基于 FCM 聚类的多超球体一类分类数字图像隐藏信息检测

戴 蒙[1] 林家骏[2] 刘云翔[1),2)]

[1)](上海应用技术学院计算机与信息工程系,上海 200235) [2)](华东理工大学信息科学与工程学院,上海 200237)

摘 要 从净图角度出发,提出了以 BMP、JPEG 净图特征为基础,采用 FCM 聚类的多超球体一类分类的隐藏信息检测技术。该技术针对同一类样本的特征存在着部分差异的特点,先将净图样本进行模糊 C 均值聚类,再将该样本的各子类样本特征输入一类 SVM 分类器进行训练,建立净图样本各子类的超球体分类模型,以此解决净图检测正确率低的问题。实验结果表明,该方法具有一定的通用性和泛化能力,减少了虚警率和漏检率。

关键词 隐藏信息检测 模糊 C 均值聚类 一类支撑向量机

中图法分类号:TN918.91 **文献标识码**:A **文章编号**:1006-8961(2008)10-1918-04

Steganalysis using OC-SVM with Multi Hyper-spheres Based on FCM

DAI Meng[1)], LIN Jia-jun[2)], LIU Yun-xiang[1),2)]

[1)] (*Computer Science & Information Engineering Department*, *Shanghai Institute of Technology*, *Shanghai* 200235)

[2)] (*School of Information Science & Engineering*, *East China University of Science and Technology*, *Shanghai* 200237)

Abstract The main focus in this paper is the detection techniques based on the cover images, which are detected using FCM OC-SVM. The feature set of cover samples are firstly clustered by the FCM algorithm. Then, the sub-class data are trained separately and the multi hyper spheres classification models are established. This technology can improve the detection of cover image and stego image and decrease false detection. Meanwhile the effect of many coefficients on the detecting accuracy is analyzed and generalized for broad application.

Keywords steganalysis, FCM, OC-SVM(one class-support vector machine)

1 引 言

现有检测技术是以净图与隐藏图像两类样本为研究对象,泛化能力不强。如同密码学中破译学滞后编码学,隐藏信息检测技术滞后于隐藏技术一样。本文从净图角度出发,提出了基于 BMP(bitmap)、JPEG 净图特征分析的隐藏信息检测技术。

目前,通用盲检测技术的训练样本均来自原始图像和含秘图像,对于每种隐写算法均需要设计相应的支持向量分类器[1,2],而隐写算法的数量数以千计,为每种隐写算法设计对应的分类器是不现实的。另一方面,如果有新的隐写算法出现,因为没有对这种隐写算法生成的隐藏信息图像进行训练,以前设计好的分类器将无用武之地。一类分类器(one-class classification)则可以有效地解决上述两个问题。一类分类器只需训练一类样本,这类样本可以从原始图像中提取,它生成的分类边界是一个闭合的超球体。在检测时,如有样本点在超球体的外面,则认为这些样本点来自于隐藏图像。但是,同一类样本的特征也存在着部分差异,如果只按照单超球体分类模型分类,则可能将一些非正常的样本错误地判别为正常样本。采用多超球体来覆盖训练样本,它具有更高的分类精度。

收稿日期:2008-06-20;**改回日期**:2008-07-31

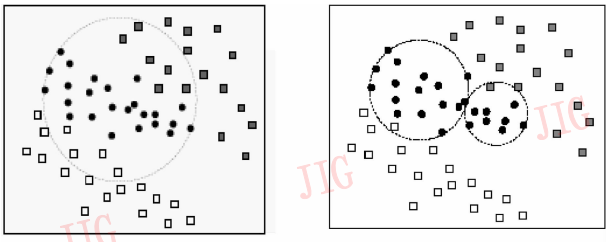
第一作者简介:戴 蒙(1979~),女,讲师。2007 年于华东理工大学获检测技术与自动化装置专业博士学位。主要研究领域为信息安全、图像隐写分析、数字图像处理等。E-mail:damon_1111@163.com

