

隐密分析系统中的特征选择方法研究

姜莹¹, 孔祥维¹, 尤新刚^{1,2}, 王波¹

(1. 大连理工大学 信息安全研究中心, 辽宁 大连 116024; 2. 北京电子技术应用研究所, 北京 100091)

摘 要: 隐密分析技术的目的是能够准确、高效的对隐密术进行分析; 通用的盲隐密分析方法提取的大量统计特征增加了隐密分析系统的复杂度, 影响了隐密分析系统的效率. 文中在对特征选择方法进行研究的基础上, 利用 RELIEF 算法去除对分类贡献小的弱特征, 利用特征之间的相关性去除特征空间中的冗余特征. 实验结果表明该方法能够在保持原始算法分类能力的基础上, 有效地削减特征维数, 从而提高了隐密分析系统效率.

关键词: 隐密分析; 特征选择; RELIEF; 特征相关性;

中图分类号: **文献标识码:** A **文章编号:** 0367-6234(2006)增刊-0860-03

Feature selection for steganalysis

JIANG Ying¹, KONG Xiang-wei¹, YOU Xin-gang^{1,2}, WANG Bo¹

(1. Information Security Research Center, Dalian University of Technology, Dalian 116024, China;

2. Beijing Institute of Electronic Technology and Application, Beijing 100091, China)

Abstract: The purpose of steganalysis is attacking steganography exactly and efficiently. Training based blind steganalytic algorithms utilize multi-dimensional feature vectors to form a high order statistical model and the huge number of features results in increasing complexity and decreasing efficiency of the steganalytic system. In order to solve this problem, feature selection methods are studied in this paper. RELIEF algorithm is utilized to cut down the features which have little contribution to classification and correlation based method is utilized to remove redundant features from feature space. The experimental results indicate that the method can eliminate the number of features effectively while maintaining the classification ability of the original algorithm.

Key words: steganalysis; feature selection; RELIEF; feature correlation

隐密分析是对隐写术的攻击, 目前的隐密分析方法可以分为专用的隐密分析方法和通用的隐密分析方法两大类. 专用的隐密分析方法针对特定的隐密算法进行分析^{[1][2]}, 而通用的隐密分析方法通过提取图像特征建立高阶统计模型, 利用分类器进行分类判决. 这种隐密分析方法不局限于单一的隐密算法, 通常对几种隐密算法都适用.

Farid^[3]提出的基于小波统计特性的隐密分析方法通过提取各个小波子带以及其优化线性预测误差的均值、方差、峰度和斜度组成 72 维的特征空间. 文献[4]进一步引入相位统计信息, 对于

彩色图像建立了高达 432 维的特征空间. Yun Q. Shi 等^[5]提出的基于小波特征函数统计特性的隐密分析方法通过提取图像及小波子带直方图特征函数的重心得到了 39 维的特征向量. Fridrich 等^[6]提出的基于特征的盲隐密分析方法在对 JPEG 图像隐密前后特性进行分析的基础上, 提出了二十三维的特征集合. 可见, 通用的隐密分析方法一般需要提取大量特征组成特征空间, 这些特征中不可避免的存在对分类贡献很小的特征和彼此相关性很大的特征. 直接利用这些特征进行训练及分类, 使得通用的隐密分析方法十分复杂, 时间复杂度高. 本文对特征选择方法进行了研究, 能够在保证分类正确率的前提下, 对特征空间进行降维, 从而缩减分析时间, 提高分类器效率. 由于基于特征的盲隐密分析方法对大部分的针对

收稿日期: 2006-03-31.

基金项目: 国家自然科学基金资助项目(60572111).

作者简介: 姜莹(1980-), 女, 硕士;

孔祥维(1963-), 女, 教授, 博士生导师.

JPEG 图像的隐密算法有着较好的分析能力,分析效果优于其他的通用隐密分析方法,本文就以该算法为例,进行特征选择的研究与实验。

本文分四部分,第一部分介绍 RELIEF 算法的基本原理;第二部分给出了利用特征之间相关性去除冗余特征的基本方法;第三部分给出了以基于特征的盲隐密分析方法为例进行特征选择的实验结果;最后是结论。

