的检测效果

嵌入量	隐写策略	训练效果	测试效果	虚警率	漏检率	Av. PSNR
3000 bits	naive	95.01%	85.19%	12.11%	17.52%	36.87dB
	sophisticated	94.87%	52.58%	14.53%	80.31%	36.26dB
5000 bits	naive	98.16%	89.49%	10.26%	12.76%	35.09dB
	sophisticated	98.12%	51.83%	11.71%	84.63%	34.14dB

观察表 2 和表 3，我们还发现：sophisticated 隐写策略虽然能够很好地抵抗 HOS 检测，但是在面临 SPAM 检测方法时，其效果并没有 naive 策略好。这说明文献[17]提出的特征保持方法并没有真正提高隐写的安全性。因此，该实验结果对应 4.2 节均衡局势的第 2 种情况，双方的最佳策略为混合策略。根据式(8)可得，嵌入量为 3000bits 时，均衡局势下的隐写方应以 0.935 的概率选择 naive 策略，以 0.065 的概率选择 sophisticated 策略，隐写分析方则以 0.187 的概率选择 naive 策略，以 0.813 的概率选择 sophisticated 策略，此时隐写方的期望支付为 83.06%。嵌入量为 5000bits 时，均衡局势下隐写方的混合策略为($a_{naive}=0.928$，$a_{sophisticated}=0.072$)，分析方的策略为($c_{naive}=0.214$，$c_{sophisticated}=0.786$)，隐写方的期望支付是 86.79%。表 5 列出了实验中隐写方采取最优混合策略时，分析方各个策略的检测结果。

表 5 隐写方在最优策略下的支付

嵌入量 (bit)	隐写方嵌入策略	隐写分析方		
		naive	sophisticated	Mix
3000	($a_{naive}=0.935$，$a_{sophisticated}=0.065$)	82.93%	83.09%	83.05%
5000	($a_{naive}=0.928$，$a_{sophisticated}=0.072$)	86.71%	86.78%	86.74%

结束语 目前，基于统计特征保持的隐写方法还很不成熟。本文以隐写分析算法的检测率作为支付函数，分两种对抗情况建立博弈模型，并基于这些模型讨论了特征保持隐写的安全性。根据模型的均衡局势分析，本文指出：当隐写方固定选择基于统计保持的隐写方式时，其安全性仅与博弈双方选择的特征数有关，相对安全的策略是等概率选择各特征子集；而当隐写方在一般隐写和特征保持隐写两类算法间选择时，最佳策略取决于统计保持隐写在新的检测方法下的安全性表现。值得说明的是，本文的研究是围绕特征保持隐写开展的理论探讨，在建模过程中进行了一定的假设和简化，如何使模型与实际更加接近以指导特征保持隐写算法的设计是将来研究的重点。

参 考 文 献

[1] 奚玲，平西建，张涛. 基于相邻灰度值互补嵌入的 LSB 匹配隐写改进算法[J]. 计算机科学，2010，37(9)：101-104

[2] Agaian S S, Sifuentes R R. Adaptive Steganography with Increased Embedding Capacity for New Generation of Steganographic Systems [C]// Proc of SPIE-IS&T Electronic Imaging. Bellingham: SPIE Press, 2005: 257-268

[3] Lou D C, Wu N I, Wang C M, et al. A Novel adaptive steganography based on local complexity and human vision sensitivity [J]. Journal of Systems and Software, 2010, 83(7): 1236-1248

[4] 张湛，刘光杰，戴跃伟，等. 基于隐写编码和 Markov 模型的自适应图像隐写算法[J]. 计算机研究与发展，2012，49(8)：1668-1675

[5] Filler T, Fridrich J. Design of Adaptive Steganographic Schemes for Digital Images[C]// Proc of Media Watermarking, Security, and Forensics III. Bellingham: SPIE Press, 2011, 7880: 1-14

[6] Kodovsky J, Holub V. On Dangers of Overtraining Steganography to Incomplete Cover Model[C]// Proc of ACM Multimedia & Security Workshop. New York: ACM Press, 2011: 69-76

