文章编号:1004-9037(2014)05-0749-08

基于多分类器融合的未知嵌入率图像隐写分析方法

万宝吉 张 涛 李文祥 侯晓丹 朱振浩

(解放军信息工程大学信息系统工程学院,郑州,450002)

摘要:提出一种基于多分类器融合的未知嵌入率图像隐写分析方法。通过建立多个不同嵌入率下的训练分类器模型,得到对测试图像的多个局部决策值;然后将得到的局部决策值转化为证据,并根据各分类器的漏检率和虚警率,对各局部决策值分配权重;最后由基于权重系数的 D-S (Dempster-Shafer)证据理论推理得到最终的决策。针对 LSB 匹配隐写的实验结果表明,本文方法改善了未知嵌入率下的隐写检测性能。

关键词:隐写分析;融合决策;D-S 证据理论;未知嵌入率

中图分类号:TP391 **文献标志码**:A

Multi-Classifier Fusion Based Rate-Unknown Image Steganalysis

Wan Baoji, *Zhang Tao*, *Li Wenxiang*, *Hou Xiaodan*, *Zhu Zhenhao*

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

Abstract: A rate-unknown image steganalysis scheme is proposed based on multiple-classifier fusion. Firstly, various classified results are acquired by using the multi-rate classifiers established in the training phase. Secondly, these classified results are converted to evidence and enhanced through introducing weighted coefficients which are acquired according to the missed detection rates and the false alarm rates of different classifiers. Finally, the decision is obtained by Dempster-Shafer (D-S) evidence theory based on weighted coefficients. The detection work is presented to attack LSB matching. Experimental results show that the proposed method improves detection accuracy.

Key words: steganalysis; fusion decision; D-S evidence theory; rate-unknown

引 言

自 20 世纪 90 年代以来,信息隐藏逐渐成为信息安全领域的研究热点[1]。数字隐写及与之对应的隐写分析是信息隐藏的主要技术分支之一。数字隐写的目的是将秘密消息隐藏在载体中进行传递而不引起第三方怀疑,以便实现隐蔽通信。隐写分析则是对秘密消息进行检测、提取、恢复和破坏。

现有的隐写分析方法主要可分为专用隐写分析方法和通用盲检测方法。专用隐写分析方法通过分析载体图像和载密图像统计特性,找到载密图像区别于载体图像的统计差异模式,并通过检测待测图像中是否出现这种统计差异模式来判断隐藏信息的存在性。如针对空间域最不重要比特(Least significant bit,LSB)替换隐写的 RS(Regular/singular groups)分析法[2]、χ^2 分析法[3]、样值对分析法[4]等;针对 LSB 匹配隐写[5]的局部极值法[6]、差分估计法[7]等。通用盲检测方法主要采用基于机器学习的方法,其关键是寻找能有效区分载体和载密图像的特征,因此各方法的差别也在于所提取的分类特征不同。典型的特征包括:文献[8]提出的小波系数高阶统计量特征;文献[9-10]提出的小波分解系数特征函数(Characteristic function,CF)统计矩特征;文献[11]提出基于中值滤波复原的小波特征和文献[12]提出的直方图系数特

基金项目:国家自然科学基金(60903221,61272490)资助项目。

收稿日期:2012-07-12;**修订日期**:2012-10-24

征等。

随着研究的深入,针对图像的隐写分析技术已取得了丰硕的研究成果,在实验室环境下取得了优异的检测效果。但现有隐写分析算法通常假定已知载密图像的嵌入率,而实际应用中,隐写算法的嵌入率通常是未知的,此时针对隐写算法在一个或多个固定嵌入率下训练的分类器性能会剧烈下降,因此有必要研究具备对多种嵌入率适用的隐写分析技术。一些学者给出了初步的研究结果,如文献[13]讨论了分类器训练和测试时采用的嵌入率不一致时检测算法的性能下降问题。文献[14]提出混合多个指定嵌入率的全局分类器方法。文献[15]提出融合多个指定嵌入率的融合分类器方法来解决对未知嵌入率隐写算法的检测问题,虽然这两种方法可行,但检测效果与已知嵌入率的相比仍有一定的差距。

近年来,不少学者应用信息融合技术来解决隐写分析中的一些问题。如:文献[16]对不同隐写分析的分类结果进行决策级最大值融合和均值融合;文献[17]提出一种基于 Dempster-Shafer(D-S)证据理论的图像隐写分析方法来提高检测性能等。本文借鉴将信息融合技术应用于隐写分析的思路,利用不同的分类器对各分类模式存在互补信息的优势,研究应用多分类器融合技术来实现对未知嵌入率下隐藏信息的检测。其中融合算法采用 D-S 证据理论,因为 D-S 证据理论提供了一种有用的相关证据的合成方法,其优势在于能更好地把握问题的未知性与不确定性,将不同方面、主观不确定的信息,通过 D-S 证据理论信息融合原理有效地转化为确定性的决策结果。针对 LSB 匹配隐写的实验结果表明,本文方法改善了未知嵌入率下的隐写检测性能。

