

校园网认证计费系统的研究与实现

田志英¹, 廖晓群², 赵安新²

(1. 西安科技大学 通信与信息工程学院, 陕西 西安 710054;

2. 西安科技大学 网络中心, 陕西 西安 710054)

摘要:为了构建安全可靠的数字化校园环境,实现用户身份认证和单点登录,建立了结合灵活计费策略的校园网认证计费系统。该系统基于RADIUS通信协议,采用Web+DHCP接入认证技术,通过LAMP应用架构,实现了认证网关和RADIUS服务器的联动,可以灵活地改变计费策略,并有效地进行网络监控数据的交互。系统采用PHP+MySQL技术实现了网络安全管理提供了认证计费管理平台和用户提供了自助服务平台的完美结合,为校园网络的运维管理提供了便利。系统已应用一年,成功实现了对教师和学生用户统一有效的认证计费管理,为用户提供了相对安全的网络环境。它不仅解决了校园网络管理的问题,而且给局域网(公司、校区、网吧、酒店等)认证计费系统的建设提供了一种思路。

关键词:身份认证;计费策略;自助服务

中图分类号:TP311.52

文献标识码:A

文章编号:1673-629X(2010)05-0202-05

Research and Implementation of Campus Network Authentication and Accounting System

TIAN Zhi-ying¹, LIAO Xiao-qun², ZHAO An-xin²

(1. College of Communication and Information Engineering, Xi'an University of Science and Technology, Xi'an 710054, China;

2. Network Information Center, Xi'an University of Science and Technology, Xi'an 710054, China)

Abstract: In order to build a secure and reliable digital campus environment, to achieve user authentication and single-point login, establish the campus network authentication and accounting system combined strategy of flexible billing method. The system based on RADIUS communication protocol and Web+DHCP access authentication technology, through the LAMP application framework, to achieve the certification gateways and RADIUS server interaction, the flexibility to change the billing strategy and effective interaction of network monitoring data. The system uses PHP+MySQL technology to achieve network security management and provide authentication and accounting management platform, user self-service platform may provide a perfect combination for the campus network. This system has facilitated the operation and maintenance management. System has been applied for one year, it achieved for teachers and students an effective and integrated user authentication and accounting management successfully, and provided users with a relatively secure network environment. It not only solved the campus network management problems, but also provided a line of thought for the local area network (corporate, campus, Internet cafes, hotels, etc.) the construction of authentication and accounting system.

Key words: user authentication; billing method; self-service

0 引言

随着Internet的发展和CERNET的接入,校园网络资源越来越丰富,功能越来越复杂。这虽然为用户提供了更广泛的资源共享和信息交流网络平台,但对

网络管理和网络安全问题提出了新的挑战。作为网络安全管理的重要组成部分,认证计费系统的建设势在必行。

目前,认证计费系统普遍存在以下三方面的问题:

①网络对接入用户缺乏有效的接入控制,包括认证、计费、带宽限制、时间限制等,也无法灵活地按要求限制用户的接入。

②单纯的网络连接服务和统一的包月收费这种粗放型的计费方式不能满足不同用户的要求,需要一种以用户为主的,精细、灵活的计费方式。

收稿日期:2009-09-23;修回日期:2009-12-11

基金项目:电子信息产业发展基金项目(XDJ2-0514-27);西安科技大学培育基金(200830)

作者简介:田志英(1985-),女,山西五台人,硕士,研究方向为网络管理、信息技术;廖晓群,高工,研究方向是信息技术。

③网络的管理、运营存在大量的手工操作,不能及时、准确地完成如开户、销户、交费、退费、定期结算等操作,效率较为低下。

针对上述问题,该系统提供了一种解决方案。为了有效控制用户网络接入,对 RADIUS 数据包 attribute 域的值进行修改和添加,实现了对账户 IP、MAC、上行带宽、下行带宽、上网时限等信息的管理;为了满足不同用户的要求,提出了以包月、计时、计流量为计费原型的计费策略方案,实现了相对灵活的计费;为了减轻网络管理的手工操作,设计了人性化的用户自助服务子系统,实现了用户信息注册、开户申请、续费申请、充值申请、销户申请等功能,申请提交后,等待网管人员的审核,提高了信息录入的准确度^[1,2]。