本文采用模糊 C 均值(fuzzy C-mean,FCM)聚类的方法将训练样本分成互不相交的子类,使分类器在保证净图检测正确率较高的同时降低隐藏图像的漏检率,具有更高的分类精度。净图特征描述见文献[3]。

2　模糊 C 均值聚类及多超球体一类分类器

用一类分类器对一类训练样本进行数据描述来判断新的对象是否与训练样本同类[4,5]。与传统分类器不同,一类分类器仅有一类样本可以利用,这类样本对象统称为目标对象,而所有其他对象统称为异常对象[6~8]。

同一类样本的特征也存在着部分差异,如果只按照单超球体分类模型分类,则可能将一些非正常的样本错误地判别为正常样本。如图 1(a)中,如果圆点表示的是净图样本,方块表示的是隐藏图像样本,单超球体将许多隐藏图片误判为净图,影响了整体样本的分类精度。因此,提出采用多超球体来覆盖训练样本。图 1(b)为具有两个超球体的一类分类器,与图 1(a)相比,它具有更高的分类精度。



(a)一类分类器　　(b)具有两个超球体的一类分类器

图 1　具有单超球体与两个超球体一类分类器比较图

Fig. 1　Differentiate of one-class classification with single hyper-sphere and 2 hyper-spheres

FCM 聚类[9~11],即众所周知的模糊迭代自组织数据分析算法(ISODATA),是用隶属度确定每个数据点属于某个聚类的程度的一种聚类算法。1973 年,Bezdek 提出了该算法,作为早期硬 C 均值聚类(hard C-mean, HCM),K 均值聚类方法的一种改进。

FCM 把 n 个向量 $\boldsymbol{x}_i(i = 1,2,\cdots,n)$ 分为 c 个模糊组,并求每组的聚类中心,使得非相似性指标的价值函数达到最小。FCM 与 HCM 的主要区别在于 FCM 用模糊划分,使得每个给定数据点用值在 0,1 间的隶属度来确定其属于各个组的程度。与引入模糊划分相适应,隶属矩阵 $\boldsymbol{U}$ 允许有取值在 0,1 间的元素。不过,加上归一化规定,一个数据集的隶属度的和总等于 1:

$$\sum_{i=1}^{c} u_{ij} = 1 \qquad \forall j = 1,\cdots,n \tag{1}$$

FCM 的价值函数(或目标函数)为

$$J(\boldsymbol{U},\boldsymbol{c}_1,\cdots,\boldsymbol{c}_c) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c}\sum_{j}^{n} u_{ij}^m d_{ij}^2 \tag{2}$$

式中,u_{ij} 介于 0,1 间;$\boldsymbol{c}_i$ 为模糊组 i 的聚类中心,$d_{ij} = \|\boldsymbol{c}_i - \boldsymbol{x}_j\|$ 为第 i 个聚类中心与第 j 个数据点间的欧几里德距离;且 $m \in [1,\infty)$ 是一个加权指数。

构造如下新的目标函数,可求得使式(2)达到最小值的必要条件:

$$\bar{J}(\boldsymbol{U},\boldsymbol{c}_1,\cdots,\boldsymbol{c}_c,\lambda_1,\cdots,\lambda_n) = J(\boldsymbol{U},\boldsymbol{c}_1,\cdots,\boldsymbol{c}_c) + \sum_{j=1}^{n}\lambda_j\left(\sum_{i=1}^{c} u_{ij} - 1\right) = \sum_{i=1}^{c}\sum_{j}^{n} u_{ij}^m d_{ij}^2 + \sum_{j=1}^{n}\lambda_j\left(\sum_{i=1}^{c} u_{ij} - 1\right) \tag{3}$$

式中,$\lambda_j, j = 1,\cdots,n$,是式(1)的 n 个约束式的拉格朗日乘子。对所有输入参量求导,使式(2)达到最小值的必要条件为

$$\boldsymbol{c}_i = \frac{\sum_{j=1}^{n} u_{ij}^m \boldsymbol{x}_j}{\sum_{j=1}^{n} u_{ij}^m} \tag{4}$$