1 RELIEF 算法

特征选择方法的目的是在不降低识别率的前提下尽量降低特征维数。按照特征子集的形成方式,特征选择方法可以分为穷举法,启发法和随机法。穷举法虽然能获得最优解,但是其巨大的算法复杂度和时间耗费使其很难在实际中应用。随机法是一种较新的特征子集搜索方法,但是它存在算法复杂,参数设置困难的问题。启发法是一种近似算法,一般情况下能够获得接近最优解的次优解,相比与其他两种方法,它的算法简单,实现容易。RELIEF^[7]是应用最为广泛的启发式的特征选择方法,它通过权值搜索进行特征子集选择。权值搜索的方法为每维特征赋予一个权值,以权值表征特征与类别的相关性,也就是特征对于分类的贡献。通过不断调整权值逐步显现出特征与类别的相关性,最后选择权值较大的那些特征。

RELIEF 算法中一个重要概念是假设间隔 θ ,它指的是在保持样本分类不变的情况下决策面所能移动的最大距离:

$$\theta = \frac{1}{2}(\|x - M(x)\| - \|x - H(x)\|) \quad (1)$$

其中 $H(x), M(x)$ 为 x 的同类和非同类最近邻点。将各样本的假设间隔累加起来作为特征的权值。样本 x 更新特征 p 权值的公式为: $W_p^{i+1}(x) = W_p^i(x) - \text{diff}(p, x, H(x))/m + \text{diff}(p, x, M(x))/m$ (2)

对于连续特征:

$$\text{diff}(p, x, x') = \frac{|x_p - x'_p|}{\max(p) - \min(p)} \quad (3)$$

如果一个特征对分类贡献较大,意味着同类样本的距离较近,而不同类样本的距离较远。那么 m 个样本中大部分样本的假设间隔会较大,从而导致该特征的权值较大。特征的权值表征的就是特征对分类的贡献大小,在此引入弱特征的概念:

定义:弱特征指的是与类别不相关或者是对分类贡献较小的特征,在 RELIEF 算法中,若

$W_p(x) < \delta, \delta$ 为门限值,则称特征 x 为弱特征。

RELIEF 算法根据特征的权值进行排序,去除权值较小的弱特征。对于两类的分类问题,可以很好的去除弱特征。

2 利用相关性去除冗余特征

虽然 RELIEF 算法可以去除特征空间中的弱特征,但是,特征空间中除了弱特征之外,还存在大量的冗余特征。文献[8]指出:在原始特征集中增加或删除冗余特征,不影响该特征集的分类能力。因此我们应该在去除弱特征的基础上,进一步的去除彼此之间相关性很大的冗余特征。特征之间的相关性有多种评价方式,这里采用最大信息压缩准则来衡量特征之间的相关性。最大信息压缩准则 $(\lambda_2)_{xy}$ 定义如下:

$$(\lambda_2)_{xy} = \frac{1}{2}[(\text{var}(x) + \text{var}(y)) - \sqrt{(\text{var}(x) + \text{var}(y))^2 - 4\text{var}(x)\text{var}(y)(1 - \rho(x, y)^2)}] \quad (4)$$

其中 $\text{var}(x)$ 表示 x 的方差, $\rho(x, y)$ 表示 x, y 之间的相关系数。随着 x 与 y 之间相关性的降低, $(\lambda_2)_{xy}$ 的值逐渐增大。容易证明,最大信息压缩准则满足对称性,并且对变量缩放敏感,适合于用于特征降维。

基于以上的分析,我们将 RELIEF 算法和去除冗余特征的方法结合起来,进行特征选择,算法步骤如下:

第一步:去除弱特征。利用 RELIEF 算法,去除权值趋近于 0 以及权值较小的弱特征,将剩下的特征按照权值大小进行排序,得到特征集合 $F = \{f_1, f_2, \dots, f_m\}$ 。

第二步:去除冗余特征,利用最大信息压缩准则确定 F 中特征之间的相关性,若 $(\lambda_2)_{ff_j} < \theta$, 表示特征 i, j 之间的相关性很强,也就是说 i, j 互为对方的冗余特征,故去掉其中对分类贡献较小的特征。

第三步:输出经筛选后的 F ,即为最后选取出的特征。

本文利用上述方法,以基于特征的盲隐密分析方法为例,进行了特征选择实验,在第三部分中给出了详细的实验结果和分析。

3 实验结果

基于特征的盲隐密分析方法^[6]通过提取 DCT 系数直方图的统计特征,空域块不连续性的扩展特征以及块与块之间的相关性信息等组合成

为二十三维的特征向量空间大量实验表明该方法具有较高的检测可靠性,因此本文以此为例进行实验,需要注意的是本文提出的是一个通用的特征选择方法,在其它的特征集合上也是适用的。

