第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·安全技术· 文章编号：1000—3428(2007)12—0148—03 文献标识码：A 中图分类号：TP309

基于图像的信息隐秘检测系统的设计

刘 佳[1]，杨晓元[1,2]，王育民[2]，唐玉华[1]
(1. 武警工程学院电子技术系网络与信息安全武警部队重点实验室，西安 710086；2. 西安电子科技大学ISN国家重点实验室，西安 710071)

摘 要：设计并初步实现了一个基于图像的隐秘检测系统，其目的是在没有原图像载体的条件下，提高发现网络中的隐秘图像的准确率。系统采用对彩色图像每个颜色通道分别进行小波分解，根据小波分解系数绝对值和绝对值线性预测的对数误差生成特征向量，并采用非线性的支持向量机进行模式分类。讨论了该系统的结构、工作原理、控制流程及设计中的关键技术，并对系统性能进行了测试评估，指出了可进一步改进完善的方向。

关键词：信息隐藏；盲检测；支持向量机；模式识别

Design of Blind Detecting System for Image Steganalysis

LIU Jia[1], YANG Xiaoyuan[1,2], WANG Yumin[2], TANG Yuhua[1]
(1. Network and Information Security Key Laboratory, Electronics Department of Engineering College of the APF, Xi'an 710086;
2. National Key Laboratory on ISN, Xidian University, Xi'an 710071)

【Abstract】 This paper designs and implements a blind detecting system for images steganalysis. The aim of devising the blind detecting systems is to discover images in networks with more veracity at condition of no original images. The wavelet decomposition is implemented in each color channel, the magnitude of decomposition coefficients and the log error between the actual coefficient and the predicted coefficient magnitudes are used to yield statistics. The non-linear support vector machine algorithm has been employed in the pattern discrimination. Its structure, principle, controlling process as well as the key designing technique of software are also presented in detail. It points out improvement direction.

【Key words】 Information hiding; Blind detecting; Support vector machines; Pattern recognition

1 概述

信息隐藏分析技术可以分为攻击技术、破解技术和检测技术3种。破解技术难度很大，至今还没有深入的研究成果。基于图像的信息隐藏分析的研究主要集中在检测和攻击技术上。攻击技术相对简单，便于实现。对图像文件的裁剪、旋转、效果改变、格式转换都可视作一种攻击。检测技术作为信息隐藏分析的第一步，显得尤为重要。

隐藏检测技术可分为2大类：对比检测技术和盲检测技术。在对比检测技术中，检测过程需要隐秘载体和原始载体对比，这种方法相对简单。通常从原始载体和隐秘载体的像素之间的关联分析、变换域系数的关联分析中，发现隐藏信息的可能性。盲检测技术是指在没有原始载体相对比的情况下，仅通过隐秘载体检测隐藏信息，检测难度较大。根据检测的特征，基于图像的信息隐藏检测方法包括基于签名的检测[1]和基于统计的检测[2]。前一种方法针对已知的隐藏算法和工具，分析信息嵌入的模式，从而判定是否存在该算法或工具实现的信息隐藏。该方法的优点是检测准确性高，可以分辨出具体的嵌入算法和工具，缺点是无法检测未知的隐藏算法和工具；基于统计的检测，则根据图像在嵌入信息前后统计特征的不同判定是否存在信息隐藏。该算法的优点在于寻求一类图像或算法的检测方法，具有较通用的检测能力，但缺点是检测难度高，检测准确性受外界因素影响大，无法分辨是哪一种隐藏工具和算法。

基于图像的信息隐藏检测技术是近几年信息安全领域研究的重要方面，国外起步较早，在军事、国防领域，基于图像的信息隐藏检测系统已经部分投入了使用[3]。国内还没有具有自主知识产权的图像隐秘检测产品发布。本文结合了基于签名和基于统计的检测方法，利用多分辨率分析的图像特征形成算法和支持向量机的分类算法，研究设计了一个隐秘图像盲检测系统。实验表明，它能有效地检测出当前流行的几种隐秘软件生成的隐秘图像。

2 系统结构与工作原理

隐秘图像检测系统的总体结构如图1所示。该系统包括：

(1)图像收集器，负责从网络中收集数字图像文件，自动分辨图像的格式、特性，将图像按格式分类。

(2)特征形成和提取模块，负责生成图像的特征，是检测系统的核心模块。系统采用了小波包分解系数及其预测误差的统计模型生成特征。

(3)训练模块，从特征形成模块接收正常图像特征，进行支持向量机训练，将结果输出到统计检测模块。训练模块还对已知隐藏工具和算法的隐秘图像进行训练，训练结果作为签名模块的检测标准。

