基于不确定性推理的JPEG图像通用隐藏信息检测技术

朱婷婷[1,2,3],王丽娜[1,2],胡东辉[1,2],付建伟[1,2],王旻杰[1,2]
(1.武汉大学计算机学院,湖北武汉 430079;2.空天信息安全与可信计算教育部重点实验室,湖北武汉 430079;
3.海军工程大学信息安全系,湖北武汉 430033)

摘 要: 目前隐写分析通常被作为一种确定性问题进行研究,研究中忽略了不确定性因素的影响,这导致了检测可靠性下降.本文对通用隐写分析中的不确定性因素进行了分析.在此基础上,构建了基于不确定性推理的隐写分析模型,设计了基于证据推理的通用隐写分析算法.实验证明了算法具有较好的可扩展性和可靠性,从而也验证了使用不确定性推理方法解决隐写分析问题的有效性.

关键词: 隐写分析;不确定性;证据理论;支持向量机
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2013) 02-0233-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.02.005

JPEG Image Steganalysis Method Based on Uncertainty Reasoning Theory

ZHU Ting-ting[1,2,3], WANG Li-na[1,2], HU Dong-hui[1,2], FU Jian-wei[1,2], WANG Min-jie[1,2]
(1. *Computer School, Whuhan University, Whuhan, Hubei* 430079, *China*;
2. *The Key Laboratory of Aerospace Information Security and Trust Computing, Ministry of Education, Wuhan, Hubei* 430079, *China*;
3. *Department of Information Security, Navy Engeering University, Whuhan, Hubei* 430033, *China*)

Abstract: Steganalysis was discussed as a certain problem without considering the uncertain factors, which reduced the reliability of steganalysis. Accordingly, the uncertainty factors, in universal steganalysis, are analyzed. Then, based on uncertainty reasoning method, a steganalysis model considering the uncertain factors from features extraction, classifier training and decision is put forward. Moreover, an universal steganalysis algorithm is proposed based on Dempster-Shafer(D-S) evidence theory. The experimental results show that the reliability and scalability of the algorithm is higher than previous algorithms and uncertainty theory is validity to resolve the steganalysis problems.

Key words: steganlysis; uncertainty; dempster-shafer evidence theory; support vector machine

1 引言

JPEG图像是广泛使用的隐写载体,基于JPEG图像的隐藏信息通用检测(又称为通用隐写分析)成为研究的热点.目前,通用隐写分析算法设计主要基于"特征提取-分类器训练-决策"的模式,通常通过构建敏感特征提高算法检测率.隐写分析中的特征构建包括两个重要步骤:图像校准和敏感特征提取.图像校准主要包括局部校准与全局校准.文献[1]首次提出了基于剪切的全局校准方法.文献[2,3,4]等也使用了该方法取得了较好的效果.文献[5,6]提出了全局校准与局部校准结合的思路,在剪切全局校准的基础上,分别使用均值滤波、像素预测的局部校准方法.由于大多数JPEG隐写算法通过改变量化后的DCT系数实现隐写.因此,提取DCT域特征对隐写分析更有效.使用Markov转移概率矩阵描述DCT系数之间的关系,从而提取Markov特征是一种常用的方法.文献[5,6,7]等均采用此种方法,取得了较好的效果.文献[4]提取了偏序Markov特征.文献[8]基于DCT系数SαS模型提取特征,并在此基础上提出了一种基于净图定量描述的隐写分析方法.

由此可见,目前的研究均将隐写分析作为一种确定性问题进行探讨.所谓确定性是指客观事物联系和发展中清晰的、必然的、精确的属性.也就是说,通用隐写分析特征提取、分类器训练以及决策等各个环节均应刻画

收稿日期:2012-03-26;修回日期:2012-08-23
基金项目:国家自然科学基金(No.60970114,No.61100042);国家863高技术研究发展计划(No.2009AA01Z44);海军工程大学自然科学基金(No.HGDQNJJ11023)