和

$$u_{ij} = \frac{1}{\sum_{k=1}^{c}\left(\frac{d_{ij}}{d_{kj}}\right)^{2/(m-1)}} \tag{5}$$

由上述两个必要条件,模糊 C 均值聚类算法是一个简单的迭代过程。

3　基于模糊 C 均值聚类的多超球体一类分类隐藏图像检测流程

采用多超球体来覆盖训练样本,即先对净图样本的特征向量集采用模糊 C 均值聚类方法进行聚类,然后将聚类的结果输入到一类 SVM 分类器进行训练,得到多超球体模型,以此来提高净图样本的检测正确率和隐藏图像的检出率,减少虚警率和漏检率。

基于模糊 C 均值的多超球体一类分类隐藏图像的检测方法的第 1 步与其他通用检测方法是相同的,即

第 1 步　对训练的干净样本图像集进行特征提取,以特征集抽象地描述每幅未隐藏信息的图像;

第 2 步　将净图训练特征集进行模糊 C 均值聚类;

第 3 步　将经过模糊 C 均值聚类处理的净图特征集分别作为 SVM 一类分类器的训练集,按照 SVM 训练算法的步骤搜寻支撑向量,得到多超球体。

第 4 步　提取测试样本图像的特征集。

最后,利用训练好的 SVM 分类器 Model 对测试样本集进行分类,从而区分隐藏图像与净图。图 2 是基于多超球体一类分类器的隐藏图像检测流程。

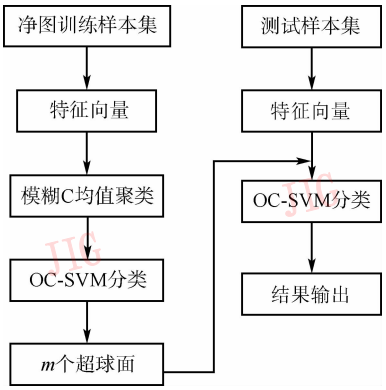


图 2　多超球体一类分类隐藏图像检测流程

Fig. 2　Detect procedure of OC-SVM with multi hyper-spheres

4　参数分析及实验

4.1　样本及特征属性说明

实验中,SVM 分类器的算法采用目前较为流行的 LibSVM[12],由台湾大学的林智仁教授开发。

实验中所用到的特征为文献[3]第 4 章所述的 BMP、JPEG 图像的统计特征,样本集中共 2 576 幅净图,其中 1 850 幅是 JPEG 格式,826 幅 BMP 格式;各类隐写算法的隐藏图像共 3 073 幅,其中 1 950 幅是 JPEG 格式,1 023 幅是 BMP 格式。实验时,不同来源的净图特征集只按 BMP、JPEG 的格式不同分开存放,其样本标识标定为 1;不同来源及不同隐写算法的隐藏图像的样本特征集只按 BMP、JPEG 的格式不同分开存放,其样本标识标定为 -1。训练集样本数目与测试集样本数目的比例为 3:2。净图样本和隐藏图像样本的详细信息见表 1 ~ 表 3 所示(表 2、3 中 ECUST: East China University of Science and Technology; MSS: ministry of state security)。

表 1　净图测试样本说明

Tab. 1　Details about the test cover images

样本数目	样本大小(像素)	样本来源	样本格式
500	256 × 256	Philips dataset	JPEG
500	640 × 480	Canon PS A75	JPEG
500	480 × 320	Corel Draw dataset	JPEG
350	83 × 90 ~ 1024 × 768	MSS	JPEG
200	256 × 256	汉王 6800 扫描仪	BMP
126	512 × 512	MSS	BMP
500	256 × 256	ECUST	BMP