(4)预检测模块，对收集的图像进行过滤，提高系统的处理速度。预检测模块具有较高的灵敏度，大量的正常数字图像被它过滤，稍有异常的图像就进入正式检测模块。

(5)基于统计检测模块，可以集成多种统计算法，通过多种统计算法的检测结果的融合；得到信息隐藏的可能性。将

基金项目：国家自然科学基金资助项目(60473029)；信息安全教育部重实验室课题资助项目(200409)；武警部队军事科研项目
作者简介：刘 佳(1982－)，男，硕士，主研方向：网络与信息安全，秘分析；杨晓元，教授；王育民，教授，博导；唐玉华，硕士
收稿日期：2006-09-08 **E-mail：**twinlj77@gmail.com

一组基于支持向量机的分类器置于该模块中，该模块将输入的可疑图像区分为正常图像和隐秘图像。

(6)基于签名检测模块，针对具有相似特征的隐藏算法和工具，可以识别具体的隐藏工具或算法。该模块作为可选模块，每个检测方案由训练模块对已知隐藏算法或工具的隐秘图像进行训练得到。

(7)综合分析模块，把基于统计检测模块的结果和基于签名检测模块的结果，利用专家知识进行综合分析，确定该图像文件嵌入隐藏信息的可能性和可能使用的隐藏算法或工具。

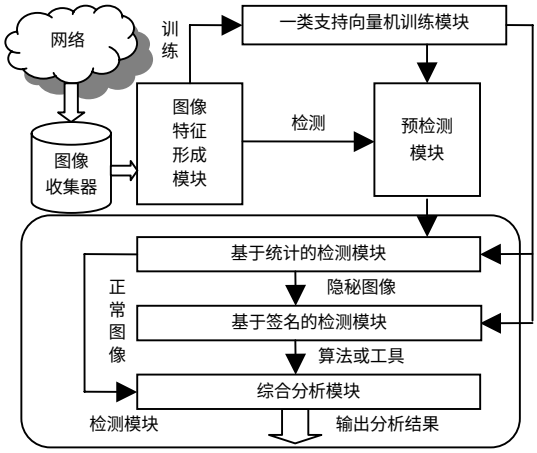

图 1 系统主要工作模块及程序流程

图像收集器现在还没有全部完成，系统测试时所需的图像，直接由人工在网络上获得。

从功能上来说，可将整个系统划分为训练子系统和检测子系统：训练过程负责构建分类器，通过调整支持向量机训练参数可以调整分类器的性能。对于预检测模块，分类器应保证有较低的漏报率，误报率则不做过高要求。对于正式的检测模块，训练参数保证分类器有较低的误报率。检测过程中，待测图像形成特征向量，依次经过预检测、统计检测、签名检测，最后经过综合分析得到图像文件嵌入隐藏信息的可能性和可能使用的隐藏算法。

根据检测系统的处理速度，可以建立 2 种形式的检测模型：(1)实时检测模型；(2)事后分析模型。它们都可以引入分布式处理机制，提高系统的检测速度。本系统采用了事后分析模型，使系统定期地从图像收集器中获得图片，进行特征的形成、提取及检测。

系统的特点主要表现在：

(1)通过多种不同类型的算法的融合与综合分析，提高了检测的准确性、普适性。

(2)通过预检测器和分布式处理方法，加快系统的处理速度，可以大大提高系统检测的速度。

(3)统计方法和签名方法的综合分析，不仅可以估计数字图像隐藏信息的可能性，还可以对嵌入算法、工具进行识别。

(4)整个系统是一个闭环系统，通过自动和人工介入对检测偏差进行修正，可以不断提高系统的检测精度。

3 系统设计中的关键技术

3.1 小波包分解系数绝对值线性预测模型

在系统开发过程中，研究比较了现有的 χ^2 检测、RS 检测、基于JPEG 格式兼容性的检测和基于多分辨分析的检测等多种统计检测方法。其中，多分辨分析具有不受隐藏方法限制、效果良好的突出优点。在R.W.Buccigrossi[4]等人提出的小波分解系数邻居的定义和小波分解系数绝对值线性预测模型的基础上，设计了自然图像小波包分解系数绝对值线性预测模型，并将其作为本系统使用的图像高阶统计分布模型的一个重要组成部分。