出能够区分隐写载体与原始载体的必然的、精确的属性.然而,通用隐写分析各个环节均存在不确定性问题,具体分析如下:(1)特征难以清晰的、精确的刻画出隐写载体与原始载体的区别.不同的特征能够区分的隐写算法有限、各有侧重,并且这种区分是一种大比数区分的方式,即大多数存在这样的差异,也存在少部分受复杂载体影响无法区分的特例;(2)分类器训练容易受到可变初始条件的影响.隐写分析中分类器训练的初始条件主要包括:初始训练样本集及初始参数.这些初始条件直接影响了判决结果,即使相同的检测样本,由于分类器学习时初始条件不同,检测结果也会大相径庭;(3)决策规则不能清晰的反映载体样本与隐写样本之间的区别.多数分类器采用"0"、"1"硬判决方式.然而,这种判决无法精确的揭露待检载体的真实属性.例如,以 0.51 的概率被判决为隐写的样本与以 0.51 判决为载体的样本之间的差别并不明显.这种差别也许并不是载体隐写与否的差别,而有可能是以上不确定因素所带来的差别.正是由于判别没有考虑这种不确定性,才使得这种边界样本容易被误判,从而影响检测的可靠性.

综上所述,通用隐写分析的研究中存在诸多不确定信息,传统确定性问题的解决思路和方法直接应用于隐写分析中存在一定的局限性,这影响了隐写分析的可靠性.因此,本文将隐写分析问题作为一种不确定性问题进行探讨,将不确定性理论和方法应用于通用隐写分析中.

2 基于不确定性推理的隐写分析模型

2.1 问题描述

通过前面的分析可知,通用隐写分析问题是一类不确定性问题.通过以下定义描述通用隐写分析系统:

定义 1 系统 $\Omega=\{I;U;F;\Delta U\}$ 为通用隐写分析系统,I 为待测样本,U 为不确定性度量方法集,F 为隐写辨识方法集,ΔU 为不确定性判别时允许的约束.

定义 2 不确定性度量函数 $f_{\text{uncertainty}}: I\times U\rightarrow(0,1)$,其中 $U=\{u_1,u_2,\cdots,u_n\}$,$u_i(1\leqslant i\leqslant n)$ 为第 i 次度量使用的方法.在这种情况下,如果度量值越高说明不确定度越大,判决的可信性越小.

定义 3 不确定性判别约束 $f_{\text{uncertainty}}(I,U)\leqslant\Delta U$,即不确定性度量值不得高于 ΔU.

定义 4 隐写辨识函数 $f_{\text{steganalysis}}: I\times U\times F\times\Delta U\rightarrow\{0,1\}$.输出隐写分析结果,值为 0 表示为载体数据;值为 1 表示为被隐写数据.

2.2 模型构建

通过前面的分析可知,通用隐写分析中不确定信息主要来源于三个层次,即样本层、特征层、分类器层.虽然不确定性和确定性是信息在不同知识粒度上的不同表现,可以按照不同的粒度划分进行不确定性度量.然而,通用隐写分析不确定性的细粒度划分及度量非常复杂、困难.因此,本文将通用隐写分析不确定性作为整体性问题进行探讨,基于不确定性推理的思路构建模型.

如图 1 所示,在数据获知层,获取待测样本的数据信息;在特征获取层,多角度提取隐写分析特征,多类特征的选择旨在降低单一特征片面性的影响;考虑到数据获取、特征提取以及机器学习等环节的不确定性影响,在不确定性推理层构建不确定性推理知识模型综合考虑各环节的影响;在推理决策层构建基于不确定性推理的融合模型,对不同推理知识模型的描述进行综合判断,给出隐写分析结论.

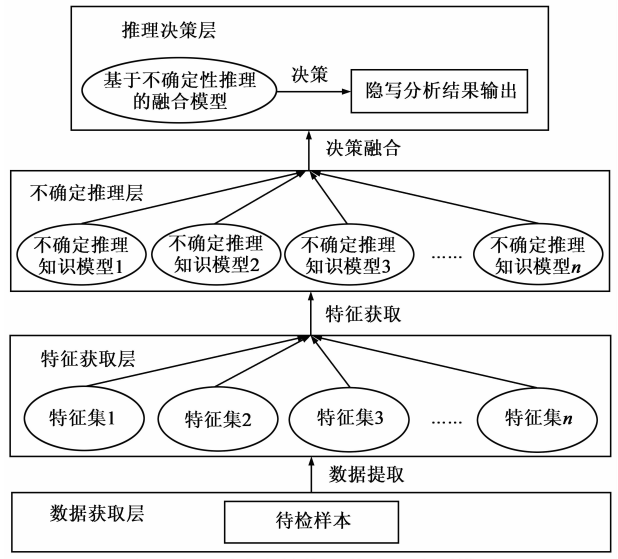


图1 基于不确定性推理的隐写分析模型

3 基于证据推理的隐写分析算法

3.1 算法设计思路

证据理论在表达和量化不确定性方面具有如下优势[9,10]:(1)可以表达和处理不确定性的多维特性,包括随机性和不具体性;(2)可以用来表达和处理非精确性概率,能表达未知性和不确定性程度.因此,本文以证据理论为基础,依据证据推理的思路,设计基于证据推理的隐写分析算法.算法设计思路如图 2 所示:

(1)证据优选与 BPA 函数构造

根据各个假设应互斥且完整地描述问题所有可能的要求,确定辨识框架 $\Theta=\{0,1\}$,其中 0 为非隐写,1 为隐写.由于不同的特征从不同的侧面反映样本的信息,为决策提供证据支持.因此,依据特征的优良与否优选证据得到证据集 $\{\boldsymbol{E}_1,\boldsymbol{E}_2,\cdots,\boldsymbol{E}_n\}$.在此基础上,构建基本概率赋值(basic probability assignment,BPA)函数.

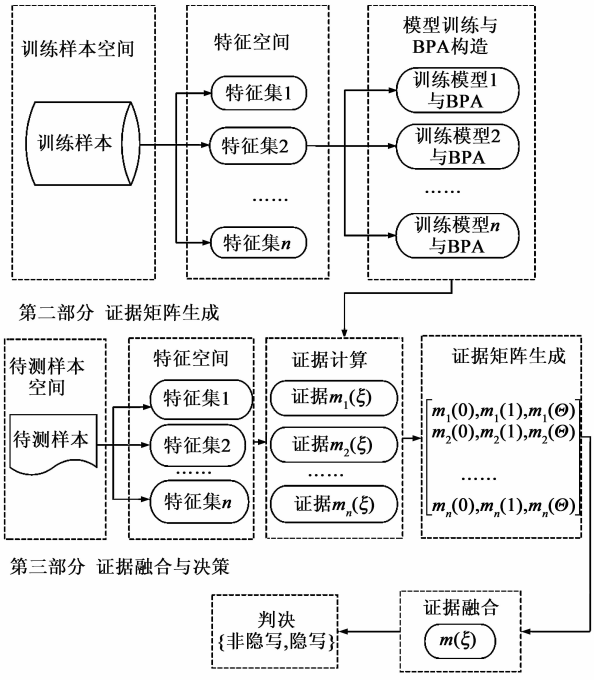


图2　基于证据推理的隐写分析流程

(2)证据矩阵生成

获取每个证据所支持焦元的 BPA 函数值 $m_i(\xi)$ ($m_i(\xi)=\{m_i(0),m_i(1),m_i(\Theta)\}$),进而生成证据矩阵 $\boldsymbol{E}$:

$$\boldsymbol{E}=\begin{bmatrix} m_1(0),m_1(1),m_1(\Theta) \\ m_2(0),m_2(1),m_2(\Theta) \\ \cdots\cdots \\ m_n(0),m_n(1),m_n(\Theta) \end{bmatrix} \tag{1}$$

(3)证据融合与决策

依据融合规则(记为 $f(x)$)实现证据融合得到融合结果 $m(\xi)$,即:

$$m(\xi)=f(E) \tag{2}$$

根据判决规则推测出待测样本的状态(即,隐写还是非隐写).

3.2　算法设计关键

(1)证据选择

证据的好坏直接影响隐写判决的准确与否.结合隐写分析特点,按照以下标准优选证据:(1)证据能够从不同侧面对判决提供支持;(2)证据能够对判决提供有效的支持.基于以上标准,综合考虑图像校准与敏感特征提取等影响证据的因素,优选证据如下:

Set1　基于全局剪切校准多类融合特征[2]的证据.

Set2　基于全局剪切校准与预测误差局部校准多向 Markov 特征[5]的证据.

Set3　基于全局剪切校准与均值滤波局部校准 Markov 特征[6]的证据.

Set4　基于全局剪切校准偏序 Markov 特征[4]的证据.

(2)BPA 函数构造

本文引入对分类不确定性的描述,通过改造后验概率 SVM,得到 BPA 函数.

