基于择多准则的新隐写分析方法*

邓诗智[1,2]，张卫明[1,2]，刘九芬[1,2]

(1. 解放军信息工程大学,信息工程学院 信息研究系，郑州 450002; 2. 中国科学院 研究生院 信息安全国家重点实验室，北京 100049)

摘 要: 为了达到更为可靠的检测,综合利用现有的检测算法,根据择多准则提出了一个择多分类算法的简化模型,得到了择多分类算法的理论错误分类概率的表达式,错误分类概率的上界和分类效果与检测算法数目的关系。应用该算法到图像空域 LSB(least significant bit) 隐写的分类问题,得到的实验结果表明该算法在一定程度上改善了分类效果。

关键词: 隐写分析; 择多准则; ROC 分析

中图分类号: TP391 **文献标志码**: A **文章编号**: 1001-3695(2007) 09-0118-03

New steganalysis approach based on majority theory

DENG Shi-zhi[1,2], ZHANG Wei-ming[1,2], LIU Jiu-fen[1,2]

(1. Dept. of Information Research, Institute of Information Engineering, the PLA Information Engineering Univercity, Zhengzhou 450002, *China; 2. State Key Laboratory of Information Security, Graduate School, Chinese Academy Sciences, Beijing* 100049, *China)*

Abstract: To detect more reliably synthesizing , this paper gave a simplified frame with the majority theory. It got the expression and the upper bound of the new method's theoretic wrong classifying probability along with the relationship between the classifying effect and the number of detecting methods. Applying the frame into LSB steganalysis in spatial domain, the experiment's result shows that the new approach improves the classifying effect in a sense.

Key words: steganalysis; majority theory; ROC analysis

信息安全保障了国家安全和社会稳定。信息隐藏作为新兴的技术成为信息安全的热点问题。数字隐写(steganography) 和隐写分析(steganalysis) 是信息隐藏的重要分支。前者是将秘密消息隐藏在载体中进行传送而不引起第三方怀疑,达到隐蔽通信的目的;后者是对数字隐写的攻击,如对隐秘信息的检测、提取、恢复和破坏。数字隐写隐藏了互相通信的事实,成为隐蔽通信的有效方式。尽管如此,数字隐写可能被不法使用,成为危害国家政治和经济安全的工具(媒体多有报道) 。到目前为止,因特网上有超过 200 种隐写软件,这些均可能被一般人使用。总而言之,隐写分析是迫切需要研究的领域。

目前,在隐写分析领域中开展的研究基本上集中于对隐蔽信息的检测。由于 LSB (least significant bit) 隐写方法使用的广泛性,针对它的隐蔽信息检测更是隐写分析的重点。其中性能较好的算法有 RS 方法[1]、SPA 方法[2]、DIH 方法[3]、EsLsb 方法[4]、improved SPA 方法[5]。D. K. Andrew[6] 则通过大量的实验评估了 Pairs [7]、RS 和 SPA 分析方法的可靠性,并对这三种方法给出了多种改进方案。本文综合利用已有检测算法,提出了一种新的隐写分析方法,笔者称这种方法为择多分类方法。

1 择多分类算法的简化框架

隐蔽信息的检测可以看做是一个分类问题,即判断检测对象是属于载体对象的集合还是载密对象的集合。错误分类是指分类结果与实际不相符,也就是说,检测对象为载体对象却被归类为载密对象,检测对象为载密对象却被归类为载体对象。

设有 N 个用于分类检测对象的检测算法,每个算法的错误分类概率均小于 1/2。针对每个检测对象,应用这 N 个算法进行分类,并统计分类结果。根据择多准则,出现次数最多的分类结果被认为是检测对象的类型。这种综合利用多种检测算法进行分类的算法称之为择多分类算法。下面给出择多分类算法的简化模型。

假设一个检测算法的分类结果只有载体对象和载密对象两类。设可利用的检测算法数目为 $2k+1$。其中: $k=1,2,3,\cdots$。取算法数目为奇数是为了避免择多准则下讨论两类结果时,出现两类结果的算法数目相等的情况。