1 D-S 多分类器融合的图像隐写分析法

1.1 基本框架

本文研究基于 D-S 证据理论的多分类器融合技术以实现对未知嵌入率载密图像的有效检测。整个过程分为两个阶段:一是训练阶段(图 1);二是测试阶段(图 2)。

训练阶段:首先用某种隐写算法对训练载体图像以嵌入率 r_1 到 r_N(r_1 到 r_N 必须包含从低到高

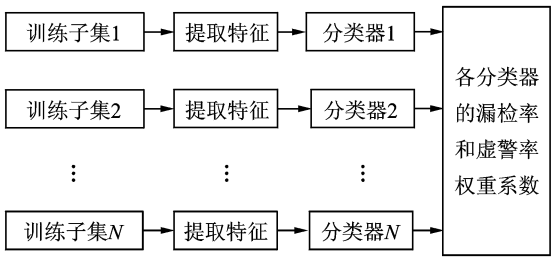

图 1 未知嵌入率隐写分析方法的训练框图

Fig. 1 Training process of rate-unknown steganalysis

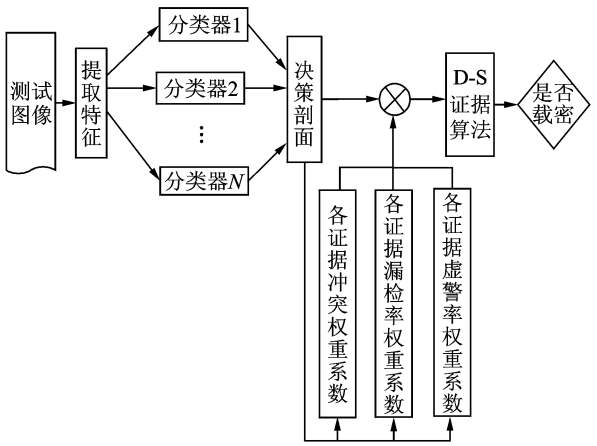

图 2 未知嵌入率隐写分析方法的测试框图

Fig. 2 Test process of rate-unknown steganalysis

的不同嵌入率,如从 0.1 到 1.0)嵌入秘密消息,得到 N 组不同嵌入率的训练载密图像。由训练载体图像和 N 组载密图像构成训练子集 1 到 N。然后对 N 组训练子集提取特征,将特征送至分类器中进行训练,得到 N 个分类器训练模型。利用训练好的分类器测试不同嵌入率的训练子集,得到 N 组漏检率和虚警率,并按照 1.4 节的步骤计算出各分类器的漏检率权重系数和虚警率权重系数。

测试阶段:首先将待测图像按照训练阶段提取特征的方法提取特征,并将特征分别输入到已训练好的分类器中进行局部决策,得到其属于载体和载密的概率。其中分类器的概率输出可通过对分类器的参数设置得到,例如在支持向量机(Support vector machine, SVM)[18]分类器中,通过对 SVM 训练模型参数 b(概率估计)的赋值可得到用于概率估计的支持向量分类器(Support vector classifier,SVC),测试时将测试样本集输入此分类器中并对测试模型参数 b 赋值可得概率输出。然后将所有分类器的概率输出构成一个决策剖面,并将决策剖面转化为证据。最后运用改进的基于权重系数的证据合成方法进行全局决策。其中,权重系数包

括原有证据合成方法中的各证据冲突权重系数，以及训练阶段得到的对隐写分析有重要影响的各证据的漏检率权重系数和虚警率权重系数。

1.2　权重系数的证据合成方法

为了选取证据和计算权重系数，本节介绍 D-S 证据理论的基本概念和基于权重系数的证据合成方法。设 Θ 为识别框架，基本概率分配函数 m 是一个从集合 2^{Θ} 到[0,1]的映射，A 表示识别框架 Θ 的任一子集，记作 $A\subseteq\Theta$，且满足

$$\begin{cases} m(\phi)=0 \\ \sum\limits_{A\subset\Theta} m(A)=1 \end{cases} \tag{1}$$

式中：$m(A)$称为事件 A 的基本概率分配函数，它表示证据对 A 的信任程度。如果 $A\subseteq\Theta$ 且 $m(A)>0$，则称 A 为焦元。

