

## 指纹认证在考试管理中的应用

杨文伟, 严继良

(广东工业大学计算机学院, 广东 广州 510090)

[摘要] 针对考试替考、做假证件代考等作弊问题,提出将自动指纹识别技术应用到考试管理上,利用考生和管理人员的指纹特征值来判别其真实身份,设计出基于指纹认证的考试管理系统体系结构,并解决在研究的过程中所遇到的关键问题,最后对整个系统进行了实验研究,验证了该系统的可行性。

[关键词] 自动指纹识别技术; 考试管理; 广东教育考试院

[中图分类号] TP39 [文献标识码] A [文章编号] 1000-9965(2009)01-0054-03

### Research of exam management based on fingerprint authentication

YANG Wen-wei, YAN Ji-liang

(Guangdong University Of Technology, Guangzhou 510090, China)

[Abstract] Fingerprint recognition will be applied to the examination administration for Cheating, This paper designed exam management architecture based on fingerprint authentication is on this background, and resolved the key issues. Finally, designed all of the modules, analyzed the experimental results, the experiment concluded that the article on the examination of fingerprint authentication management applications is feasible.

[Key words] automatic fingerprint recognition technology; exam management; the education examinations authority of Guangdong Province

随着社会和经济的发展,对自动指纹识别技术的理论和应用的广泛研究,自动指纹识别技术也日益成熟,已经成为身份认证的最有效手段,在电子商务、犯罪识别、信息安全等领域得到广泛的应用。

考试作弊一直是困扰社会的一大问题,尽管考试管理人员做出了种种措施来应对,但是替考、做假证件代考等现象时有发生。如何加强对考试的管理已成为一个不容忽视的问题。将自动指纹识别技术应用到考试管理上,利用考生和管理人员的指纹特征来判别其真实身份,最终可以真正实现考试的公平和公正。

目前国内外将指纹识别技术应用到身份认证中的方法是:首先考试管理部门将考生的指纹特征信息存储在 IC 卡中;然后利用验证终端将 IC 卡中存

放的考生信息同考生活体指纹进行匹配。此方法存在两大问题:IC 卡中存放的考生指纹信息易被恶意修改;考生携带 IC 卡容易丢失,并且增加了考生买 IC 卡的费用。

针对上述问题,结合广东省教育考试院现有系统硬件和软件的实际情况,本文提出并设计一种基于指纹识别技术的考试管理系统方案,通过实验验证了该方案的可行性。

### 1 自动指纹识别技术

自动指纹识别技术是利用人类指纹的唯一性,通过对指纹图案的采样、特征信息提取并与库存样本相比较的过程来实现身份识别的技术<sup>[1]</sup>,它通常包括个体指纹采集、指纹图像预处理、指纹特征值提

取和指纹匹配四大部分<sup>[1]</sup>。

### 1.1 指纹采集

指纹采集是通过图像采集终端设备将指纹图像真实地传输到计算机中,交给计算机进行处理。指纹采集主要分为“脱机”模式和“联机”模式两种,光学采集仪和 CMOS 工艺的电容式采集仪是目前应用最广泛的两种指纹采集设备。

### 1.2 指纹图像预处理

指纹图像预处理就是对低质量的指纹图像采用一定的算法进行处理,使其纹线结构清晰化,尽量突出和保留固有的特征信息以避免产生伪特征信息。通常,指纹图像预处理流程如图1所示<sup>[2]</sup>。

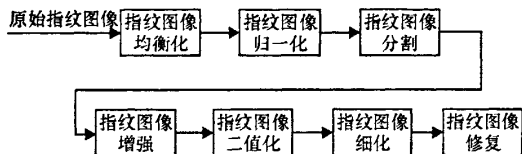


图1 指纹图像预处理流程图

### 1.3 指纹特征值提取

指纹特征值的提取就是采用邻域判定法对指纹图像的脊线逐一进行检测,提取所有的特征点。

### 1.4 指纹匹配

指纹匹配就是将当前输入的指纹特征值与先前保存的指纹特征模板值相比较,判断是否属于同一指纹。指纹匹配的算法主要包含基于点模式匹配算法、基于纹理模式匹配算法和基于图的匹配算法<sup>[3]</sup>。目前,经典的指纹匹配算法都是基于点模式匹配的,它是采用相似变换的方法把两个特征值集  $P$  和  $Q$  中相对应的点匹配起来,其中  $P = \{P_1, P_2, \dots, P_m\}$  从一幅图像抽取,  $Q = \{Q_1, Q_2, \dots, Q_n\}$  从另一幅图像抽取它们之间的匹配就是找到一个校准函数  $G(t_x, t_y, s, \theta)$ , 即  $G(P_i) = Q_j$ , 以使两个点集有最大数量的点对之间存在稳定的对应关系<sup>[4]</sup>。

## 2 基于指纹认证的考试管理系统分析与设计

### 2.1 系统分析

考试管理系统客户端采集考生基本信息成功后,立即采集该考生指纹特征信息,如果与指纹库里指纹匹配成功则重新采集,否则采集成功。另外,为了对管理员登陆系统进行身份认证还需采集系统管理人员的指纹特征信息。考试前,管理人员在广域网上远程下载本区域的考生指纹信息到指纹识别终端设备上;在考生进入考场前,利用指纹识别终端设备对考生身份进行认证。

