多矢量曲线水印检测的 SVM 分类融合方法

陈 欢 孙广玲
(上海大学通信与信息工程学院,上海 200027)

摘 要 针对矢量图形的版权保护问题,提出了一种基于 SVM 分类融合的多矢量曲线水印检测方法。该方法在水印嵌入阶段,对多条曲线嵌入由嵌入密钥生成的水印;在检测阶段,对多条曲线检测由检测密钥生成的水印,同时多条曲线的检测相关值按一定的顺序构成一个特征向量;然后由 SVM 两类别分类器对该特征向量进行决策,以判定这多条曲线是否嵌入了由检测密钥生成的水印。SVM 分类器的学习样本是模仿各种多矢量曲线变换和攻击下,相应产生了由多曲线检测相关值构成的特征向量。该方法本质上是基于 SVM 分类的多个检测相关值的融合方法。理论分析和仿真结果证明,该方法是可行的和有效的。

关键词 矢量曲线 密钥 水印 SVM 融合
中图法分类号:TP309 **文献标识码**:A **文章编号**:1006-8961(2008)10-1963-04

Watermark Detection of Vector Curves Using SVM Classification Fusion Method

CHEN Huan, SUN Guang-ling
(*Shanghai University*, *School of Communication and Information Engineering*, *Shanghai* 200072)

Abstract In order to protect the copyright of the vector graphics, in this paper we introduce a fusion rule for watermark detection of vector curves using SVM classification. At the embedding stage, the watermarks are embedded into multi vector curves with the same key. At the detecting stage, firstly, the watermarks are detected using the embedded key then a eigenvector is obtained which is created by detection correlative values in a certain order. Finally the SVM classification can determine whether those curves have the watermarks that embedded with a right key. The study samples of SVM classification are imitating all kinds of eigenvector, which are detected from the attacked and transformed curves. Essentially it is a fusion rule of multi related values, which based on the SVM classification. Theoretical analysis and simulation results prove it is feasible and effective.

Keywords vector curve, key, watermark, SVM, fusion

1 引 言

在多媒体技术和网络技术迅速发展的今天,矢量图形因其特有的性质被广泛应用。矢量图形主要由矢量定义的直线和曲线组成,用于对轮廓的几何特性进行描述,其具有数据量小、精度高的特点。此外,矢量图形与分辨率无关,任意地移动、缩放、旋转等都不会影响其清晰度。常见的矢量图形有地理信息系统(geographical information systems,GIS)、可扩展矢量图形(scalable vector graphics,SVG)、计算机辅助设计(computer aided design,CAD)等。随着计算机网络的普及和应用,矢量图形的存储、复制、下载与传播变得非常简单和方便,这也使得矢量图形被篡改盗用日益突出,因而对矢量图形数据的产权进行保护就显得尤为重要。

数字水印是一种有效的数字产品版权保护和数字安全维护技术,在图像、音频和视频等方面已得到迅速发展,其在 2 维矢量图形方面,也有了初步发展。根据水印嵌入的位置,矢量图形水印可分为空间域和变换域方法。空间域方法即通过直接修改多边形的顶点值来嵌入水印,Ohbuchi 等人提出了一种基于四叉树划分的矢量地图空域水印算法[1]。Zhou 等人依据周长不变的原则将多边形参数化成圆,在圆心角中

收稿日期:2008-06-15;**改回日期**:2008-07-22
第一作者简介:陈 欢(1982~),女。现为上海大学在读硕士研究生。主要从事矢量图形数学水印方面的研究。E-mail:chenhuan@shu.edu.cn

嵌入水印,取得了较好的效果[2]。此外, Schulz 等人提出先将矢量图形划分成指定大小的块,然后通过修改块中顶点的分布来嵌入水印[3]。在变换域方面, Solachidis 等人针对多边形数据,提出将水印嵌入到某一条闭合多边形顶点序列的 1 维离散傅里叶描述子的幅度中[4]。傅里叶描述子的性质,使得该方法对多种几何攻击具有很好的鲁棒性。另外,王炎等人找到一种新的描述方式,即对多边形进行 ICA 分解,先得到仿射不变描述子,然后在描述子中嵌入水印[5],该方法对仿射变换具有很强的鲁棒性。