设 $m_1,m_2,\cdots,m_n$ 是同一识别框架 Θ 上的 n 个基本概率分配函数，焦元分别为 $A_i(i=1,2,\cdots,N)$，则 D-S 合成规则为

$$m(A)=\begin{cases} \dfrac{\sum\limits_{\cap A_i=A}\prod\limits_{1\leqslant i\leqslant N} m_i(A_i)}{1-k} & A\neq\phi \\ 0 & A=\phi \end{cases} \tag{2}$$

式中：$k=\sum\limits_{\cap A_i=\varphi}\prod\limits_{1\leqslant i\leqslant N} m_i(A_i)$，$k$ 的大小反映了所有证据之间的总冲突程度。$1-k$ 称为归一化因子，其作用是为了避免在合成时将非零的概率赋给空集。

当证据完全冲突或冲突较大时，即 $k\to1$ 时，D-S 证据合成式(2)失效，为解决此问题，文献[19]通过引入权重系数和冲突概率的重新分配来得到新的证据合成方法。

假设 n 个不同的证据源同时提供证据，其证据集为 $E=\{E_1,E_2,\cdots,E_n\}$，则需要确定的权重系数组成的权重向量为 $\boldsymbol{W}=(w_1,w_2,\cdots,w_n)$。

计算证据集 E 中证据 E_i 与其他证据 $E_j(j=1,2,\cdots,n,j\neq i)$之间的冲突程度 k_{ij}，构成证据 E_i 的冲突向量

$$\boldsymbol{K}_i=(k_{i1},k_{i2},\cdots,k_{ii-1},k_{ii+1},\cdots,k_{in}) \tag{3}$$

式中：$k_{ij}=\sum\limits_{\substack{A_i\cap A_j=\varphi \\ A_i\in E_i,A_j\in E_j}} m_i(A_i)m_j(A_j)$ 且 $i=1,2,\cdots,n$。

对冲突向量进行归一化，计算归一化后的熵值并取倒数

$$\boldsymbol{K}_i^N=\frac{\boldsymbol{K}_i}{\sum\limits_{j=1,j\neq i}^{n} k_{ij}}=(k_{i1}^N,k_{i2}^N,\cdots,k_{ii-1}^N,k_{ii+1}^N,\cdots,k_{in}^N) \tag{4}$$

$$\boldsymbol{H}_i=\sum_{j=1,j\neq i}^{n} k_{ij}^N\ln(k_{ij}^N)\qquad i=1,2,\cdots,n \tag{5}$$

$$\boldsymbol{H}_i^{-1}=\frac{1}{\boldsymbol{H}_i} \tag{6}$$

计算各证据的冲突权重系数

$$w_i=\frac{\boldsymbol{H}_i^{-1}}{\sum\limits_{j=1}^{n}\boldsymbol{H}_j^{-1}} \tag{7}$$

得到冲突权重向量 $\boldsymbol{W}=(w_1,w_2,\cdots,w_n)$。

进一步可得每个基本概率分布的“折扣率”

$$\alpha_i=\frac{w_i}{\max\{\boldsymbol{W}\}} \tag{8}$$

则每个调整后的基本概率分配值为

$$\begin{aligned} m_i^*(A_d)&=\alpha_i m_i(A_d) \\ m_i^*(\Theta)&=1-\sum_{k=1}^{d_i} m_i^*(A_d) \end{aligned} \tag{9}$$

式中：$d=1,2,\cdots,d_i$，d_i 为证据 E_i 提供的辨识框架中非 Θ 的焦元数。

构成新的证据合成公式

$$\begin{aligned} m(\phi)&=0 \\ m(A)&=p(A)+k\cdot q(A)\quad A\neq\phi,\Theta \end{aligned} \tag{10}$$

式中：$p(A)=\sum\limits_{\substack{A_i\in E_i \\ \cap_{i-1}^{N}A_i=A}} m_1^*(A_1)\cdot m_2^*(A_2)\cdots m_n^*(A_n)$；$k=\sum\limits_{\substack{A_i\in E_i \\ \cap_{i-1}^{N}A_i=\phi}} m_1^*(A_1)\cdot m_2^*(A_2)\cdots m_n^*(A_n)$；$q(A)=\dfrac{1}{n}\sum\limits_{i=1}^{n} m_i^*(A)$。