用随机变量 X 表示一个检测算法分类的结果,设其错误

收稿日期: 2006-06-29; 修返日期: 2006-09-07 基金项目: 国家自然科学基金资助项目(60473022);河南省自然科学基金资助项目(0511011300)

作者简介: 邓诗智(1984-),男,安徽桐城人,硕士研究生,主要研究方向为信息隐藏、隐写分析(happydsz@ sohu.com);张卫明(1976-),男,河北保定人,讲师,博士研究生,主要研究方向为密码学、信息隐藏;刘九芬(1963-),女,河南焦作人,副教授,硕导,主要研究方向为小波理论及其应用、信息隐藏与数字水印.

分类的概率是 $p, 0 < p < 1/2$。记 $P\{$错误分类$\} = P\{X = 1\} = p < 1/2$, $P\{$正确分类$\} = P\{X = 0\} = 1 - p > 1/2$。又设 $2k+1$ 种不同检测算法分类结果对应的随机变量分别为 $X_1, X_2, \cdots, X_{2k+1}$。

定理 1　设 $2k+1$ 种不同检测算法分类结果对应的随机变量 $X_1, X_2, \cdots, X_{2k+1}$ 与随机变量 X 同分布, 而且 $2k+1$ 种检测算法的分类过程相互独立, 则择多分类算法的错误分类概率为 $p' = \sum_{i=0}^{k} C_{2k+1}^{1} (1-p)^i p^{2k+1-i}$。

证明　这是一个贝努里概型。根据择多准则, 在 $2k+1$ 个分类结果中, 择多分类算法的错误分类概率等于错误分类结果出现次数超过 k 次的概率。

据二项分布的概率表达式得到 $p' = \sum_{i=k+1}^{2k+1} C_{2k+1}^{i} p^i (1-p)^{2k+1-i} = \sum_{i=k+1}^{2k+1} C_{2k+1}^{2k+1-i} p^i (1-p)^{2k+1-i} = \sum_{i=p}^{k} C_{2k+1}^{i} (1-p)^i p^{2k+1-i}$

从图 1 看出, 随着 $2k+1$ 的增加, p 趋向于 0。其中单个算法的错误分类概率 $p = 0.15$。

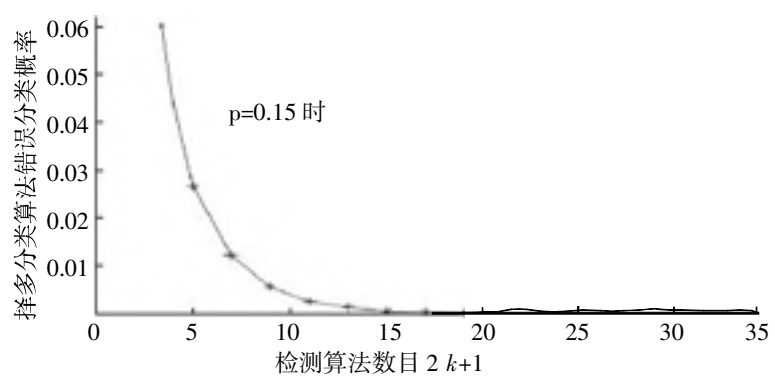

图 1　算法数目和择多分类算法错误分类概率的关系图

引理 1　(Chernoff Bound)[8]　设 $p \leq 1/2$, $X_1, X_2, \cdots, X_{2k+1}$ 是相互独立的 0 - 1 随机变量, 对每个 i 有 $P\{X_i = 1\} = p$。当 $0 < \varepsilon \leq p(1-p)$ 时, 有

$$P\left\{\left|\sum_{i=1}^{n} X_i / n - p\right| > \varepsilon\right\} < 2 \cdot e^{-\{\varepsilon^2 / [2p(1-p)]\} n}$$

定理 2　在定理 1 的条件下, 择多分类算法的错误分类概率 P 满足如下不等式:

当 $1 - \sqrt{2}/2 \leq p < 1/2$ 时, $P' \leq 2e^{(1/2-p)^2/[2p(1-p)] \cdot (2k+1)}$