表 2　JPEG 隐藏图像测试样本说明

Tab. 2　Details about the JPEG format test stego images

样本数目	样本大小(像素)	隐写软件或隐写算法	嵌入容量(%)	来源
450	640 × 480	Jstegshell2. 0	7	ECUST
50	640 × 480	JStegshell2. 0	0. 1	MSS
500	480 × 320	Outguess0. 13	5	ECUST
200	1024 × 768, 800 × 600	JPhwin	8	MSS
200	1024 × 768	Outguess0. 2	2	MSS
50	800 × 600, 720 × 501 …	F5	0. 1	MSS
500	480 × 320	F5	< 10	ECUST

表 3　BMP 隐藏图像测试样本说明

Tab. 3　Details about the BMP format test stego images

样本数目	样本大小	隐写软件或算法	嵌入容量(%)	来源
50	300 × 300 左右	S-tools	5	MSS
6	640 × 480	Eshow	5	MSS
47	480 × 320	Webstego	5	MSS
50	300 × 300 左右	Hide4pgp	5	MSS
200	256 × 256	Hide4pgp	5	ECUST
50	500 × 500 左右	steganos	5	MSS
500	480 × 320	S-tools	< 15	ECUST
120	480 × 320	Hide4pgp	< 10	ECUST

4.2　参数分析及实验结果

为了防止“过学习”,测试样本中正类(净图)样本数和负类(隐藏图像)样本数的比例为 10:1,测试样本的标定均为正类样本的标定。构造 SVM 分类器时,选择不同的核函数以及不同的参数会造成不同的训练结果和分类结果,将采用 RBF(radial basis function)核作为核函数,其核函数为

$$K(\boldsymbol{x}_i,\boldsymbol{x}_j) = \exp(-\gamma\|\boldsymbol{x}_i - \boldsymbol{x}_j\|^2) \qquad \gamma > 0 \quad (6)$$

下面将讨论使用 LibSVM 时,参数 μ 和参数 γ 对分类效果的影响。

4.2.1　μ 对分类精度的影响

为了测试参数 μ 对分类精度的影响,选定固定 γ 值($\gamma = 0.1$),分类精度随 μ 值的增大分别在 [0,0.1],[0.1,1) 出现了两个峰值,如图 3 所示。

4.2.2　γ 对分类精度的影响

为了讨论 γ 值对分类效果的影响,可固定 μ 值,选取不同的 γ 值来训练 RBF 核 SVM,正确分类率随 γ 的变化关系如图 4 所示。从实验结果可以看出,随 γ 值增大其对分类精度的影响不大。

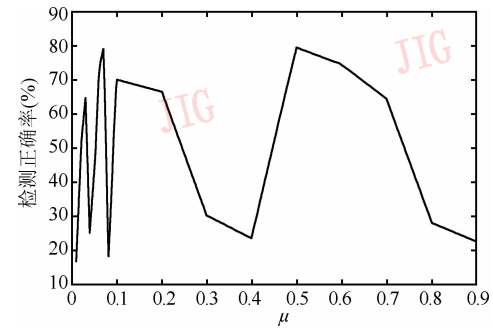


图 3　μ 对检测正确率影响

Fig. 3　Training result of different μ

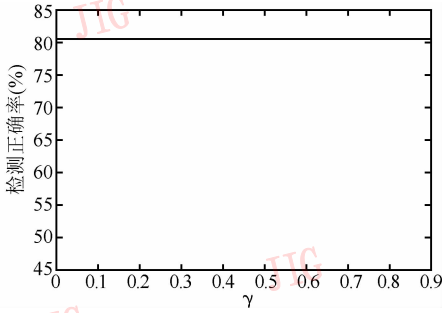


图 4　检测正确分类率与 γ 的变化关系

Fig. 4　Rate of right classifying plotted as a function of γ

4.2.3 超球体个数对分类精度的影响

通过对图 1(a)与图 1(b)比较后可以看出,具有 2 个超球体的一类分类器其隐藏图像的检测正确率要高于具有 1 个超球体的分类器。表 4 为比较分别具有 1、2、3、4 个超球体分类器的分类精度。