文献[12]中使用 sigmoid 函数作为连续函数把 SVM 输出映射到[0,1],实现 SVM 后验概率输出:

$$P(y=1\mid f)=\frac{1}{1+\exp(Af+B)} \tag{3}$$

其中,A、B 可以通过最小化已知训练数据和其决策值 f 的负的对数似然函数得到:

$$\min -\left(\sum_i t_i\log(p_i)+(1-t_i)\log(1-p_i)\right) \tag{4}$$

其中 $p_i=\dfrac{1}{1+\exp(Af_i+B)}$, $t_i=\dfrac{y_i+1}{2}$, y_i 为样本类别标签.

然而,这种后验概率输出仅体现了绝对判别的概率,没有考虑 SVM 判别的不确定性.因此,对以上输出进行改造.

判决的不确定性通常与检测样本、训练样本、分类器等因素有关.因此,对以下因素不确定性进行描述:

分类器不确定因子 u_{svm}:依据 SVM 识别误差上界的定义[13],得到分类器不确定因子计算公式(如式 5 所示):

$$u_{\text{svm}}=\frac{E(N_{SV})}{N-1} \tag{5}$$

其中,N_{SV}为支持向量的数量,N 为训练样本的数量.

训练样本不确定因子 u_{train}:同样的分类器,使用不同的样本进行训练会得到不同的分类规则.因此,通过式(6)描述这种不确定性:

$$u_{\text{train}}=\frac{1}{n}\sum_{i=1}^{n}\left(\frac{N_i'}{N_i}\right) \tag{6}$$

其中,N 为测试样本数,N' 为错检样本数,n 为检测次数.

检测样本不确定因子 u_{image}:临近分类边界的样本容易被错分,这主要因为它被判别为"1"和"0"的概率差距不大.因此,通过"1"、"0"检测概率差描述检测样本的不确定性(其中 p_1 判断为隐写的概率,p_0 判断为非隐写的概率),如式(7)所示:

$$u_{\text{image}}=\left|p_1-p_0\right| \tag{7}$$

根据式(5)~(7),得到 SVM 不确定度输出如式(8)所示:

$$\theta=\begin{cases} 0.1, p_1=p_0 \\ \dfrac{k u_{\text{svm}} u_{\text{train}}}{u_{\text{image}}}, p_1\neq p_0 \end{cases} \tag{8}$$

其中,$\theta\in(0,1)$,k 为约束因子,将 θ 约束在取值范围中.不同的检测图像 u_{image}取值不同,θ 随 u_{image}呈动态变化.因此,这里把 θ 称为动态不确定因子.

利用公式(3)~(8)得到 BPA 输出:

$$m_i(0)=\frac{1}{1+e^{Af(x_i)+B_i}}(1-\theta) \tag{9}$$

$$m_i(1)=\frac{e^{Af(x_i)+B_i}}{1+e^{Af(x_i)+B_i}}(1-\theta) \tag{10}$$

$$m_i(\Theta)=\theta \tag{11}$$

由式(9)~(11)计算得到证据的 BPA 值,即 $\{m_i(0),m_i(1),m_i(\Theta)\}(i=1,2,3,4)$.

(3)证据融合与决策

为了降低冲突证据对判决的影响,借鉴文献[13]的思路,设计降低证据冲突影响的证据融合规则.此辨识框架 Θ 下,幂集 $2\Theta=\{A1,A2,A3,A4\}$,设 C 为冲突阈值,BPA 函数 $m1,m2,\cdots mn$,它们的正交和如式(12)所示:

$$m=m_1\oplus m_2\oplus\cdots\oplus m_{n-1}\oplus m_n \tag{12}$$

定义融合规则:

$$m(\phi)=0 \tag{13}$$

$$\boldsymbol{m}(\boldsymbol{A})=\begin{cases}K^{-1}\sum\limits_{\cap A_i=A1\leqslant i\leqslant n}\prod\limits m_i(A_i), K<C\\ \dfrac{(n-1)K^{-1}\sum\limits_{\cap A_i=A1\leqslant i\leqslant n-1}\prod\limits m_i(A_i)+m_n(A_i)}{n}, K\geqslant C\end{cases} \tag{14}$$

其中

$$K=\sum_{\cap A_i\neq\Phi 1\leqslant i\leqslant n}\prod m_i(A_i) \tag{15}$$

针对融合结果,根据如下规则进行判决:

$$\begin{cases}\text{非隐写}, m(0)>m(1)\\ \text{隐写}, m(0)<m(1)\end{cases} \tag{16}$$

3.3 算法描述

Step1 优选特征集 Set1、Set2、Set3、Set4 作为证据支持.