当 $0 < p < 1 - \sqrt{2}/2$ 时, $P' < 2e^{-[p(1-p)(2k+1)]/2}$

证明　根据择多准则, 在 $2k+1$ 个分类结果中, 择多分类算法的错误分类概率等于错误分类结果出现次数超过 k 次的概率, 且 k 是整数, 有

$$p' = P\left\{\sum_{i=1}^{2k+1} X_i \geq k+1\right\} \leq P\left\{\left|\sum_{i=1}^{2k+1} X_i/(2k+1) - p\right| \geq 1/2 - p\right\}$$

根据引理 1 得到: 当 $1/2 - p \leq p(1-p)$, 即 $1 - \sqrt{2}/2 \leq p < 1/2$ 时, $p' \leq P\left\{\left|\sum_{i=1}^{2k+1} X_i/(2k+1) - p\right| \geq 1/2 - p\right\} < 2e^{(1/2-p)^2/[2p(1-p)] \cdot (2k+1)}$; 当 $1/2 - p > p(1-p)$, 即 $0 < p < 1 - \sqrt{2}/2$ 时, $p' \leq P\left\{\left|\sum_{i=1}^{2k+1} X_i/(2k+1) - p\right| \geq 1/2 - p\right\} < P\left\{\left|\sum_{i=1}^{2k+1} X_i/(2k+1) - p\right| \geq p(1-p)\right\}$。

再根据引理 1 得到

$$p' < 2e^{[p(1-p)]^2/[2p(1-2)] \cdot (2k+1)} = 2e^{[-p(1-p)(2k+1)]/2}$$

从上界的表达式可以看出, 择多分类算法的出错概率 p 随着检测算法数目 $2k+1$ 的增加呈指数减小。推论 1 表明其错误分类概率随着算法数目的无限增加趋向于 0。推论 2 给出在给定择多分类算法错误分类概率的情况下, 所需要检测算法的数目。

推论 1　在定理 1 的条件下, 择多分类算法的错误分类概率 p 满足 $\lim_{2k+1 \to \infty} p' = 0$。

推论 2　在定理 1 的条件下, 给定错误分类概率 p 的上界 ρ 则当 $1 - \sqrt{2}/2 \leq p < 1/2: 2k+1 \geq -\ln(\rho/2)/[2(1/2-p)^2]$ 时, 满足 $p' \leq \rho$; 当 $0 < p < 1 - \sqrt{2}/2: 2k+1 > -(1/2)\ln(\rho/2)$ 时, 满足 $p' < \rho$。

2　择多分类算法应用实例: 空域 LSB 隐写分类问题

正确分类是指分类结果与实际相符。检测率是指将载密对象正确分类为载密对象的概率。分类不可避免地出现错误, 将载体对象错误分类为载密对象的概率称为虚警率, 将载密对象错误分类为载体对象的概率称为漏报率。

用全局检测率来表示正确分类的概率。定义全局检测率为

$$Pr = 1 - Pe \tag{1}$$

其中: Pe 为平均错误概率: $Pe = \eta P$(隐藏消息) + αP(非隐藏消息); η 为漏报率; α 为虚警率; P(隐藏消息) 为检测对象中随机抽取到载密的概率; P(非隐藏消息) 为检测对象中随机抽取到载体的概率。

用 ROC(receiver operating characteristic) 曲线图反映阈值连续变化时, 虚警率和检测率的对应关系。

2.1　择多分类算法具体步骤

第一章提出的模型是一个简化模型, 假设所有算法的错误分类概率均相等, 对应的正确分类概率即全局检测率也相等, 首先需要通过实验得到每个算法的阈值 $\alpha_i, i = 1, 2, \cdots, 2k+1$, 这些阈值用于判断是否载密, 当检测结果大于阈值认为载密, 小于阈值认为载体。