对真彩(RGB)图像的每个颜色分量做小波包分解，尺度为 i 的低频、垂直、水平及斜线高频中一点的绝对值分别表示为 $A_i^c(x,y)$、$V_i^c(x,y)$、$H_i^c(x,y)$、$D_i^c(x,y)$，这里 $c\in\{r,g,b\}$。以尺度为 i 的绿色分量的垂直高频为例，其小波包分解系数绝对值线性预测模型可以表示为

$$\begin{aligned}|V_i^g(x,y)| = {} & w_1|V_i^g(x-1,y)| + w_2|V_i^g(x+1,y)| + w_3|V_i^g(x,y-1)| \\ & + w_4|V_i^g(x,y+1)| + w_5|V_{i+1}^g(x/2,y/2)| + w_6|D_i^g(x,y)| \\ & + w_7|D_{i+1}^g(x/2,y/2)| + w_8|V_i^r(x,y)| + w_9|V_i^b(x,y)|\end{aligned}$$

其中，w_k 为权值；$V_i^g(x,y)$ 表示尺度为 i；位置为(x, y)的垂直高频小波包分解系数。这种线性关系可以用矩阵表示：

$$\vec{v} = Q\vec{w}$$

其中，$\vec{w} = (w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8, w_9)^T$；$\vec{v}$ 是垂直高频小波包分解系数矩阵中将 $V_i^g(x,y)$ 的绝对值按列方向串接而成的列向量；矩阵 Q 的各列则对应垂直高频小波包分解系数绝对值预测模型中相邻位置、方向和尺度小波包分解系数的绝对值。最小化下面的均方误差函数：

$$E(\vec{w}) = |\vec{v} - Q\vec{w}|^2$$

可得到垂直高频小波包分解系数绝对值线性预测值的权值 $\vec{w}$。线性预测模型的对数误差由下式给出：

$$\vec{E}_A = \log(\vec{v}) - \log(|Q\vec{w}|)$$

同理可得，红色、蓝色分量的水平高频、斜线高频小波包分解系数绝对值线性预测模型及其对数误差。

3.2 图像特征形成算法

基于小波包分析的图像特征形成算法是该隐秘检测系统的一个关键技术，其主要思想是：

(1)按设定层数对图像进行小波包分解，保存所有终端结点的分解系数；

(2)判断终端结点方向，对所有低频终端结点再进行一次一层小波包分解(因为在计算小波包分解系数绝对值线性预测模型时需要用到所有低频终端结点的更高一层小波包分解结点的系数)；

(3)计算所有终端结点的小波包分解系数绝对值预测模型；

(4)计算所有终端结点系数的统计特性数及其绝对值预测模型对数误差的统计特性数。

由此得到 2 种统计量：一种是在多个方向和尺度上的子频带的系数，包括：均值，方差，偏度，峰度；另一种是基于系数大小的最佳线性预测误差的统计特征。这些统计量共同构成了特征向量。

3.3 分类器设计

如果把所有正常图像特征向量的集合视为正常图像模式类，而把所有隐秘图像特征向量的集合视为隐秘图像模式类，那么图像隐秘检测就转化为一个模式识别问题。

在基于盲检测的技术中，隐藏算法和工具大都是未知的，这无疑增加了分类的困难程度。将支持向量机应用到隐秘检测系统中，可以保证在先验知识不足的情况下，分类器仍有较好的分类正确率，从而使得整个隐秘检测系统具有较好的

检测性能。本文提出了一种基于一类支持向量机[5]的隐秘图像盲检测模型，并将其运用到系统设计中去。

一类支持向量机，最初是用于高维分布估计，即用来寻找超平面 VC 维的估计值。对于没有任何分类信息的训练向量，Tax 等人提出用超球面来划分数据集的想法。其思路是通过计算包含一组数据的最小超球形边界来对该组数据进行描述，以此最小超球作为一类问题的分类器，如图 2 所示，图中，c 为超球面球心；R 为半径；实心圆点代表正常图像样本点；方框代表隐秘图像的样本点。

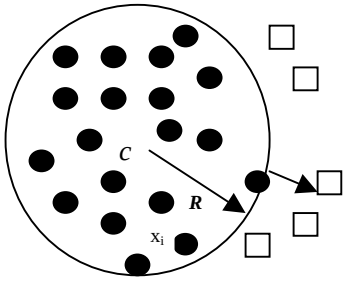

图 2 一类支持向量机分类

在 d 维空间中给定一个包含 n 个的样本的数据集 $\{\vec{x}_1,...,\vec{x}_n\}$，一类支持向量机通过映射 $\phi: R^d \to F$ 将数据对象映射到一个高维的空间中，在此空间寻找一个最小体积的超球体(圆心为c，半径为R)，使尽可能多的x_i都包含在该球体内。通过解一个二次优化问题可得到超球面的圆心和半径。