1 相关技术

1.1 AAA 系统和 RADIUS 协议

认证计费系统一般简称为 AAA 认证系统,是指 Authentication(认证)、Authorization(授权)和 Accounting(计费)。一套完善的 AAA 认证计费系统可以很好地解决网络管理和运营过程中出现的问题,比如认证计费 and 用户管理等。

RADIUS(Remote Authentication Dial In User Service, 远程验证拨号用户服务)是解决 AAA 最常用的通信协议。接入服务器和认证计费系统间的通信协议多采用 RADIUS。该协议采用客户机/服务器模式,能支持多种认证体系(PAP、CHAP、UNIX Login)。它通过 UDP 协议来传送数据包,包的格式允许其封装的属性可以不断增加,以支持新出现的认证需求^[3,4],提供了良好的可扩展机制^[5,6]。

目前, freeradius 服务被广泛地应用到 RADIUS 服务器中,它具有高性能和高可配置性,是符合 GPL 规范的免费软件。它带有基于 PHP 的 Web 管理接口 dialup-admin,支持 SQL 数据库用户管理。

1.2 接入认证技术

用户终端与接入服务器之间的接入协议或方式就是接入认证技术,目前最流行的有 PPPoE、Web 和 802.1x 3 种。PPPoE 认证与电信运营商非对称数字用户线(ADSL)接入业务相结合,应用最为广泛;Web 认证和 802.1x 认证主要应用在以太网接入上,也获得了规模应用。这几种认证技术支撑了整个宽带用户接入的发展,对建设可运营、可管理的网络起到了非常大的作用^[7,8]。

Web 兼容性好,应用业务可扩展性强,而且不需要客户端软件,所以备受青睐。Web 认证过程属全三层处理,可以跨越多个网络,灵活性好^[9]。在设备需求

方面,Web 认证和 PPPoE 认证要求相同,需要 BAS 和计费认证系统的支持,但 Web 认证过程中没有 PPP 的打包处理,所以不存在采用 PPPoE 认证方式中的 MTU 影响性能的问题。802.1x 认证的设备一般是成本较低的交换机,其可靠性和安全性都不是很好,抗攻击能力相对来说比较差,所以这种认证方式主要用于用户比较少的网络。而 Web 认证可以提供大容量的用户接入,能够在较大范围内提供高密度用户接入解决方案^[10]。

Web 认证步骤如下:

①用户 PC 机启动,系统程序通过 DHCP,向 DHCP 服务器请求 IP 地址。

②接入服务器(如认证网关)为该用户添加访问记录,目的是限制用户只能访问一些内部服务器、个别外部服务器如 DNS。

③用户登录 Web 认证界面(内部服务器提供服务),提交认证请求信息。

④接入服务器通过 RADIUS 协议和认证系统进行通信,请求对用户进行认证。

⑤认证系统返回认证结果,如果认证通过,用户可以自由访问网络。在使用两次地址分配的情况下,客户端会触发用户重新获取新的 IP 地址。

⑥用户下线时,接入服务器会更新用户记录,并通告计费系统停止计费,用户的网络访问受限。如果使用两次地址分配,客户端会触发用户再次获取 IP 地址^[11]。

该系统采用 Web 方式进行接入认证,用户数据包的识别方式为 IP+VLAN+MAC,安全性高。

2 系统组成

2.1 系统工作基本原理

系统主要由认证网关、RADIUS 服务器和后台数据库三部分组成。认证网关和 RADIUS 服务器之间通过 UDP 协议进行传输,传输时用共享密钥来加密(key),且共享密钥不在网上传输。默认认证端口是 1812,计费端口是 1813。

系统实现的体系框图如图 1 所示。

用户向认证网关提交认证请求;认证网关向 RADIUS 服务器转交用户认证信息;RADIUS 服务器将用户信息与数据库信息进行比对,如果符合,则认证通过并授权,用户可以顺利访问网络资源,并开始计费,否则,认证失败,用户被拒绝访问网络资源。

可见,RADIUS 服务器是整个系统的核心,它与认证网关连接,处理用户的认证和计费请求。在认证阶段,从认证网关提取用户名和密码,连接数据库,进行

查询比较。在计费阶段,连接数据库,更新计费信息记录、上网日志记录等。

2.2 系统功能模块

该系统可分为三个子系统:网管子系统、用户自助服务子系统和后台通信子系统。

网管子系统由系统管理维护功能模块(数据库备份与恢复、日志管理、系统信息管理、系统升级管理)和用户管理维护功能模块(用户信息管理、账户使用明细查询等)组成。用户自助服务子系统功能主要包括用户注册、账号充值申请、账号续费申请、使用明细查询和用户信息维护。功能框图如图 2 所示。