1.3　证据选取和基本概率分配函数

首先，采用已训练好的 N 个分类器为证据源，各分类器的概率输出为证据。然后，建立识别框架为 $\Theta=\{w_{\text{cover}},w_{\text{stego}}\}$，其中 w_{cover} 和 w_{stego} 分别表示载体图像类和载密图像类。本文采用各证据的检测正确率作为基本概率分配函数。设 $m_1,m_2,\cdots,m_N$ 分别表示基于 N 种训练嵌入率下证据的基本概率分配函数，即

$$\begin{aligned} m_1(w_{\text{cover}})&=p(w_{1c}\mid\text{Test}) \\ m_1(w_{\text{stego}})&=p(w_{1s}\mid\text{Test}) \\ m_2(w_{\text{cover}})&=p(w_{2c}\mid\text{Test}) \\ m_2(w_{\text{stego}})&=p(w_{2s}\mid\text{Test}) \\ &\vdots \\ m_N(w_{\text{cover}})&=p(w_{Nc}\mid\text{Test}) \\ m_N(w_{\text{stego}})&=p(w_{Ns}\mid\text{Test}) \\ m_1(\Theta)&=m_2(\Theta)=\cdots=m_N(\Theta)=0 \end{aligned} \tag{11}$$

1.4 新的权重系数的计算

由于不同嵌入率训练的分类器对图像的漏检率(False positive rate, FP)和虚警率(False negative rate, FN)不一样,在实验 2.3.1 节中进行了验证。因此在文献[19]中冲突系数权重的基础上,本文引入各证据的漏检率权重系数和虚警率权重系数,分别为 $\boldsymbol{W}_2$ 和 $\boldsymbol{W}_3$。把式(11)代入式(3～7)中可得到各证据的冲突向量。设式(7)中的冲突权重向量为 $\boldsymbol{W}_1=(w_{11},w_{12},\cdots,w_{1N})$。

各证据漏检率权重向量 $\boldsymbol{W}_2$ 的计算流程为:

(1)计算每个证据源对所有 n 个训练图像集的漏检率之和

$$\mathrm{FN}_i=\sum_{j=1}^{n}\mathrm{FN}_{ij} \tag{12}$$

式中:FN_{ij} 表示第 i 个证据(即训练分类器)对第 j 个训练图像集得到的漏检率。

(2)得到每个证据在所有证据中的漏检率概率

$$p_i=\frac{\mathrm{FN}_i}{\sum_{i=1}^{N}\mathrm{FN}_i} \tag{13}$$

(3)为了得到的漏检率最小,对式(13)取倒数得

$$\overline{w}_{2i}=\frac{1}{p_i} \tag{14}$$

(4)归一化

$$w_{2i}=\frac{\overline{w}_{2i}}{\sum_{i=1}^{n}\overline{w}_{2i}} \tag{15}$$

(5)得到 $\boldsymbol{W}_2=(w_{21},w_{22},\cdots,w_{2N})$。

各证据虚警率的权重向量按以上各证据漏检率权重向量的计算步骤,把 FN 换为 FP,即可得 $\boldsymbol{W}_3=(w_{31},w_{32},\cdots,w_{3N})$。

定义参数 a,b,c,满足 $a+b+c=1$。则新的权重向量为

$$\boldsymbol{W}=a\boldsymbol{W}_1+b\boldsymbol{W}_2+c\boldsymbol{W}_3 \tag{16}$$

用户可通过设置不同的参数以满足实际需要。新的权重系数仍满足 $w_i\in[0,1]$ 且 $\sum_{i=1}^{N}w_i=1$。因为

$$\sum\boldsymbol{W}=\sum(a\boldsymbol{W}_1+b\boldsymbol{W}_2+c\boldsymbol{W}_3)=a\sum\boldsymbol{W}_1+b\sum\boldsymbol{W}_2+c\sum\boldsymbol{W}_3=a\sum_{i=1}^{N}w_{1i}+b\sum_{i=1}^{N}w_{2i}+c\sum_{i=1}^{N}w_{3i}=a+b+c=1。$$

这样,通过引入 3 个方面的权重系数,即各证据间的冲突权重系数,各证据漏检率和虚警率权重系数,得到新的权重系数。新权重系数充分考虑了各证据相互间的作用和对隐写分析的影响。把得到的新权重系数式(16)代入式(8,9)中可得到调整后的基本概率分配函数值 $m_1^*(w_{\mathrm{cover}}),m_1^*(w_{\mathrm{stego}}),m_2^*(w_{\mathrm{cover}}),m_2^*(w_{\mathrm{stego}}),\cdots,m_N^*(w_{\mathrm{cover}}),m_N^*(w_{\mathrm{stego}})$ 和 $m_1^*(\Theta),m_2^*(\Theta),\cdots,m_N^*(\Theta)$,再由式(10)可计算出合成后的结果 $m(w_{\mathrm{cover}})$ 和 $m(w_{\mathrm{stego}})$,分别为

$$\begin{aligned}m(w_{\mathrm{cover}})&=p(w_{\mathrm{cover}})+k\cdot q(w_{\mathrm{cover}})\\ m(w_{\mathrm{stego}})&=p(w_{\mathrm{stego}})+k\cdot q(w_{\mathrm{stego}})\end{aligned} \tag{17}$$