[7] Kodovsky J, Fridrich J. Steganalysis of JPEG Images Using Rich Model[C]// Proc of Media Watermarking, Security, and Forensics XIV. Bellingham: SPIE Press, 2012, 8303: 1-13

[8] Fridrich J, Pevny T, Kodovsky J. Statistically Undetectable JPEG Stenanography: Dead Ends, Challenges, and Opportunities [C]// Proc of the 9th ACM Multimedia & Security Workshop. New York: ACM Press, 2007: 3-14

[9] 刘春庆，李忠新，王执铨. 隐秘通信系统的对策论模型[J]. 通信学报，2004，25(5)：160-165

[10] 刘光杰，戴跃伟，赵玉鑫，等. 隐写对抗的博弈论建模[J]. 南京理工大学学报：自然科学版，2008，32(2)：199-204

[11] Schottle P, Bohme R. A Game-Theoretic Approach to Content-Adaptive Steganography[C]// Proc of Inforamtion Hiding. Berlin: Springer-Verlag, 2012: 125-141

[12] Fridrich J, Goljan M. Practical Steganalysis of Digital images: State of the Art[C]// Proc of SPIE Photonics Imaging 2002, Security and Watermarking of Multimedia Contents IV. Bellingham: SPIE Press, 2002, 4675: 1-13

(下转第 235 页)

3.2 实验结果

图 2 评价了查询时间段的长度对 CRSKQ 和 LS 算法运行时间的影响。如图 2 所示，随着监控的查询时间段的增长，这两种算法的运行时间也增大。对于 CRSKQ 而言，这是因为随着查询时间的变长，查询点 q 到达路段端点的可能性增大，则需要发起新的查询的可能性也增大；对于 LS 而言，其原因在于所需发起的静态查询的次数随着查询时间段的增长而增多。

图 3 评估了系统内对象数对算法性能的影响。由图 3 可知，这两种算法的运行时间随着对象数的增加而有所增大。其原因在于，随着对象数的增加，系统内对象的密度增大，位于监控范围内的对象数也会增大。因此，查询处理所需的对象距离值计算和比较工作量也相应增加，从而加大了查询处理的时间代价。

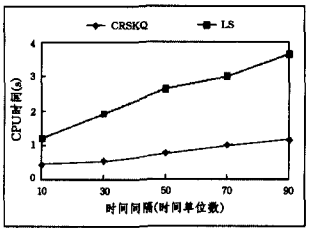

图 2 查询时间段长度对算法运行时间的影响

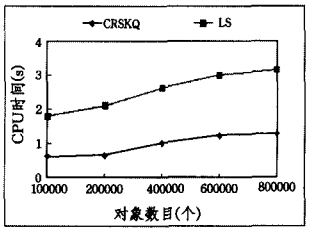

图 3 对象数对算法运行时间的影响

图 4 评估了变化的关键字数目对这两种算法运行时间的影响。如图 4 所示，LS 算法的性能随着关键字数目的增加稍有增大。而 CRSKQ 算法的运行时间随关键字数目的增加而有所减少。对于 CRSKQ 而言，关键字多时，算法处理过程将过滤掉较多的不满足关键字要求的对象，从而减少监控的候选对象数，则相应的候选对象距离值计算和比较的操作也会相应减少，从而减少查询处理所需的 CPU 运行时间。

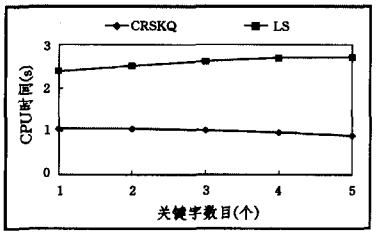

图 4 关键字数目对算法运行时间的影响

结束语 近几年来，研究者开始关注综合考虑距离因素和关键相似性的空间关键字查询处理问题。但现有的研究成果大都是局限于欧氏空间，不适用于路网中空间关键字查询的处理。本文重点讨论了路网中连续空间关键字范围查询问题，提出了有效的查询处理算法。算法分为初始结果获取和查询结果连续监控两阶段，能够充分利用前面时刻的查询结果来减少查询结果连续监控的代价，具有良好的性能。最后，模拟实验验证了所提算法的有效性。