通信子系统是解决认证网关和 RADIUS 服务器的实时信息交互问题,是基于 RADIUS 协议的 UDP 数据包传输。 workflows 如图 3 所示。

3 系统的实现

3.1 freeradius 安装

从 <http://freeradius.org/download.html> 下载 freeradius2.0.0.tar.gz 文件,解压缩后执行 ./configure、make all、make install 编译并安装。freeradius 的主配置文件(radiusd.conf、sql.conf、client.conf)放在 /usr/local/etc/raddb 目录下,radiusd 运行文件放置在 /usr/local/sbin 目录下。最后,执行 radiusd -X 命令,启动 freeradius 服务。若正常启动,则会出现:

Listening on authentication address * port 1812

Listening on accounting address * port 1813

Listening on proxy address * port 1814

Ready to process requests.

3.2 数据库设计

该系统后台数据库使用的就是 MySQL 数据库。利用 PowerDesigner 工具软件创建 xkradius 数据库。通过对系统三大功能模块的功能细化和详细设计,将库表分为四类:用户信息表类、账户信息表类、计费策略

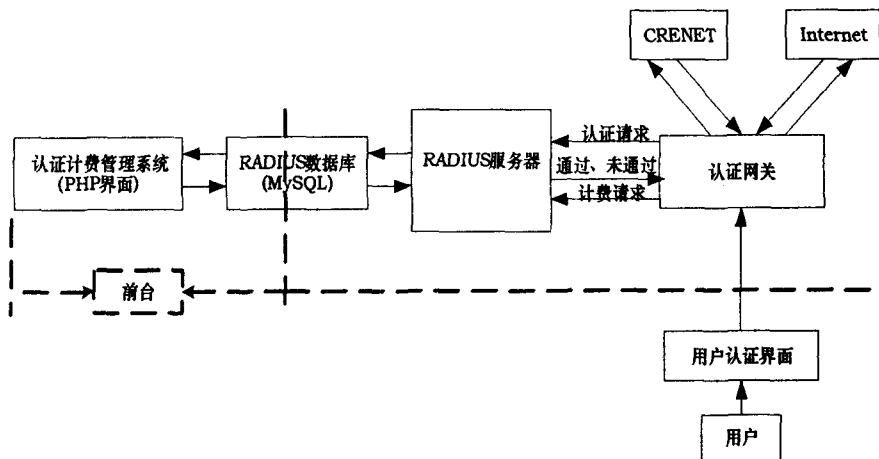


图 1 系统体系框图

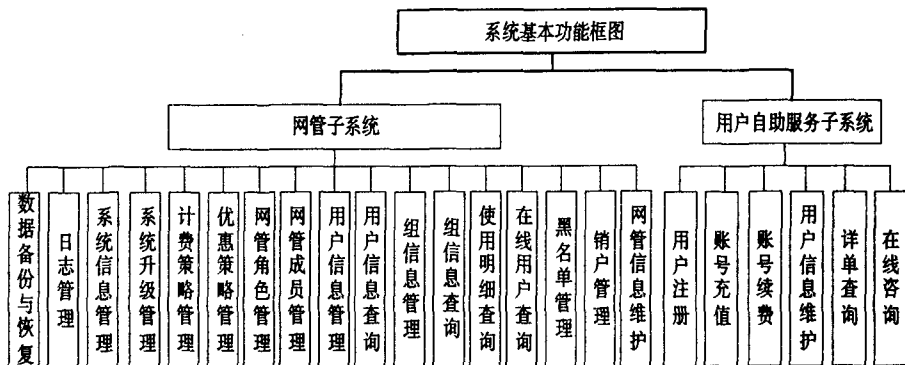


图 2 系统基本功能框图

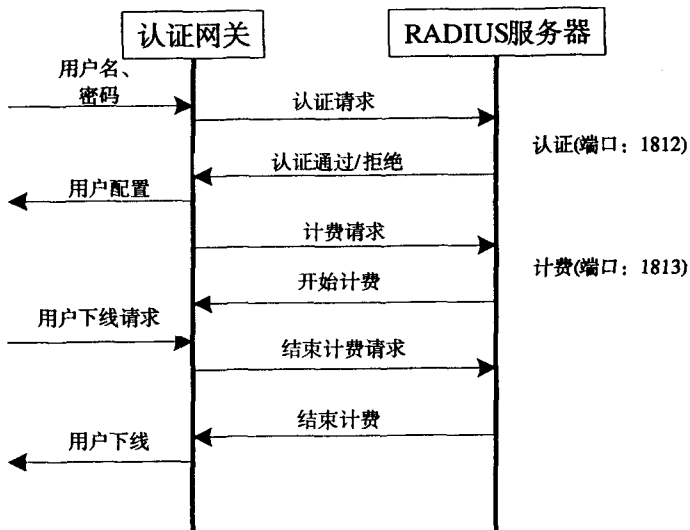


图 3 通信子系统工作流程图

表类、RADIUS 后台通信表类。其中,用户信息表类中的表字段信息可以从校园网信息平台的学籍管理系统和教务管理系统直接获取^[12];账户信息表类可以同校园一卡通系统和财务管理系统共享;计费策略表类为系统计费功能的扩展提供了有效的后台数据库支持,以实现计费策略灵活管理;RADIUS 后台通信表类的设计主要是为了存放认证网关上定时接收到的账户信

息(IP、MAC、上线时间、下线时间等)。