Step2 利用式(9)~(11)计算得到证据的 BPA 输出值,即 $\{m_i(A_{\text{cover}}),m_i(A_{\text{stego}}),m_i(\Theta)\}(i=1,2,3,4)$.

Step3 利用式(13)~(15)实现证据融合,得到隐写分析结果 $\{m(A_{\text{cover}}),m(A_{\text{stego}}),m(\Theta)\}$.

Step4 利用式(16)进行决策,确定是否隐写.

4 实验结果与分析

4.1 实验准备

为了论证方法、算法设计思路的正确性,实验准备阶段注意以下问题:

(1)原始样本数量与类别:实验使用 5000 幅未经压缩原始图像,其中 1200 幅来源于 *UCID*[14](uncompressed colour image database)图像库(为 TIFF 格式)和 3800 幅自拍图像(为 RAW 格式),图像大小为 512×384(或 384×512).

(2)隐写算法的选择:实验中选择了 5 种常用的 JPEG 隐写算法进行测试,即 F5、Outguess、JPHS、Steghide、MB.同时,选择相对嵌入率 100%、50%、25%嵌入信息.

(3)训练策略:训练样本集包括随机选择 3000 幅原始图像及其相应的隐写图像,训练采用 4.3 中所描述的非对等策略.实验使用 Libsvm2.9 作为分类器,选择 RBF(radial basis function)作为核函数.

4.2 实验结果及分析

将文献[2,4,5,6,7]的五种方案与本文方案进行实验对比,实验结果如表 1 所示.经过实验数据分析可知:各种隐写分析算法对不同的隐写算法敏感度不同.例如,文献[4]算法较其他算法对 JPHS 有较好的敏感度,但对其他隐写算法没有明显检测优势.而文献[7]算法对 JPHS 检测有明显的劣势,但对 MB 有着相对较好的检测效果.这种差异由特征的片面性所带来.而本算法能够融合各个算法的优势,提高算法的整体检测率.

从另一个角度来看,本算法一定程度上降低了特征片面性带来的不确定性影响.这种基于不确定性推理的方法能够提高算法的可靠性.

4.3 训练策略优化与检测性能问题

算法中,SVM 分类效果好坏直接影响 BPA 输出结果.目前,隐写分析中主要采用单嵌入率或多嵌入率平均混合的方式进行训练,通过参数优化提高 SVM 分类效果.然而,不同的训练样本组合对分类结果存在不同的影响,这种训练方式忽略了这样的影响.以 Set1 为例进行分析,测试结果如图 3 所示.图 3 展示了不同训练样本组合情况下 Set1 的检测率.当使用 3000 幅载体样本(即嵌入率 0%)与嵌入率为 25%、50%、100%的隐写样本各 1000 幅训练(记为训练 1)时,TNR 值高,但低嵌入率的 TPR 最低;调整两类训练比例,选择 1000 幅载体样本(记为训练 2),很明显看出 TNR 非常低;当选择载

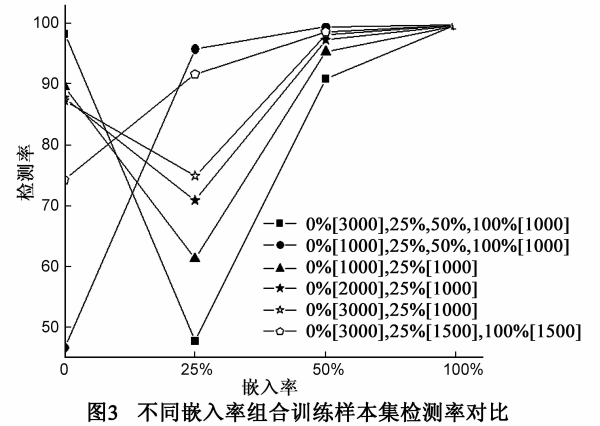


图3 不同嵌入率组合训练样本集检测率对比

体样本 3000 幅、隐写样本(嵌入率 25%)1000 幅(记为训练 3)时,低嵌入率 TPR 虽然没有训练 2 高,但 TNR 得到了提高.随着训练策略调整,TNR 与 TPR 也随之变化.基于此,考虑通过调整不同嵌入率样本组合,寻找较好的 TNR 与 TPR 的平衡点.遍历所有的组合选择结果最好的训练方式,即载体 3000 幅、嵌入率 100% 与 25% 各 1500 幅.