但上述算法大多是在单一的曲线中嵌入和检测水印。按照“数据融合”理论,根据多个传感器或多源信息进行综合判决,则能够获得较单一传感器更为准确、可靠的决策[6];同样,先在多条曲线中嵌入和检测水印,再融合各曲线水印的检测结果,应能获得比单一曲线更好的检测性能,而且实际的矢量图形大都存在多条曲线,这说明利用多曲线的思路是完全可行的。特别对于一些检测性能要求曲线顶点数目足够多才能得到保证的方法(比如文献[4]方法,若多边形的顶点数目过少,则将导致误判率增加),在顶点数目的确有限的情况下,就可通过多曲线检测融合的策略来弥补检测性能的下降。事实上,已存在一些多曲线检测融合策略的文献。如 Nikolaidi 等人先将水印嵌入到多边形曲线集,然后利用多种融合技术进行检测,并用实验对常见的融合方法进行了比较[7]。Victor 等人也提出在多条曲线中嵌入水印和使用融合技术来提升判决准确率[8]。但这两篇文献中的似然比方法都是针对具体水印的嵌入和检测算法,不具备广泛的适用性,而且他们都假设各曲线的检测值是独立的,而笔者认为曲线的检测值之间是存在相关性的。为此,本文提出了基于 SVM 分类[9]的多曲线水印检测融合方法。其优势在于,一方面其适用于任何水印嵌入和检测方法,这就具有了广泛的适用性;另一方面,由于没有检测值独立的假设,因此对实际情况的要求更加宽松。

2 数据融合规则

“数据融合”在本文研究的问题中可定义为:找到一个合适的运算法则 f,对 N 个 $\hat{c}_i$ 进行运算输出一个最佳的

$$r = f(\hat{c}_0, \cdots, \hat{c}_{N-1})$$

N 为嵌入水印的曲线数目, $\hat{c}_i$ 为单条曲线的水印检测相关值, r 为融合后的相关值。判断矢量图形是否含有水印,可选择一个合适的门限 T,若 $r > T$,则判断矢量图形含有水印,否则不含水印。

文献[7]列举了若干融合规则,其中的“加权的 $\hat{c}_i$ 均值”被验证为是最佳的融合规则:

$$r = \frac{\sum_{i=0}^{N-1} w_i \hat{c}_i}{\sum_{i=0}^{N-1} w_i}$$

文中分别对 $w_i = M_i$ 和 $w_i = M_i^2$ 两种情况进行了实验, M_i 表示第 i 条曲线的节点数目。

3 基于 SVM 分类的融合方法

支持向量机(support vector machine, SVM)是源于统计学习理论[9](statistical learning theory)的一种机器学习方法,它是以结构风险最小化为目的,其优于神经网络学习的方法。该方法在解决小样本、非线性及高维模式识别的问题中具有明显优势,在模式识别、函数逼近和概率密度估计等领域已取得良好的效果,其原理详见文献[9]。

3.1 可行性

将 SVM 分类方法用于多曲线水印检测之所以是可行的,是基于以下几点:

(1)水印检测问题可看成是两类别分类问题,而 SVM 分类器最初就是用来解决两类别分类问题的,而且在两类别问题上具有最优的性能和最完美的形式。

(2)若嵌入密钥和检测密钥相同,则因每条矢量曲线的形状具有自身特点,从而使其在原始形式(即没有任何攻击或变换)和各种攻击或变换之下的水印检测值 $c_i^{\text{in}}(i = 1,2,\cdots,M_{\text{in}})$, i 是曲线各种可能的形式之一, M_{in} 是不同形式曲线的数量,以下同)服从于一定的 1 维统计分布,这很类似于 1 维特征的类内样本;而在多条曲线的情况下,由多条曲线的检测值构成的检测向量 $\boldsymbol{c}_i^{\text{in}}(i = 1,2,\cdots,M_{\text{in}})$ 自然就服从于一定的高维联合统计分布,且各曲线的检测值 $\hat{c}_j(j = 0,1,\cdots,N-1; N$ 是曲线个数)之间是存在相关性的,这就类似于具有高维特征的类内样本;显然,可将 $\boldsymbol{c}_i^{\text{in}}(i = 1,2,\cdots,M_{\text{in}})$ 看成是类内样本集合, M_{in} 是类内样本个数。注意,对于多条曲线,只有每条曲线的嵌入密钥和检测密钥都相同,才满足“嵌入密钥和检测密钥相同”的条件。