实验选取 Nikon E5700 相机拍摄的 JPEG 格式自然图像 500 幅(200 幅训练,300 幅测试)。分别按照 Jsteg, F5, OutGuess 的算法原理隐藏信息。文献[6]虽然给出了单一特征下的分类性能,但是按照单一特征的分类能力进行特征降维并不能取得满意的实验结果,这是因为特征之间存在不同程度的相关性。因此我们利用 RELIEF 加去除冗余特征的方法进行降维实验。在特征选择之前将数据归一化到[0,1]之间。

表 1 中给出了特征选择后的实验结果。图中隐密图像的信息含量分别为隐密信息最大容量的 15%, 50%, 100% (下面提到的信息

含量均指的是对应于载体图最大容量的相对容量)。这里,对分类正确率采用检测可靠性 $\rho = 2A - 1$ 来衡量,其中 A 表示 roc 曲线下的面积, $\rho \in [0, 1]$, ρ 的大小体现了分类器分类能力的强弱。为了直观起见,还专门给出了如图 1 中所示的针对 Jsteg 算法的实验结果,从该图可以直观的看到降维后的特征子集仍然可以保持较高的检测可靠性。

由实验结果可以看出,对特征空间降维后,攻击算法仍可以达到很高的识别率。从图 1 中容易看出,有时还能够达到相对于原始特征空间更好的分类效果。这是因为弱特征和冗余特征的存在有可能为分类器引入噪声。此外,通过实验结果我们可以看出,信息含量越高,特征空间可降维的潜力就越大,如信息含量为 100% 时,特征维数降到 3 维时,仍可以达到非常好的检测效果。这是因为

在信息含量大的时候特征变化显著,因此少量的特征便可以达到和原始特征空间相同的效果。由于实际中要求分析方法尽可能的对低信息含量的隐密图也具有很好的分析能力,因此我们使用针对小信息含量隐密图提取出的特征,来对大信息含量的隐密图进行分析。根据表 1 的实验结果,我们利用特征空间降到 6 维时,针对信息含量为 15% 的隐密图所选择出的 6 个特征,组合成特征空间 F_6 ,对相应的信息含量分别为 50% 和 100% 的测试库进行检测,实验结果如表 2。

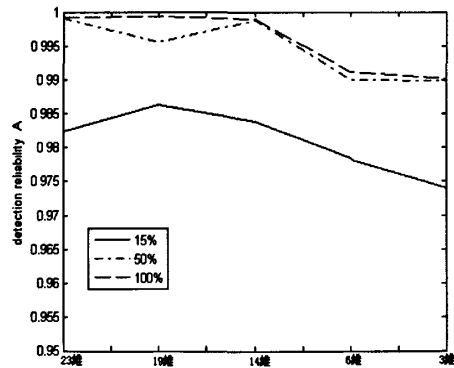


图 1 针对 Jsteg 隐密算法的实验结果

由实验结果可以看出,用针对低信息含量隐密图所选取出的特征来分析高信息含量的隐密图,可以达到和原始特征空间几乎相同的准确率。

此外,特征选择的结果有助于我们更好地对特征进行分析,进而指导以后的特征提取工作。对特征强弱和相关性的研究,可以帮助我们更加直观的理解隐密算法对图像统计特性造成的影响,进而提取出更有意义的统计特征,这对今后隐密分析算法的设计有重要的指导意义。

表 1 RELIEF 与去除冗余特征结合进行特征选择

Method	Rate	23D	19D	14D	6D	3D
Jsteg	15%	0.9824	0.9863	0.9839	0.9785	0.9744
	50%	0.9991	0.9956	0.9987	0.9900	0.9898
	100%	0.9992	0.9993	0.9989	0.9912	0.9901
F5	15%	0.7101	0.7165	0.6678	0.6456	0.3587
	50%	0.9800	0.9821	0.9851	0.9800	0.9721
	100%	0.9891	0.9916	0.9858	0.9821	0.9800
OutGuess	15%	0.9668	0.9555	0.9192	0.9229	0.7312
	50%	0.9885	0.9881	0.9864	0.9565	0.9423
	100%	0.9980	0.9985	0.9955	0.9901	0.9823

the stego key [A]. Security, Steganography and Watermaking of Multimedia Contents of EI SPIE 5306 [C], 2004, 70 - 82.

[6] Hide2Bmp v1.0a. <http://allnews.3322.org:802/godbest/Hide2Bmp.rar>.

[7] Masker v7.0.2. <http://yzdown.com/soft/10894.htm>.

[8] Stegspy2.1. <http://www.spy-hunter.com/index.html>.

[9] CHANDRANMOULI R. A mathematical framework for active steganalysis [J]. ACM Multimedia Systems Journal, Special Issue on Multimedia Watermarking, 2003, 9(3):301 - 311.