式中:

$$p(w_{\mathrm{cover}})=m_1^*(w_{\mathrm{cover}})\cdot m_2^*(w_{\mathrm{cover}})\cdots m_N^*(w_{\mathrm{cover}})$$

$$p(w_{\mathrm{stego}})=m_1^*(w_{\mathrm{stego}})\cdot m_2^*(w_{\mathrm{stego}})\cdots m_N^*(w_{\mathrm{stego}})$$

$$q(w_{\mathrm{cover}})=\frac{1}{n}\sum_{i=1}^{N}m_i^*(w_{\mathrm{cover}})$$

$$q(w_{\mathrm{stego}})=\frac{1}{n}\sum_{i=1}^{N}m_i^*(w_{\mathrm{stego}})$$

$$k=1-m_1^*(w_{\mathrm{cover}})\cdot m_2^*(w_{\mathrm{cover}})\cdots m_N^*(w_{\mathrm{cover}})-m_1^*\cdot(w_{\mathrm{stego}})\cdot m_2^*(w_{\mathrm{stego}})\cdots m_N^*(w_{\mathrm{stego}})$$

1.5 全局判决

利用基于权重系数的证据合成方法,由式(17)可得多分类器融合后的合成结果 $m(w_{\mathrm{cover}})$ 和 $m(w_{\mathrm{stego}})$。全局判决规则为

$$\mathrm{Test}=\begin{cases}w_{\mathrm{cover}} & m(w_{\mathrm{cover}})>m(w_{\mathrm{stego}})\\ w_{\mathrm{stego}} & m(w_{\mathrm{stego}})>m(w_{\mathrm{cover}})\end{cases} \tag{18}$$

这两个结果中哪个概率分配函数值大,则将待测图像则判为哪一类,即得到的最终判决结果应具有最大的可信度。

2 实验结果及分析

2.1 实验设置

本实验采用 Camera 图像库[20],该图像库包含 3 164幅大小为 512×512 的未压缩灰度图像。从中随机选取 1 600 幅进行试验,其中随机选择 600 幅用于训练,剩余 1 000 幅用于测试。训练和测试的分类器采用支持向量机[18],具体实现用 LIBSVM 2.86[21],选用径向基函数作为核函数。

为了验证本文方法在嵌入率未知时对隐写算法的有效检测性能,本文以 LSB 匹配嵌入算法[5]为例,文献[12]提出的 70 维特征作为分类特征,并取 $N=10$,指定嵌入率为 0.1, 0.2, …,1。对训练

的 600 幅图像，用 LSB 匹配算法以 10 种不同嵌入率构造训练载密图像集，对每种嵌入率的载体载密图像集提取分类特征，用 SVM 训练，得到训练好的分类器。剩余的 1 000 幅测试图像以同样的嵌入方法，得到 10 种不同嵌入率的测试载密图像集。将 1 000 幅的测试图像均分成 10 份，每份分别以 0.1～1.0(以 0.1 递增)的嵌入率嵌入得到混合嵌入率测试图像；用嵌入率为 0.15，0.25，0.35，0.45，0.55，0.75 分别嵌入测试图像可得到 6 种单一嵌入率的测试图像。

2.2　评估指标

本文采用下列指标进行评估：

假阳率：将载体数据误识为载密数据的比率，也称虚警率。

假阴率：将载密数据误识为载体数据的比率，也称漏检率。

设待检测的载体数据和载密数据的样本数分别为 C 和 S，其中被正确识别的载体数据和载密数据的样本数分别为 N 和 P，则检测正确率 ACC 定义为

$$\mathrm{ACC}=\frac{P+N}{S+C} \tag{19}$$

其中，FP 和 FN 越接近于 0，ACC 越接近于 1，表示算法的检测性能越好。

2.3　结果及分析

2.3.1　固定嵌入率训练的分类器性能

本节采用传统的固定嵌入率训练的分类器，来测试不同嵌入率下的待测图像，并得到相应的漏检率和虚警率。通过观察和分析，结果验证了 2.2 中引入权重系数的必要性。应用实验设置里训练好的各固定嵌入率分类模型和 10 种不同嵌入率的测试图像集进行实验。

图 3 为固定嵌入率训练的分类器漏检率曲线，其中，图例 0.1，0.3，0.5，0.7，0.9 分别表示嵌入率为 0.1，0.3，0.5，0.7，0.9 时训练的分类器，横坐标 0.1～1.0 分别表示嵌入率为 0.1～1.0 时生成的相应嵌入率下的待测图像集，纵坐标表示固定嵌入率训练的分类器测试不同嵌入率的待测图像集时的漏检率 FN。