a) 选择进行检测的 $2k+1$ 种算法, 并对大量图像进行实验得到该检测算法的 ROC 曲线图。根据 ROC 曲线的数据得到阈值、虚警率和检测率三者的对应关系。根据式(1) 得到阈值和全局检测率的对应关系。记每个算法均能取到的最大全局检测率为 Pr, 检测算法对应的阈值 α_i, $i = 1, 2, \cdots, 2k+1$。

b) 针对一个检测对象, 检测算法对嵌入率(嵌入秘密消息长度占图像整个长度的比例) 的估计值为 p_i, $i = 1, 2, \cdots, 2k+1$。根据择多准则, 定义分类结果为

$$\text{result} = \sum_{i=1}^{2k+1} \text{sgn}(p_i \geq \alpha_i)$$

其中: $\text{sgn}(p_i \geq \alpha_i) = \begin{cases} 1, & p_i \geq \alpha_i \\ -1, & p_i < \alpha_i \end{cases}$。

分类算法的总数目 $2k+1$ 是奇数, 所以 result $\neq 0$; 当 result > 0 时分类检测对象为载密对象, 当 result < 0 时分类检测对象为载体对象。

c) 统计分类的结果, 得到择多分类算法的分类效果, 包括虚警率、检测率和全局检测率。

2.2 应用择多分类算法于空域 LSB 隐写

选取 3 000 幅 800 ×600 ×8 bit BMP 图像为载体对象,应用空域 LSB 隐写算法嵌入 0.05 bit/pixel 的密文序列于载体对象构成载密对象,载体图像和载密对象在一起构成检测对象。由于载体和载密数目相等,利用式(1)计算全局检测率时的 P(隐藏消息)和 P(非隐藏消息)均为 1/2。

2.2.1 实验步骤与结果

a) 选取五种针对空域 LSB 隐写的检测算法分别为 RS、SPA、DIH、EsLsb、improved SPA。对包含 5 000 幅 BMP 图像的图像库进行实验,得到五种算法的 ROC 曲线图,见图 2。根据 ROC 曲线的数据,选择合适的全局检测率 Pr = 0.890,得到五种算法的阈值分别为 0.034 43、0.063 92、0.022 19、0.024 28、0.034 47。

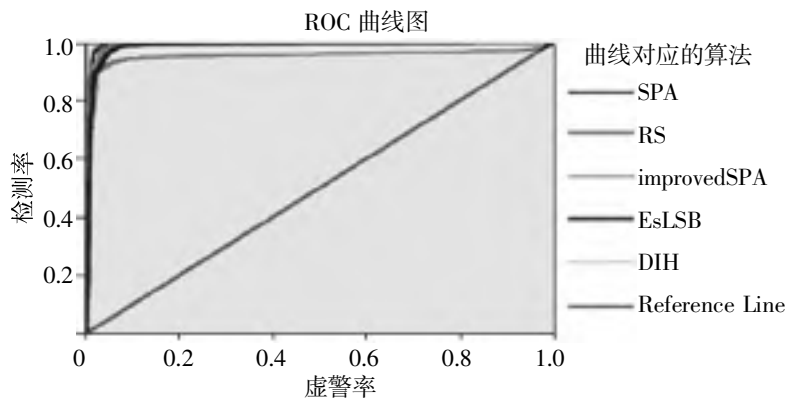

图 2 五种算法对应的 ROC 曲线图

b) 按照 2.1 节的步骤 a) 和 b),对 6 000 幅检测对象利用前三种检测算法进行检测,结果如表 1 所示;使用五种检测算法进行检测得到更好的结果如表 2 所示。

表 1 RS、SPA、DIH 算法和择多分类算法的分类效果比较

算法	阈值	虚警率/%	检测率/%	全局检测率/%
RS[1]算法	0.034 43	0.076	0.856	0.890
SPA[2]算法	0.063 92	0.113	0.889	0.888
DIH[3]算法	0.022 19	0.176	0.956	0.890
择多分类算法	无	0.075 9	0.907 0	0.915 5