[10] TRIVEDI S, CHANDRANMOULI R. Active steganalysis of sequential steganography [A]. SPIE conference 5020(13) [C], California, 2003, 123 - 130.

[11] TRIVEDI S. Secret key estimate in sequential steganography [D]. Hoboken, New Jersey: Stevens Institute of Technology, 2003.

[12] WESTFELD A, PFITZMANN A. Attacks on Steganographic Systems [A]. Proc. the Third Information Hiding Workshop, LNCS 1768 [C], New York: Springer - Verlag, 1999, 61 - 76.

[13] MA Ning, ZHANG Weiming, LIU Wenfen. Extracting Attack to Sequential JSteg Stegosystems [A]. Proceedings of the 10th Joint International Computer Conference [C], Beijing: International Academic Publishers, World Publishing Corporation, 2004, 277 - 281.

[14] ZHANG Weiming, LI Shiqu. Security Measurements of Steganographic Systems [A]. Proc. The Second International Conference of Applied Cryptography and Network Security. LNCS 3089 [C], New York: Springer - Verlag, 2004, 194 - 204.

[15] ZHANG Weiming, LI Shiqu, CAO Jia et al. Information - Theoretic Analysis for the Difficulty of Extracting Hidden Information [J]. Wuhan University Journal of Natural Sciences, 2005, 10(1): 315 - 318.

[16] FRIDRICH J, GOLIAN M, SOUKAL D et al. Forensic Steganalysis: Determining the Stego Key in Spatial Domain Steganography [A]. Proc. EI SPIE [C] San Jose, CA, 2005, 631 - 642.

[17] 张卫明, 刘九芬, 李世取. LSB 隐写术的密钥恢复方法 [J]. 中山大学学报(自然科学版). 2005, 44(3): 29 - 33.

[18] MA Ning, ZHANG Weiming, LIU Wenfen. Extracting Attack to LSB steganography of JPEG Images [A]. Proceedings of the 10th Joint International Computer Conference [C], Beijing: International Academic Publishers, World Publishing Corporation, 2004, 336 - 340.

[19] FRIDRICH J, GOLIAN M, DU R. Attacking the outguess [A]. Proceedings of the ACM Workshop on Multimedia and Security [C]. France, 2002. http://www.ws.binghamton.edu/fridrich/Research/acm_outguess.pdf.

(上接第 862 页)

表 2 低信息含量时提取出的特征对高信息含量的隐密图进行检测

Method	50%		100%	
	23 比特 征检测	F ₀ 进 行检测	23 比特 征检测	F ₀ 进 行检测
Jsteg	0.9991	0.9951	0.9992	0.0087
F5	0.9800	0.9800	0.9891	0.9862
OutGuess	0.9885	0.9781	0.9980	0.9921

4 结 论

本文对通用的隐密分析算法中的特征选择问题进行了研究,详细阐述了特征选择方法的基本原理,给出了详尽的实验结果,并对实验结果进行了分析.实验结果表明我们所使用的特征选择方法既能够在很大程度上削减特征维数,又能够保证很高的分类识别率.下一步的研究包括如何在特征选择的基础上,将不同的特征和不同分类器进行组合,进一步提高隐密分析系统的效率.

参考文献:

[1] Westfeld A, Pfitzmann A. Attacks on Steganographic Systems. Proc. 3rd Intl Workshop in Information Hiding. Springer Verlag, 1999, 61 - 76.

[2] Fridrich J, Goljan M. Reliable Detection of LSB Steganography in Grayscale and Color Images. Proc. ACM, Special Session on Multimedia Security and Watermarking. Ottawa CA, 2001, 27 - 30.

[3] Farid H, Siwei Lyu. Detecting Hidden Messages Using Higher - Order Statistics and Support Vector Machines. 5th Information Hiding Workshop, Noordwijkerhout, Netherlands, 2002, 340 - 354.

[4] Lyu S, Farid H. Steganalysis using higher - order image statistics. Information Forensics and Security, IEEE Transactions. March 2006, 111 - 119.

[5] Guorong Xuan, Yun Q. Shi, Jianjiong Gao et al. Steganalysis Based on Multiple Features Formed by Statistical Moments of Wavelet Characteristic Functions. Preproc. of 7th Int. Workshop on Information Hiding, 2005.

[6] Fridrich J. Feature - Based Steganalysis for JPEG Images and Its Implications for Future Design of Steganographic Schemes. International Workshop on Information Hiding (IH 2004), 2004, 67 - 81.

[7] Kira K, Rendell L. A Practical Approach to Feature Selection. Proc. 9th International Workshop on Machine Learning, 1992, 249 - 256.