图 3 表明，不同嵌入率训练的分类器对测试图像的漏检率差异较大。低嵌入率训练的分类器对整个测试图像集都有很低的漏检率，表明检测效果很好，如嵌入率为 0.1 时训练的分类器。而高嵌入率训练的分类器测试高嵌入率的图像时漏检率低，但测试低嵌入率的图像时，漏检率很高，导致检测失效，如嵌入率为 0.7，0.9 时训练的分类器。

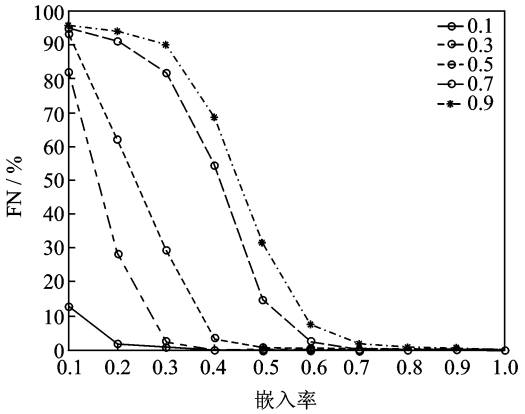

图 3　固定嵌入率训练的分类器漏检率

Fig. 3　FN of embedding rate-specific classifier

图 4 所示为固定嵌入率下训练的分类器虚警率曲线。横坐标表示嵌入率为 0.1～1.0 时训练的分类器，纵坐标表示固定嵌入率训练的分类器测试不同嵌入率的待测图像集时的虚警率 FP。因为测试图像的载体都一样，且 SVM 分类器已训练好，所以同一嵌入率训练的 SVM 分类器对不同嵌入率的测试图像有相同的虚警率。

图 4 表明，低嵌入率训练的分类器虚警率高，如嵌入率为 0.1，0.2 时训练的分类器。而高嵌入率训练的分类器虚警率低，如嵌入率为 0.9，1.0 时训练的分类器。

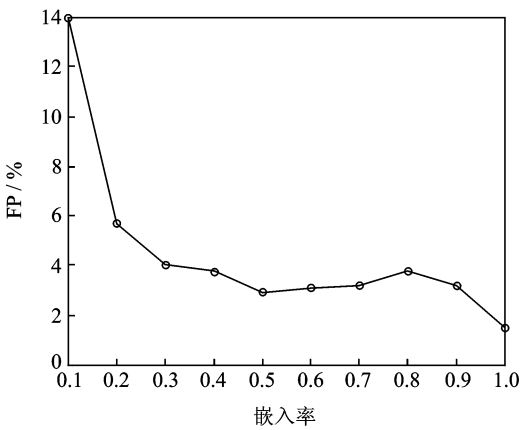

图 4　固定嵌入率训练的分类器虚警率

Fig. 4　FP of embedding rate-specific classifier

由图 3，4 得出，虽然低嵌入训练的分类器对不同嵌入率的测试图像漏检率都比较低，但虚警率很高。而高嵌入训练的分类器对低嵌入率的测试图

像漏检率高,但虚警率低。

为了使漏检率和虚警率都能达到较低的目的,应用本文提出的基于多分类器融合的未知嵌入率图像隐写分析方法,通过调整权重系数的参数 a,b,c 可得到理想的漏检率和虚警率。

2.3.2 参数的选择

使用 4 组参数 a,b,c 来测试不同嵌入率的待测图像,得到不同参数下的漏检率和虚警率,如表 1 所示。表中第 2～11 列为参数值测试不同嵌入率的待测图像集时得到的漏检率 FN,最后一列为虚警率 FP。

通过表 1 可知,设置不同的参数会得到不同的漏检率和虚警率,且漏检率的权重对检测结果影响较大,尤其是针对低嵌入率的测试,权重越大检测效果越好。为了平衡漏检率和虚警率,并考虑实际工作的需要,本文取 $a=0.1$,$b=0.8$,$c=0.1$。

2.3.3 与其他方法的性能比较

为了测试本文方法与固定嵌入率方法和全局分类器方法的检测性能,对 6 种单一嵌入率的测试图像和混合嵌入率的测试图像进行检测。

方法 1 为固定嵌入率或已知嵌入率,训练和测试选择的嵌入率相同。比如测试的载密图像嵌入率是 0.35,训练 SVM 分类器时载密图像的嵌入率也是 0.35。

方法 2 是文献[14]提出的全局分类器方法。即对 10 种指定的嵌入率(嵌入率为 0.1～1.0)混合在一起构成训练图像集进行训练,得到一个全局分类器,之后对 6 个单一嵌入率及混合嵌入率的图像集分别进行测试得到检测结果。