参 考 文 献

[1] Papadias D, Zhang Jun, Mamoulis N, et al. Query processing in spatial network databases[C]// Proc of VLDB. Gerlin: Morgan Kaufmann, 2003: 802-813

[2] Kolahdouzan M, Shahabi C. Voronoi-based k-nearest neighbor search for spatial network databases[C]// Proc of VLDB. Toronto: Morgan Kaufmann, 2004: 840-851

[3] Mouratidis K, Yiu Manlung, Papadias D. et al. Continuous nearest neighbor monitoring in road networks[C]// Proc of VLDB. Seoul: ACM Press, 2006: 43-54

[4] Huang Yuan-ko, Chen Zhi-wei, Lee Chiang. Continuous K-Nearest neighbor query over moving objects in road network[C]// Proc of APWeb-WAIM. Suzhou: Springer, 2009: 27-38

[5] Zheng Bai-hua, Xu Jian-liang, Lee Wang-chien, et al. Grid-partition index: a hybrid method for nearest-neighbor queries in wireless location-based services[J]. The International Journal on Very Large Data Bases, 2006, 15(1): 21-39

[6] Zhou Y, Xie X, Wang C, et al. Hybrid index structures for location-based web search [C]// Proc of ACM CIKM. Bremen: ACM Press, 2005: 155-162

[7] Ed Felipe I, Hristidis V, Rishe N. Keyword search on spatial databases [C]// Proc of ICDE. Cancun: IEEE, 2008: 656-665

[8] Wu D, Yiu M L, Jensen C S, et al. Efficient continuously moving top-k spatial keyword query processing [C]// Proc of ICDE. Hannover: IEEE, 2011: 541-551

[9] Lu J, Lu Y, Cong G. Reverse spatial and textual k nearest neighbor search[C]// Proc of SIGMOD. Athens: ACM Press, 2011: 349-360

[10] Li G, Feng J, Xu J. DESKS: Direction-Aware Spatial Keyword Search[C]// Proc of ICDE. Washington DC: IEEE, 2012: 474-485

[11] Wu D M, Yiu M L, Cong G, et al. Joint Top-k Spatial Keyword Query Processing [J]. IEEE Transaction on KDE, 2012, 24 (10): 1889-1903

[12] Guttman A. R-Tree: A Dynamic Index Structure for Spatial Searching[C]// Proc of ACM-SIGMOD International Conference on Management of Data. San Jose: ACM Press, 1995: 47-57

(上接第 209 页)

[13] Pevny T, Bas P, Fridrich J. Steganalysis by Subtracting Pixel Adjacency Matrix[J]. IEEE Transactions on Information Forensics Security, 2010, 5(2): 215-224

[14] Nash J. Equilibrium Points in n-Person Games[J]. Proceedings of the National Academy of Sciences of the United States of America, 1950, 36: 48-49

[15] Kodovsky J, Fridrich J. On Completeness of Feature Spaces in Blind Steganalysis[C]// Proc of the 10th ACM Multimedia & Security Workshop. New York: ACM Press, 2008: 123-132

[16] Lyu S, Farid H. Steganalysis Using Higher-Order Image Statistics[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(1): 111-119

[17] Orsdemir A, Altun H O, Sharna G, et al. Steganalysis Aware Steganography: Statistical Indistinguishability Despite High Distortion [C]// Proc of Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. Bellingham: SPIE Press, 2008, 6819: 9-18

[18] Schaefer G, Stich M. UCID: An Uncompressed Color Image Database [C]// Proc of SPIE Electronic Imaging, Storage and Retrieval Methods and Applications for Multimedia. Bellingham: SPIE Press, 2003, 5307: 472-480

[19] 陈园园，朱孝成，叶甫谕. 一种改进的 DCT 信息隐藏算法[J]. 重庆理工大学学报：自然科学版，2011，25(12)：100-105