xkradius 数据库包括 18 个表:用户基本信息表(user_base_info)、radius 响应信息表(radreply)、radius 检测信息表(radcheck)、radius 组响应信息表(radgroupreply)、radius 组检测信息表(radgroupcheck)、radius 用户组信息表(radusergroup)、radius 授权信息表(radpostauth)、badusers_table(黑名单表)、account_log_table(账户日志表)、online_table(在线信息表)、admin_table(管理员信息表)、user_traffic_table(用户流量表)、prepaid_log_table(充值日志表)、conpaid_log_table(续费日志表)、accountclapol(计费策略分类表)、pakgepol(包月策略表)、timepol(计时策略表)、trafficpol(计流量策略表)。在表中添加相应的字段后,生成 xkradius.sql 文件,以便导入到 MySQL 数据库中。

3.3 配置 freeradius 服务

radiusd.conf 文件:去掉 authorize 和 accounting 函数体内的 sql 注释(#),确保 sql 功能可用。

sql.conf 文件:修改 server(数据库服务器 IP 地址值)、login(root)、password(MySQL 的 root 密码)、radius_db(数据库名)的值。

clients.conf 文件:插入 client{} 函数,以添加认证网关服务器的相关信息(IP、secret、shortname)等。

3.4 Web 服务管理

系统 Web 服务是建立在目前最流行的 Web 应用

基础架构 LAMP(Linux + Apache + MySQL + PHP)上。因此,只需考虑 Web 服务的管理问题,webmin 应用服务软件提供了一个友好的可视化 Web 管理平台。在 webmin 中,只要打开 Apache Webserver 选项,修改 virtual server 下的 address、port、Document root(dialup-admin 文件包路径)的值,配置 Web server 服务。然后,打开 MySQL Database Server 选项,添加数据库 xkradius,导入已生成的 xkradius.sql 数据库文件,相当于在 MySQL 数据库中创建了 18 个表,并且可以进行管理和修改。

3.5 功能的实现

3.5.1 网管子系统和用户自助服务子系统的实现

这两个子系统功能主要是通过 PHP 语言技术对后台数据库的操作来实现的。数据流图如图 4 所示。

3.5.2 通信子系统的实现

该子系统功能通过 C 语言技术对基于 RADIUS 协议的 freeradius 服务的实现来完成。认证计费流程图如图 5 所示。

4 结束语

该系统已应用一年,成功实现了对教师和学生用户统一有效的认证计费管理,为用户提供了相对安全的网络环境。它不仅解决了校园网络管理的问题,而且给局域网(公司、校区、网吧、酒店等)认证计费系统