表 4　不同超球体个数对检测正确率的影响(JPEG)

Tab. 4　Testing result of different number of hyper-spheres(JPEG)

单位:%

图像	超球体个数			
	1	2	3	4
净图	91.1	90.6	89.3	87
隐藏图像	80.6	85.3	86	86.7

从表中数据可以看出,随着超球体数目的增加,净图样本检测正确率有所下降,且下降速度有所增加,隐藏图像检测正确率得到提高,但是当超球体增加到 4 个时,隐藏图像检测正确率的提高作用不大。

表 5 列出了不同超球体对 BMP 格式净图和隐藏图像的检测正确率的影响。表中 1,2,3,4 表示超球体个数。

表 5　不同超球体个数对检测正确率的影响(BMP)

Tab. 5　Testing result of different numbers of hyper-spheres(BMP)

单位:%

图像	超球体个数			
	1	2	3	4
净图	85.1	85	84.3	83
隐藏图像	70.4	78.7	86	86.3

5　结　论

本文主要研究的是基于模糊 C 均值聚类的多超球体一类分类的隐藏信息检测。针对同一类样本的特征存在着部分差异的特点,提出了先将同一类样本进行模糊 C 均值聚类,再将该样本的各子类样本特征给一类 SVM 分类器进行训练,建立净图样本各子类的超球体分类模型。实验数据表明:

(1)基于模糊 C 均值聚类的多超球体的分类器其分类精度高于单个球体建立的分类模型分类精度;

(2)子类超球体个数增大到一定程度(以本论文样本为例,子类超球体个数为 4 时,净图检测的漏检率不断增大,但是隐藏图像的检测正确率则没有明显提高,因此在设计分类器时,应平衡分类器超球体数目和分类器分类正确率的关系,以免子类超球体过多带来工程上不必要的时间及机器花费。

参考文献(References)

1　Farid H, Siwei L. Detecting hidden messages using higher-order statistics and support vector machines[A]. In: Proceedings of 5th International Workshop on Information hiding[C], New York, NY, USA: Springer Verlag, 2002: 340 ~ 354.

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

3　Dai Meng. Hidden Information detection Research based on the cover image features[D], Shanghai: East China University of Science and Technology, 2007:29 ~ 63. [戴蒙. 基于净图特征的分析的隐藏信息检测技术研究[D],上海:华东理工大学, 2007: 29 ~ 63.]

4　Vapnik V. Estimation of Dependences based on Empirical Data[M]. New York, NY, USA: Springer-Verlag, 1982.

5　Osuna E, Freund R, Girosi F. An improved training algorithm for support vector machines[A]. In: Proceedings of IEEE Workshop on Neural Networks and Signal Processing[C], New York NY, USA: IEEE Press, 1997:276 ~ 285.

6　Tax D M J, Duin R P W. Data domain description using support vectors [A]. In: Proceedings of the European Symposium on Artificial Neural Networks[C], Brugge, West Flanders, Belgium, 1999:251 ~ 256.

7　Tax D M J, Duin R P W. Support vector domain description[J]. Pattern Recognition Letters, 1999, **20**(11-13):1191 ~ 1199.

8　Tax D M J. One-class classification [D], Delft, SouthHolland, Netherlands: Delft University of Technology, 2001.

9　Sugeno M. Yasukawa T. A fuzzy logic based approach to qualitative modeling[J]. IEEE Transaction on Fuzzy Systems, 1993, **1**(1): 7 ~ 31.

10　Jain A K, Murt Y M N, Flynn P J. Data clustering: A review[J]. ACM Computer Survey, 1999, **31**(3): 264 ~ 323.

11　KE J. Fast Accurate Fuzzy Clustering through Reduced Precision[D]. Tampa, South Florida, USA: University of South Florida, 1999.

12　Chang C C, Lin C J. LIBSVM: a library for support vector machines [EB/OL]. http://www.csie.ntu.edu.tw/~cjlin/libsvm.2004.