综上所述,通过调整训练策略可以很好的提高低嵌入率样本的检测率,在漏检率与误检率间找到合适的平衡点,从而使算法更具有实际应用价值.本文分别针对不同特征集的特点对训练样本集进行了优化,表 1 为优化后的实验结果.

表 1　不同隐写分析算法的检测结果对比

隐写算法		相对嵌入	文献[2]	文献[7]	文献[6]	文献[5]	文献[4]	本文方案
Outguess	TNR	0%	89.05%	93.85%	90.05%	96.80%	96.50%	98.30%
	TPR	25%	93.70%	98.75%	92.80%	99.50%	99.30%	99.65%
		50%	99.90%	99.90%	99.10%	100.00%	99.95%	100.00%
		100%	100.00%	100.00%	99.80%	100.00%	100.00%	100.00%
	AR		95.67%	98.13%	95.44%	99.10%	98.94%	99.49%
F5	TPR	0%	71.75%	72.75%	67.40%	75.50%	72.60%	81.10%
	TPR	25%	75.25%	69.85%	71.15%	89.30%	80.45%	90.25%
		50%	98.25%	90.10%	83.60%	98.15%	96.65%	99.10%
		100%	99.85%	98.70%	97.10%	99.10%	98.90%	100.00%
	AR		86.28%	82.85%	79.81%	90.51%	87.15%	92.61%
MB	TNR	0%	72.25%	80.10%	74.10%	81.40%	82.40%	89.45%
	TPR	25%	91.60%	97.55%	95.60%	98.10%	97.25%	98.90%
		50%	98.55%	99.55%	99.10%	99.95%	99.60%	99.95%
		100%	99.70%	99.85%	99.25%	99.95%	99.95%	99.95%
	AR		90.53%	94.26%	92.01%	94.85%	94.80%	97.06%
Steghide	TNR	0%	85.60%	89.25%	90.50%	93.75%	92.55%	95.80%
	TPR	25%	87.25%	95.20%	91.15%	97.15%	96.85%	99.25%
		50%	99.50%	99.05%	95.90%	99.65%	99.45%	99.95%
		100%	99.85%	99.60%	98.10%	99.90%	99.85%	99.95%
	AR		93.05%	95.78%	93.91%	97.61%	97.18%	98.74%
JPHS	TNR	cover	75.85%	69.90%	71.10%	75.40%	80.75%	83.40%
	TPR	25%	73.60%	63.90%	75.15%	80.80%	82.10%	83.60%
		50%	87.35%	75.50%	78.60%	95.00%	95.55%	98.90%
		100%	97.70%	79.20%	81.45%	99.50%	99.95%	99.95%
	AR		83.63%	72.13%	76.58%	87.68%	89.59%	91.46%

5　总结与展望

以往的研究中将隐写分析问题作为一种确定性问题进行探讨,忽略了隐写分析中不确定因素的影响,使用解决确定性问题的理论和技术解决通用隐写分析问题,这是造成通用隐写分析可靠性较低的一个重要原因.本文对通用隐写分析中涉及的不确定性因素进行了分析,阐述了通用隐写分析问题是不确定性问题,并构建了基于不确定性推理的隐写分析模型.在此基础上,将证据理论应用于隐写分析,以此作为研究示例,设计了基于证据推理的通用隐写分析算法.实验验证了用不确定性方法解决隐写分析问题思路的有效性.

本文是将隐写分析问题作为不确定性问题进行研究的初步探索,有很多问题有待进一步深入研究.例如,本文将通用隐写分析中的不确定性作为一个整体解决,这种是一种粗粒度的方法,能否在更细的粒度上逐层解决不确定性问题值得探讨;其次从算法设计的角度降低此类方案的复杂度也需要深入研究的问题.

参考文献

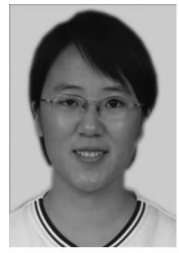
[1] Fridrich J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes [A]. Proc of the 6th International Conference on Information Hiding [C]. Berlin Heidelberg: Springer-Verlag, 2004: 67 – 81.