表 2 五种算法和择多分类算法的分类效果比较

算法	阈值	虚警率/%	检测率/%	全局检测率/%
RS[1]算法	0.034 43	0.076	0.856	0.890
SPA[2]算法	0.063 92	0.113	0.889	0.888
DIH[3]算法	0.022 19	0.176	0.956	0.890
EsLsb[4]算法	0.024 28	0.121	0.901	0.890
improved SPA[5]算法	0.034 47	0.060	0.840	0.890
择多分类算法	无	0.065 4	0.915 0	0.924 8

从表 1、2 可以看出,择多分类算法的虚警率和检测率与五种算法中最优值相差不大,尤其是虚警率,几乎保持与最优的算法相当的水平。往往虚警率的降低是以牺牲检测率为代价;反之亦然。从表 1、2 可以看出,择多分类算法同时改进了虚警率和检测率,将较优的虚警率和检测率集中在一个分类算法中。表 1 的结果利用的是三种检测算法,表 2 则是五种检测算法。比较这两个表可知,利用五种检测算法的择多分类算法的结果要优于只用三种检测算法的结果。

2.2.2 误差分析和改进

根据建立的择多分类算法框架,$2k+1=3$ 时全局检测率的理论值是 0.966 4,而实际值是 0.915 5。$2k+1=5$ 时全局检测率的理论值是 0.988 8,而实际值是 0.924 8。原因在于,实验中利用检测算法的分类结果并不是严格满足相互独立条件。

实际上,检测算法的相互独立条件比较强,可以弱化这个条件,如要求检测算法两两独立等。除此之外,可以选择更多的检测算法应用到新算法中,以弥补条件不严格成立的缺陷,并且随着算法数目的增加,检测率会快速提高。

3 结束语

本文给出了简化的择多分类算法框架,得到理论错误分类概率,分析了择多分类算法错误分类概率与检测算法数目的关系。对空域 LSB 隐写分类的实验表明,择多分类算法同时改进了虚警率和检测率,提高了全局检测率。值得一提的是,择多分类算法同样适合于针对其他隐写方法的检测算法,比如针对 $\pm k$ 随机嵌入的隐写分析算法。

本文只是给出了一个简化的择多分类算法框架,更加实际的模型有待完善。为了进一步提高分类效果,可以通过寻找更多满足条件的检测算法进行择多分类。

新算法模型表明当检测算法越来越多时,错误分类概率会越来越小。由于检测算法的不断提出,加上算法独立性要求的弱化,寻找更多满足条件的检测算法是可行的。

参考文献:

[1] RIDRICH J, GOLJAN M, DU R. Reliable detection of LSB steganography in grayseale and color images[C]//Proc of ACM, Special Session on Multimedia Security and Watermarking. Ottawa: [s. n.], 2001. 27-30.

[2] DUMITRESCU S, WU Xiao-lin, WANG Zhe. Detection of LSB steganography via sample pair analysis[C]//Proc of the 5th International Workshop on Information Hiding, LCNS 2578. Berlin: Springer-Verlag, 2002: 55-372.

[3] ZHANG Tao, PING Xi-jian. A new approach to reliable detection of LSB steganography in natural images[J]. Signal Processing, Elsevier Science, 2003, 83(10): 2085-2093.

[4] FRIDRICH J, GOLJAN M. On estimation of secret message length in LSB steganography in spatial domain[C]//Security, Steganography and Watermaking of Multimedia Contents. San Jose: SPIE Press, 2004, 5306: 23-34.

[5] LU Pei-zhong, LUO Xiang-yang, TANG Qing-yang, *et al*. An improved sample pairs method for detection of LSB embedding[C]//Proc of the 6th International Hiding Workshop. Berlin: Springer-Verlag, 2004: 116-127.

[6] KER A D. Improved detection of LSB steganography in grayscale images[C]//Proc of the 6th Information Hiding Workshop. Berlin: Springer-Verlag, 2004: 97-115.

[7] FRIDRICH J, GOLJAN M, SOUKAL D. Higher-order statistical steganalysis of palette images[C]//Proc of SPIE: Security and Wartemar King of Multicmedia Contents V. 2003: 178-190.

[8] GOLDREICH O. Foundations of cryptography[M]. Beijing: Publishing House of Electronics Industry, 2003: 11-12.