(3)若嵌入密钥和检测密钥不相同或没有嵌入水印,则曲线在原始形式和各种攻击或变换之后产

生的多个检测向量 $\boldsymbol{c}_i^{\text{out}}(i=1,2,\cdots,M_{\text{out}})$,$M_{\text{out}}$ 是曲线不同变化的数量,以下同)将不服从同一形式的统计分布,而是服从多种不同的统计分布,并且这些分布与嵌入密钥和检测密钥相同情况下的检测向量的空间分布具有一定程度的差异,即具有线性或非线性的可分性。因此,可将 $\boldsymbol{c}_i^{\text{out}}(i=1,2,\cdots,M_{\text{out}})$ 看成是非类内样本集合,M_{out} 是非类内样本个数。注意,对于多条曲线,只要有一条曲线的嵌入密钥和检测密钥不相同或没有嵌入水印就满足"嵌入密钥和检测密钥不相同或没有嵌入水印"的条件。

综上所述,将多曲线水印的检测问题纳入到 SVM 两类分类器的框架之下是完全可行的。事实上,上述分析已经给出了在当前问题下的类内学习样本集合和非类内学习样本集合的构建方法,具体实现参见实验部分。

3.2　融合规则

假设已经利用类内和非类内的学习样本得到一个 SVM 分类器,则融合规则如下:

按下式计算融合后的水印检测相关值:

$$r=\left[\sum_{\text{支持向量}} y_i\alpha_i K(\boldsymbol{c}_i,\hat{\boldsymbol{c}})-b\right],\hat{\boldsymbol{c}}=[\hat{c}_0,\hat{c}_1,\cdots,\hat{c}_{N-1}]^{\mathrm{T}}$$

为了与第 2 部分的符号表示一致,本文用 $(\hat{c}_0,\hat{c}_1,\cdots,\hat{c}_{N-1})$ 表示各条曲线的相关值,它们构成了检测向量 $\hat{\boldsymbol{c}}$;实验中取多项式核函数 $K(x,y)=[(x\cdot y)+1]^d$。其他符号的含义参见上文所述和文献[9];r 从 SVM 分类器的角度来看,是向量 $\hat{\boldsymbol{c}}$ 到最优超平面的距离,而在当前问题中,即表示融合后的相关值。

如果 $r>T$,则判断矢量图形含有水印,否则不含水印。

基于上述分析不难看出,无论在学习环节和检测环节,人们只关心相关值本身,而并不关注怎样获得相关值,也就是说本文提出的融合方法是适用于任何水印嵌入和检测方法的,只要该方法能够提供相关值即可;另外,由于 SVM 分类方法并不假设各相关值之间是独立的,因此能够获得更好的效果,这也会在实验部分得到证实。

4　实验及分析

不失一般性,本文采用文献[4]的方法进行单一曲线水印的嵌入和检测;另外,SVG 作为 W3C 的开源已成为全球图形技术的潮流,它将引领人们走向下一代互联网,同样它也不可避免地面临着数据安全和版权保护问题,因而本文以 SVG 作为实验的平台。

4.1　实验步骤

本文选择 tiger. svg 进行实验,即按照文献[4]方法对 N 条曲线进行嵌入和检测。具体步骤如下:

(1) 生成训练样本并训练

类内样本:指嵌入和检测使用相同密钥的样本。$\hat{M}_{\text{in}}$ 个类内样本 $\hat{\boldsymbol{c}}_i^{\text{in}}(i=1,2,\cdots,\hat{M}_{\text{in}})$ 是 N 条曲线在不进行变换和进行各种变换(尺度变换、加高斯噪声和中值滤波等)下得到的检测向量。N 条曲线变换不仅包括同步情况下的变换参数不同的变换,同时还包括非同步下的变换参数不同的变换。为了训练的充分性,可将密钥也作为一个变换参数。