[2] Pevny T, Fridrich J. Merging markov and DCT features for multi-class JPEG steganalysis [A]. Proc of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX[C]. San Jose: SPIE, 2007. 3 – 4.

[3] 郭艳卿,何德全,孔祥维,等.基于多元回归的 JPEG 隐密分析方案[J].电子学报,2009,36(6):1378 – 1381.
Guo Yanqing, He Dequan, Kong Xiangwei, et al. Steganalytic scheme for JPEG images based on multivariate regression[J]. Acta Electronica Sinica, 2009, 36(6): 1378 – 1381. (in Chi-

nese)
[4] Davidson J, Jalan J. Steganaysis using partially order Markov models [A]. Pro of the 12th International Conference on Information Hiding [C]. Berlin Heidelberg: Springer-Verlag, 2010: 118 – 132.
[5] 黄方军,黄继武.基于图像校准的通用型 JPEG 隐写分析[J].中国科学 F 辑:信息科学,2009,39(4):383 – 390.
Huang Fangjun, Huang Jiwu. Calibration based universal JPEG steganalysis [J]. Journal of Science in China Series F: Information Sciences, 2009, 39(4): 383 – 390. (in Chinese)
[6] Yong Wang, Ji Fenliu, Weimingzhang, et al. Reliable JPEG steganalysis based on multi-directional correlations [J]. Signal Processing: Image Communication, 2010, 25(8): 577 – 587.
[7] Shi Y Q, Chen C, Chen W. A Markove process based approach to effective attacking JPEG stegnography[A]. Proc of the 8th International Conference on Information Hiding [C]. Berlin Heidelberg: Springer-Verlag, 2006. 249 – 264.
[8] 毛家发,钮心忻,杨义先,等.基于 JPEG 净图定量描述的隐写分析方法[J].电子学报,2011,39(8):1907 – 1912
Mao Jiafa, Niu Xinxin, Yang Yixian, et al. Steganalysis method based on JPEG cover image quantitative describing[J]. Acta Electronica Sinica, 2011, 39(8): 1907 – 1912. (in Chinese)
[9] Dempster A P. Upper and lower probabilities induced by a multi-valued mapping[J]. Annual Math Statist, 1967, 38(4): 325 – 339.
[10] Shafer G. A Muthematical Theory of Evidence[M]. Princeton: Princeton University Press, 1976, 35(1): 35 – 37.
[11] 边肇祺,张学工.模式识别[M].北京:清华大学出版社,2000.
Bian Zhaoqi, Zhang Xuegong. Pattern Recognition[M]. Beijing: Qinghua Press, 2000. (in Chinese)
[12] Platt J C. Probabilistic Output for Support Vector Machine and Comparisons to Regularized Likelihood Methods [M]. MIT Press, 1999. 1 – 11.
[13] Li Liwen, Guo Kaihong. Combination rules of evidence theory and complict problem [J]. Systems Engineering Theory and Practice, 2010, 30(8): 1422 – 1431.
[14] Schaefer G, Stich M. UCID-An Uncompressed Colour Image Database[R]. School of Computing and Mathematics, Nottingham Trent University, 2008.

作者简介



朱婷婷 女,1980 年出生,湖南祁阳人,海军工程大学讲师,武汉大学博士研究生,研究方向为信息隐藏、内容安全、信息系统安全等.
E-mail: lnawang@163.com

王丽娜 女,1964 年生,博士,教授,武汉大学计算机学院副院长,空天信息安全与可信计算教育部重点实验室(B 类)主任.研究方向为信息隐藏、云计算安全、网络可生存性等.
E-mail: zlztt1688@sina.com.cn

胡东辉 男,1974 年生,副教授,武汉大学博士,研究方向隐写分析、网络与内容安全、网络信息可信度量与隐私保护等.
E-mail: hudh@hfut.edu.cn

付建伟 男,1984 年生,武汉大学硕士研究生,研究方向信息隐藏与数字水印等.
E-mail: jiandao2002oadnaij@163.com

王旻杰 男,1989 年生,武汉大学博士研究生,研究方向信息隐藏与数字水印等.
E-mail: wmj@whu.edu.cn