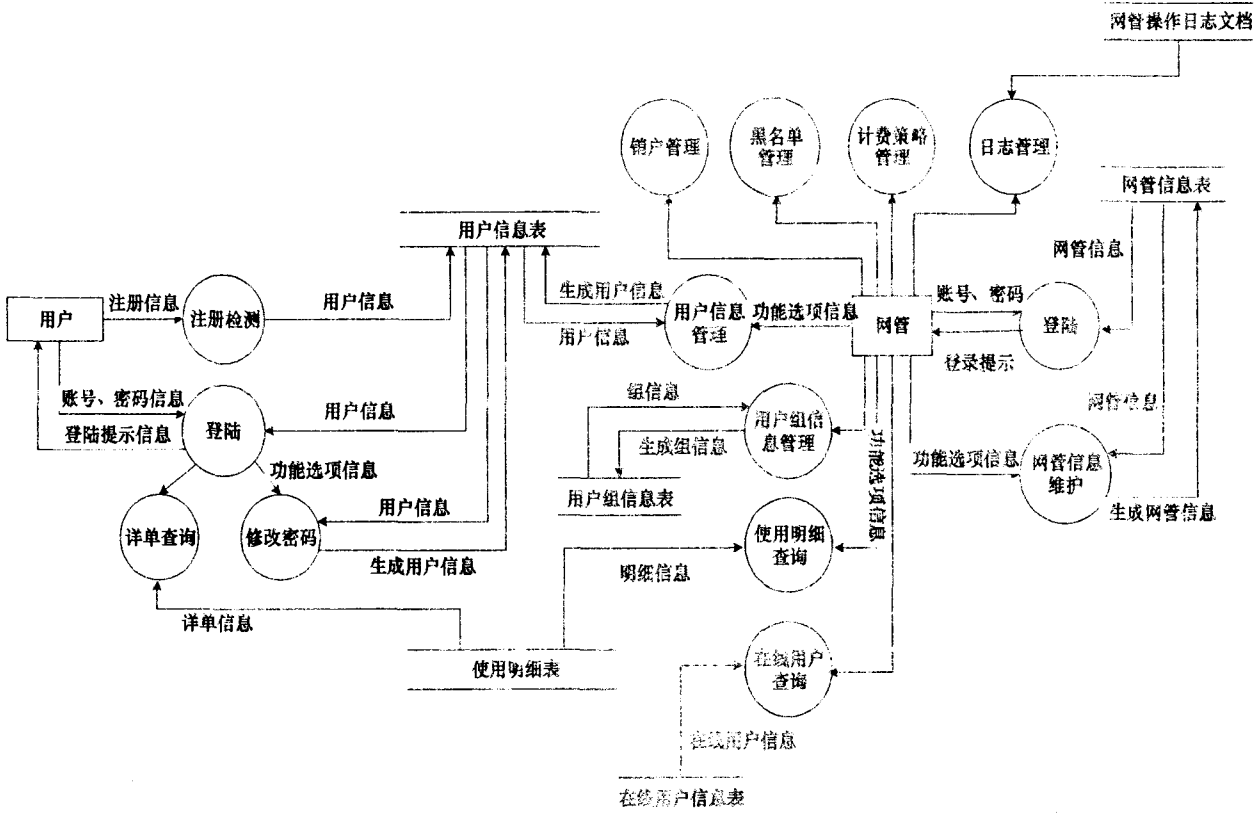


图 4 系统数据流图

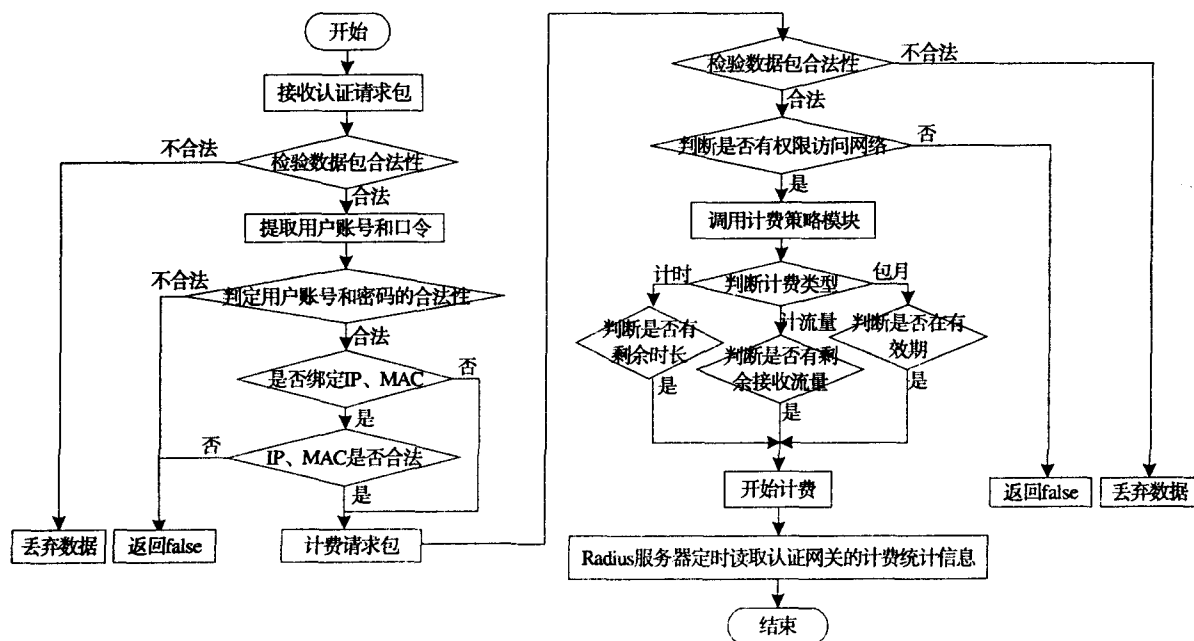


图 5 认证计费流程图

的建设提供了一种思路。

随着用户数量的不断增加,网络负荷会逐渐加重,为保证系统的快速性和稳健性,可结合接收数据流和发送数据流的分离、认证流和计费流的分离的技术对系统进行改进。

参考文献:

- [1] 梁 根. 基于 RADIUS 的校园网认证管理系统的研究与实现[J]. 计算机技术与发展, 2006, 16(6): 45-47.
- [2] 丰 艳. 基于 RADIUS 协议的 VOIP 认证/计费系统的设计与实现[J]. 计算机工程与设计, 2008, 29(3): 3478-3481.
- [3] 唐 磊, 金连埔. 大型拨号认证计费服务器的设计与实现[J]. 计算机工程与设计, 2004(7): 160-161.
- [4] 王保泉, 赵艳红, 陈发明. 网络计费系统的设计与实现[J].

南京工业大学学报, 2004, 26(5): 68-71.

- [5] IETF RFC2881. Network Access Server Requirement NAS Model[S]. 2000.
- [6] IETF RFC2865. Remote Authentication Dial In User[S]. 1997.
- [7] IETF RFC2138. Remote Authentication Dial In User[S]. 1997.
- [8] IETF RFC2139. RADIUS Accounting[S]. 1999.
- [9] IETF RFC2866. RADIUS Accounting[S]. 2000.
- [10] 肖 义. 3 种接入认证技术的浅析与比较[J]. 光通信研究, 2006(3): 25-28.
- [11] 徐云和, 谢刚生, 肖根如, 等. 基于 OLE 的校园管理信息系统实现[J]. 西安科技大学学报, 2004, 24(4): 451-455.
- [12] 王晓路, 卢建军, 马 莉. 基于 JAVA 的连接池优化 Web 数据库连接[J]. 西安科技大学学报, 2005, 25(2): 228-231.

(上接第 201 页)

- tion, 1992, 87: 7-16.