非类内样本:指检测密钥与嵌入密钥不相同和没有嵌入水印。非类内样本 $\hat{\boldsymbol{c}}_i^{\text{out}}(i=1,2,\cdots,\hat{M}_{\text{out}})$ 和类内样本 $\hat{\boldsymbol{c}}_i^{\text{in}}(i=1,2,\cdots,\hat{M}_{\text{in}})$ 的区别是,在检测时使用了和嵌入密钥不相同的随机密钥,其他生成条件相同。

将得到的训练样本 $\hat{\boldsymbol{c}}=[\hat{\boldsymbol{c}}^{\text{in}}_{(1\cdots\tilde{M}_{\text{in}})};\hat{\boldsymbol{c}}^{\text{out}}_{(1\cdots\tilde{M}_{\text{out}})}]$ 用 SVM 训练来得到融合后的水印检测相关阈值 T。

(2) 生成测试样本并进行测试

测试样本:同样包括类内和非类内样本。与步骤(1)中训练样本的生成相同,但是变换参数必须不相同。

将得到的测试样本 $\tilde{\boldsymbol{c}}=[\tilde{\boldsymbol{c}}^{\text{in}}_{(1\cdots\tilde{M}_{\text{in}})};\tilde{\boldsymbol{c}}^{\text{out}}_{(1\cdots\tilde{M}_{\text{out}})}]$ 送入步骤(1)得到的 SVM 分类器进行测试,即得到融合后的 $r_i(i=1,2,\cdots,\tilde{M}_{\text{in}}+\tilde{M}_{\text{out}})$。

(3) 绘制 ROC 曲线

算法的优劣可用 ROC(receiver operating characteristic)曲线(虚警率和漏报率)来衡量。通过改变阈值 T 对步骤(3)得到的测试样本 $r_i(i=1,2,\cdots,\tilde{M}_{\text{in}}+\tilde{M}_{\text{out}})$ 进行分类,即可获得不同的虚警和漏报率,再据其画出 ROC 曲线。

另外一种衡量算法优劣的方法是求其 EER(equal error rate)值,即 ROC 曲线上虚警率和漏报率相等的点。

因为文献[4]方法在平移和旋转变换下,检测值不变,所以实验只绘制了常见的尺度变换、加噪和滤波情况下的 ROC 曲线和 EER 值。为了说明该融合规则优于其他常见融合规则,在测试样本相同的条件下对"加权的 $\hat{c}_i$ 均值"规则也进行了仿真,并绘制了其 ROC 曲线和 EER 值。

4.2　结果和分析

实验中,参数的取值与实验结果参见表 1、表 2 和图 1、图 2。

表 1 实验参数值

Tab. 1 Values for experiment

N	$M_{in}(M_{out})$	$\hat{c}$	$\tilde{c}$	r	d
7	596	1 192 × 7	1 094 × 7	1 094 × 1	3

表 2 两种融合规则下的 EER

Tab. 2 EERs for various attacks and two fusion rules

攻击方式	不同融合规则下的 EER 值	
	$w_i = M_i^2$	SVM
尺度变换	7.6×10^{-3}	6.8×10^{-3}
中值滤波	1.2×10^{-1}	3.0×10^{-2}
高斯噪声	9.2×10^{-2}	3.5×10^{-2}