本文方法是基于多分类器融合的未知嵌入率隐写分析方法。即训练 10 个指定嵌入率(嵌入率为 0.1～1.0)的训练分类器,对 6 个单一嵌入率及混合嵌入率的图像集分别进行测试,由图 2 的步骤可得最终的检测结果。

用以上 3 种方法测试 6 种单一嵌入率的待测图像,后两种方法测试混合嵌入率的测试图像,得到检测正确率和虚警率,结果如表 2,3 所示。表 2,3 分别表示不同方法对测试图像得到的检测正确率 ACC 和虚警率 FP。

由表 2 可知,本文方法比方法 2 在单一嵌入率和混合嵌入率的情况下都表现出较好的检测正确率,尤其是在低嵌入率的时候,如嵌入率为 0.15 时的测试图像,检测正确率比方法 2 提高 5.45%;当测试载密图像嵌入率为 0.25,0.35 和 0.45 时,本文方法甚至优于方法 1。由表 3 可知,本文方法和方法 2 的虚警率接近,在低嵌入率时,本文方法和方法 2 都比方法 1 的虚警率低,如嵌入率为 0.15,0.25 时的测试图像。

表 1 不同权重参数下的漏检率和虚警率

Table 1 FN and FP with different parameters

参数值	测试图像嵌入率										FP/%
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	
$a=0.8,b=0.1,c=0.1$	95.3	79.9	21.1	3.4	0.5	0.3	0	0	0	0	3.0
$a=0.1,b=0.1,c=0.8$	96.0	88.9	27.7	6.4	1.1	0.2	0	0	0	0	2.8
$a=0.1,b=0.8,c=0.1$	53.7	6.1	1.2	0.2	0.1	0.2	0	0	0	0	4.4
$a=0.1,b=0.9,c=0$	41.5	4.9	1.0	0.1	0.1	0.2	0	0	0	0	5.7

表 2 不同方法对单一嵌入率和混合嵌入率的检测正确率

Table 2 ACC for different methods with single embedding rate and mixed embedding rate

采用的方法	测试图像嵌入率						混合嵌入率
	0.15	0.25	0.35	0.45	0.55	0.75	
方法 1	91.00	95.95	97.20	97.10	98.20	98.70	
方法 2	81.85	92.80	95.80	96.85	97.45	97.65	93.10
本文方法	87.30	96.50	97.45	97.60	97.60	97.60	94.65

表 3 不同方法对单一嵌入率和混合嵌入率的虚警率

Table 3 FP for different methods with single embedding rate and mixed embedding rate

采用的方法	测试图像嵌入率						混合嵌入率
	0.15	0.25	0.35	0.45	0.55	0.75	
方法 1	9.9	5.3	4.6	5.5	3.2	2.4	
方法 2	4.2	4.2	4.2	4.2	4.2	4.2	4.2
本文方法	4.7	4.7	4.7	4.7	4.7	4.7	4.7

3　结束语

本文采用基于 D-S 证据理论的多分类器融合技术来解决未知嵌入率下的有效检测问题。通过实验观察到，低嵌入率训练的分类器在不同嵌入率的测试图像上检测率高，同样虚警率也高，而高嵌入率训练的分类器在不同嵌入率的测试图像上检测率较低，但虚警率也低。在实际检测系统中，过高的虚警率会造成大量无意义的工作，而较低的检测率也会失去其检测的意义。

本文提出的方法无论是检测率还是虚警率都能按照实际工作的需求来设计，检测性能和虚警率在整体上有较大的改善，并且通过对参数的选择可以实现实际工作中的不同需要，实现了对未知嵌入率下的载密图像的有效检测，但在低嵌入率时与固定嵌入率训练的分类器相比还有一定的提升空间。下一步计划通过研究组合分类器的方法来实现对低嵌入率下的有效检测。虽然本文主要针对空域 LSB 匹配未知嵌入率的检测进行实验，本文方法对于其他的隐写算法也同样适用。

参考文献：

[1] Petitcolas F, Anderson R, Kuhn M. Information hiding—A survey[J]. Proceedings of the IEEE, 1999,87(7):1062-1078.

[2] Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and gray-scale images[J]. Magazine of IEEE Multimedia, Special Issue on Security, 2001,8(4):22-28.

[3] Westfeld A, Pfitzmann A. Attacks on steganographic systems[C]//Third International Workshop on Information Hiding, Lecture Notes in Computer Science. Dresden, Germany: Springer, 1999:61-76.

[4] Dumitrescu S, Wu Xiaolin, Wang Zhe. Detection of LSB steganography via simple pair analysis[J]. IEEE Trans Signal Process, 2003,51(7):355-372.