- [7] Kegl B, Krzyzak A. Piecewise linear skeletonization using principal curves[J]. IEEE Transaction on Pattern Analysis and Machine Intelligence, 2002, 24(1): 59-74.
- [8] Besl P J, McKay N D. A method for registration of 3-D shapes[J]. IEEE Trans on Pattern Analysis and Machine Intelligence, 1992, 14(2): 239-256.
- [9] Mumford D, Shah J. Optimal approximation by piecewise smooth functions and associated variational problems[J]. Commun. Pure Appl. Math, 1989, 42: 577-685.
- [10] Chan T F, Vese L A. Active Contour without Edges[J]. IEEE Trans on Image Processing, 2001, 10(2): 266-277.

- [11] Sethian J A. Level Set Methods and Fast Marching Methods Evolving Interfaces in Computational Geometry, Fluid Mechanics, Computer Vision and Materials Science[M]. 2nd ed. Cambridge, UK: Cambridge University Press, 1999.
- [12] 娄 震, 胡钟山, 杨静宇. 基于轮廓分段特征的手写体阿拉伯数字识别[J]. 计算机学报, 1999, 22(10): 1065-1073.
- [13] Malpica N, de Solorzano C O, Vaquero J J, et al. Applying watershed algorithms to the segmentation of clustered nuclei[J]. Cytometry, 1997, 28: 289-297.
- [14] Bleau A, Leon L J. Watershed-based segmentation and region merging[J]. Computer Vision and Image Understanding, 2000, 77(3): 317-370.