嵌入水印的 7 条曲线的长度分别为:364、499、256、487、637、274 和 1 051。

图 1 中,实线和虚线分别为嵌入水印前后的图形。从图中可见,矢量图形的失真很轻微,对视觉不会造成影响。

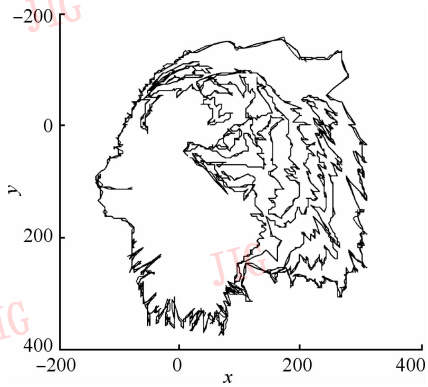

图 1 嵌入水印前后的曲线集

Fig. 1 Original and watermarked vector curves

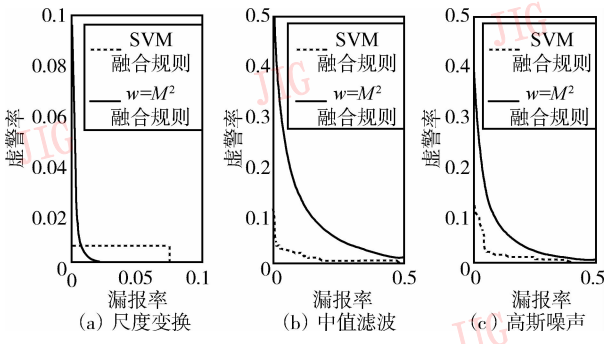

图 2 两种融合规则融合结果的比较

Fig. 2 ROC curves for two fusion rules

图 2 为“加权的 $\hat{c}_i$ 均值”规则且 $w_i = M_i^2$ 和 SVM 分类融合规则下的 ROC 曲线。图 2(a) ~ 图 2(c)分别是进行尺度变换、中值滤波和高斯加噪后两种融合规则下的漏报率、虚警率比较。从 ROC 曲线分析可见,后两种情况的 SVM 分类融合规则的结果均优于“加权的 $\hat{c}_i$ 均值”规则。对于尺度变换的情况还可以从 EER 值来分析(见表 2)。显然,SVM 融合规则下的 EER 均优于“加权的 $\hat{c}_i$ 均值”规则的 EER。

5 结 论

本文针对矢量图形的版权保护问题,提出了一种在多条矢量曲线中嵌入水印的方法,检测时,先将得到的各水印的相关值按一定顺序构成一个检测向量,然后运用 SVM 分类作为融合规则进行最终决策的方法来进行检测。理论分析和实验仿真结果均证明该方法是可行的,且具有高于常见融合算法的准确率。但由于 SVM 本身是一种机器学习方法,致使水印的检测是一种半盲检测。另外,ROC 曲线只是用来衡量算法整体的优劣,而阈值的选取则对最终的判决具有一定影响,所以如何选择最优的检测阈值也是值得进一步研究的问题。

参考文献(References)

1 Ohbuch I, Ueda H, Endoh S. Robust watermarking of vector digitalmaps[A]. In: Proceedings of IEEE Conference on Multimedia and Expo[C], Lausanne, Switzerland, 2002, **1**:577 ~ 580.

2 Zhou X, Pan X. Watermark-based scheme to protect copyright of SVG data [A]. In: Proceedings of International Conference on Computational Intelligence and Security [C], Guangzhou, China, 2006:1199 ~ 1202.

3 Schulz G, Voigt M. A high capacity watermarking system for digital maps[A]. In: Proceedings of the 2004 Multimedia and Security Workshop on Multimedia and Security[C], Magdeburg, Germany, 2004:180 ~ 186.

4 Solachidis V, Pitas I. Watermarking polygonal lines using Fourier descriptors [J]. IEEE Computer Graphics and Applications, 2004, **24**(3): 44 ~ 51.

5 Wang Y, Wang J J, Huang X M. An ICA-based polygonal curves watermarking algorithm [J]. Computer-Aided Design & Computer Graphics, 2006, **18**(7):1054 ~ 1059. [王炎,王建军,黄旭明. 一种基于 ICA 的多边形曲线水印算法[J]. 计算机辅助设计与图形学学报, 2006, **18**(7):1054 ~ 1059.]

6 Chair Z, Varshney P K. Optimal data fusion in multiple sensor detection systems [J]. IEEE Transactions on Aerospace and Electronic Systems, 1986, **22**(1), 98 ~ 101.

7 Nikolaidis N, Pitas I, Giannoula A. Watermarking of sets of polygonal lines using fusion techniques[A]. In: Proceedings of IEEE International Conference on Multimedia and Expo [C], Lausanne, Switzerland 2002, **2**:26 ~ 29.

8 Victor R, Nikolaidis N, Pitas I. An optimal detector structure for the Fourier descriptors domain watermarking of 2D vector graphics [J]. IEEE Transactions on visualization and computer graphics, 2007, **13**(5):851 ~ 863.

9 Vapnik V. The Nature of Statistical Learning Theory [M]. New York, USA: Springer, 2000.