[5] Sharp T. An implementation of key-based digital signal steganography[C]//Proceedings of 4th Information Hiding Workshop, Lecture Notes in Computer Science. Berlin:Springer-Verlag, LNCS 2137,2001:13-26.

[6] Zhang Jun, Cox I, Doërr G. Steganalysis for LSB matching in images with high-frequency noise[C]//Proceedings of the IEEE International Workshop on Multimedia Signal Processing. Chania Crete, Greece: IEEE, 2007:385-388.

[7] Zhang Tao, Li Wenxiang, Zhang Yan, et al. Steganalysis of LSB matching based on statistical modeling of pixel difference distributions[J]. Information Science, 2010,180(23):1288-1291.

[8] Farid H, Lyu S. Steganalysis using higher-order image statistics[J]. IEEE Transactions on Information Forensics and Security, 2006,1(1):111-119.

[9] Shi Yunqing, Xuan Guorong, Zou Dekun, et al. Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network [C]//Proceedings of IEEE ICME. New Orleans, USA:[s. n.], 2005: 269-272.

[10] Shi Yunqing, Xuan Guorong, Yang Chengyun, et al. Effective steganalysis based on statistical moments of wavelet characteristic function[C]//Proceedings of International Conference on Information Technology: Coding and Computing. Las Vegas, USA:[s. n.], 2005:768-773.

[11] 刘学谦，平西建，张涛，等. 基于滤波复原的小波特征 LSB 匹配隐写分析方法[J]. 数据采集与处理，2010，25(4):505-511.
Liu Xueqian, Ping Xijian, Zhang Tao, et al. Steganalysis of LSB matching based on wavelet feature of filtering restoration[J]. Journal of Data Acquisition and Processing, 2010,25(4):505-511.

[12] Cai Kaiwei, Li Xiaolong, Zeng Tieyong, et al. Reliable histogram features for detecting LSB matching [C]//Proceedings of IEEE International Conference on Image Processing. Piscataway, NJ, USA: IEEE, 2010:1761-1764.

[13] Cancelli G, Barni M, Doërr G, et al. A comparative study of ±1 steganalyzers[C]//Proceedings of the IEEE International Workshop on Multimedia Siganl Processing. Atlanta, Georgia, USA: IEEE, 2008: 791-796.

[14] Marvel L, Henz B, Boncelet C. A performance study of ±1 steganalysis employing a realistic operating scenario[C]//2007 IEEE MILCOM Conference. Albany, NewYork, USA: IEEE, 2007:1-7.

[15] Marvel L, Henz B, Boncelet C. Fusing rate-specific SVM classifiers for ±1 embedding steganalysis[C]//Proceedings of CISS 2008. Cocumbus, Ohio, USA: [s. n.], 2008:361-364.

[16] Kharrazi M, Sencar H, Memon N. Improving steganalysis by fusion techniques: A case study with image steganograohy[J]. Transactions on DHMS I, LNCS 4300. Tallahassee, USA:[s. n.], 2006:123-

1372.

[17] 孙子文,李慧,纪志成. 基于 D-S 证据理论的融合图像隐写分析[J]. 控制与决策,2011,26(8):1-5.
Sun Ziwen, Li Hui, Ji Zhicheng. Fusion image steganalysis based on Dempster-Shafer evidence theory[J]. Control and Decision, 2011,26(8):1-5.

[18] Burges C. A tutorial on support vector machines for pattern recognition [J]. Data Mining and Knowledge Discovery, 1998,2(2):121-167.

[19] 叶清,吴晓平,宋业新. 基于权重系数与冲突概率重新分配的证据合成方法[J]. 系统工程与电子技术,2006,28(7):1014-1016.
Ye Qing, Wu Xiaoping, Song Yexin. Evidence combination method based on the weight coefficients and the confliction probability distribution[J]. Systems Engineering and Electronics, 2006, 28(7): 1014-1016.

[20] Doërr G. Image database for steganalysis studies [EB/OL]. http://www.cs.ucl.ac.uk/staff/I.Cox/Content/Down-loads.html,2008-05-06/2012-06-06.

[21] Chang C, Lin C. LIBSVM: A library for support vector machines[EB/OL]. http://www.csie.ntu.edu.tw/~cjlin/libsvm, 2007-06-14/2012-06-06.

作者简介:万宝吉(1986-),男,硕士研究生,研究方向:信息隐藏、信息融合,E-mail:dirker2012@163.com;张涛(1977-),男,副教授,研究方向:信息隐藏、图像处理、模式识别;李文祥(1986-),男,博士,研究方向:信息隐藏、图像取证;侯晓丹(1989-),女,硕士研究生,研究方向:信息隐藏、图像取证;朱振浩(1988-),男,硕士研究生,研究方向:信息隐藏。