对于一个新样本，判断它是否属于目标样本，有如下的判别函数：

$$f(\vec{x}) = R^2 - \|\phi(\vec{x}) - \vec{c}\|^2$$

若 $f(\vec{x}) > 0$ 成立，则判断样本 $\vec{x}$ 属于目标样本，即接受其为该类；否则判断其为非目标样本。

在系统设计过程中，基于一类支持向量机的分类器构成了统计检测模块和签名的检测模块。将一类支持向量机应用于基于统计的检测时，系统在训练时仅需要一组正常图像的训练样本，大大减少了计算量。更重要的是，由一类支持向量机训练得来分类器对未参与训练的隐秘图像也有一定的识别率。将一类支持向量机用于基于签名的检测时，需对某类已知隐藏算法和隐藏工具的隐秘图像进行训练，得到关于此类隐秘算法的分类器，若待测图像样本属于此类，则该图像很可能是用此类隐秘算法嵌入了信息。

3.4 应用程序的设计

系统综合运用了 Matlab、Visual C++两种开发工具。由于在图像特征形成算法中多次用到小波、小波包分解、特征值计算等较复杂的数学运算，因此，利用 Matlab 在这方面的优势，开发了图像特征形成模块，分类器则在 LIBSVM 程序的基础上利用 Visual C++平台开发完成。

在系统的应用程序中，大体可以分为数据处理和过程检测 2 大基本类型。数据处理主要包括：图像特征形成，支持向量机训练，数据存储，数据显示和打印等。检测过程控制程序主要是指控制微机按照一定的方法对据进行计算、判断，然后输出以便控制检测流程或给出报警。在应用软件设计时，结合系统整体功能，采用模块化程序设计方法，把整个程序分为若干个模块，每一模块又包括若干子程序。划分模块时，本文制定并遵循了以下原则：(1)每个模块不宜太长，太长不易编写和调试，同时也失去模块化的意义。(2)力求使每个模块间界限分明而且在逻辑上相互独立，以利于单个模块的查询和测试。(3)对于一些简单的任务不必要求模块化。(4)当系统需要进行各种判断时，最好在一个模块中集中进行这些判断。

4 系统性能及实验结果

为了保证系统的有效性，在开发环境下，进行了测试。收集了 4 组图像对进行了性能测试。一组实验针对正常图像，另外 3 组实验分别针对 3 种常用隐秘软件(Jsteg4.1、H4PGP.0 和 F5r11)生成的隐秘图像，且每一组都分别包括 10%、5%、2%和 1% 4 种不同嵌入率的 4 次独立的检测实验。对系统进行训练时，选取正常图像 1 000 幅，隐秘图像各 2 000 幅。测试时隐秘图像和相同格式的正常图像各 500 幅。

实验结果如表 1 所示。表中，rE 表示嵌入率；R_tg 表示统计检测模块对隐秘图像的正确识别率；R_qm 表示签名模块的正确识别率；Time 为图像输入检测模块到输出的检测时间。

表 1 系统性能测试

rE	待测图像	R_tg	R_qm/%	Time/s
0	正常	90.50	---	18.60
1	F5R11	58.60	54.60	15.50
	H4PGP		62.20	16.40
	Jsteg		60.25	20.46
2	F5R11	75.55	76.50	17.50
	H4PGP		72.00	18.40
	Jsteg		78.56	14.53
5	F5R11	86.74	87.00	12.50
	H4PGP		71.25	19.40
	Jsteg		90.20	15.46
10	F5R11	88.33	89.50	16.50
	H4PGP		70.40	18.80
	Jsteg		100.0	17.54

由以上性能测试数据可以看出，系统对 F5r11、Jsteg4.1 和 H4PGP2.0 3 种隐秘软件 4 种嵌入率的隐秘图像均有较好的识别效果，特别是统计识别模块对正常图像和隐秘图像的识别，当嵌入率在 5%以上时，识别率基本都达到 85%以上。基于签名的检测模块检测结果也达到了 70%左右，可以在一定程度上识别出隐秘图像所用的工具和算法。

5 结束语

本文介绍了研制开发的图像隐秘检测系统的结构和功能，讨论了自然图像小波包分解系数绝对值线性预测模型、基于小波包分解的图像特征形成算法及利用一类支持向量机设计分类器等技术。该系统具有结构简单、规模扩展性好等明显优点。系统中一些核心模块已经实现，并利用多组实验证明了系统性能的可靠性。但是，系统仅对 3 种隐秘软件进行了测试，还有很多测试的工作要做，整个系统的实现是今后研究的方向。

参考文献

1 Fridrich J, Goljan M, Hogea D. Steganalysis of JPEG Images: Breaking the F5 Algorithm[C]//Proc. of the 5th Int'l Workshop on Information Hiding. Springer-Verlag, 2002.

2 Farid H. Detecting Hidden Messages Using Higher-order Statistical Models[C]//Proc. of International Conference on Image Processing, Rochester, NY. 2002.

(下转第 153 页)