### 2.2 系统设计

针对广东省教育考试院软硬件环境和原有信息系统的结构,克服 C/S 和 B/S 模式种种的局限性,本系统采用三层 C/S 和 B/S (Browser/Server) 模式相结合的体系结构,系统体系结构如图2。

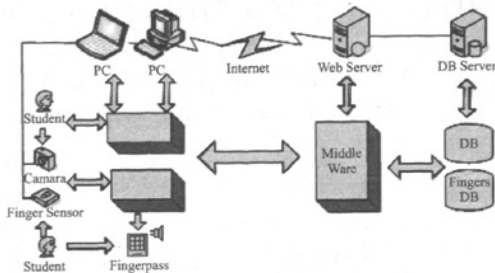


图2 系统体系结构图

系统划分为考生基本信息采集、考生联系方式采集、考生简历信息采集、考生家庭关系采集、考生报考科目采集、考生信息管理、考生相片管理、考生指纹信息管理、指纹匹配、系统管理等十一大模块。

## 3 关键问题分析与研究

### 3.1 与原有的系统集成

在不改变原有系统的前提下增加新的指纹采集和识别新业务,采用怎样的分布式信息处理技术才能成功地实现与原有的系统集成成为设计中的一大问题。通过对 CORBA、DCOM、COM、RMI 等技术和基于 Web Services 的 SOA、SCA 等系统集成参考框架的比较,为了不改变原有系统的 J2EE 架构,使用 COM 桥技术能使任何一种开发工具开发的客户都可以顺利的访问 J2EE 服务器上的 EJB 组件,如图所示:

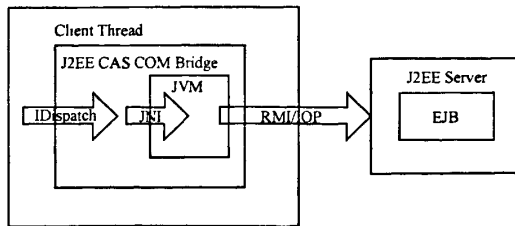


图3 COM 桥集成模型

### 3.2 基于指纹认证的网络通信安全机制研究

传统的网络通信安全机制是采用 ID + 密码的方式来保障用户的合法身份,但是这种方式难以满足现代信息平台的安全需要,为了解决信息在网络中的传输安全,结合指纹的独特性和唯一性,将指纹特征信息同 RSA 密码体制与 MD<sub>5</sub> 算法结合在一起对用户身份进行认证。

在本文所研究的基于指纹认证的网络通信安全

机制中,客户端为每个登录系统的管理员用户生成公钥  $pk_a$  和私钥  $qk_a$ ,并将管理员指纹特征值采用 RSA 加密后,传递到服务器端,服务器端使用自己的私钥  $qk_s$  进行解密,得到会话用户的公钥  $pk_s$  和用户指纹特征值,将用户指纹特征值与指纹数据库相匹配,匹配成功后,将管理员请求的消息采用  $MD_5$  进行数字签名,利用用户公钥  $pk_a$  将签名后的消息采用 RSA 加密后又发回给客户端,客户端收到后,利用私钥  $qk_a$  对其进行解密,并利用  $MD_5$  算法判断其值是否被篡改过<sup>[5]</sup>。整个通信安全机制过程如图4所示。

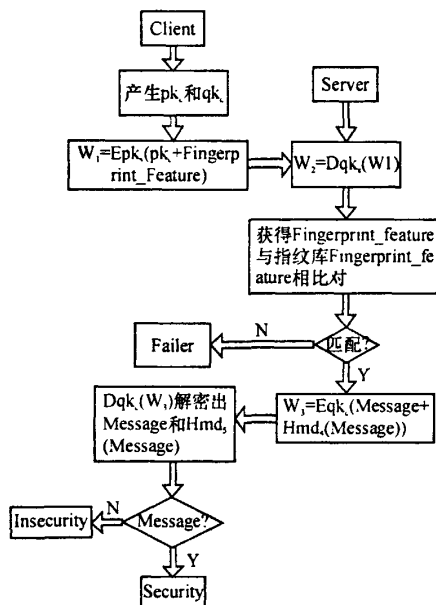


图4 基于指纹认证的网络通信安全机制

### 3.3 指纹识别模式和识别算法

指纹识别模式和识别算法的选择对指纹匹配的效率,保障系统可靠性起到了关键性的作用。

在设计过程中,针对两次指纹识别范围的不同,设计出不同的识别模式。结合考试管理的特征,在指纹采集阶段,采用  $1:N$  ( $N < \text{考区总考生人数}$ ) 的模式;在指纹识别现场采用  $1:N_{\text{few}}$  ( $N < \approx 30$  人) 的模式。

指纹识别算法选择 Neurotechnology 公司的 VeriFinger5.0 开发包,其中的指纹识别算法在国际指纹识别大赛中获得了较好的成绩。

## 4 系统实现与实验分析

系统采用 J2EE 架构实现考生基本信息的采集和系统管理员的管理模块,指纹采集模块采用 Delphi 编写的客户端,系统运行在 Fujitsu SPARC Enter-

prise M9000 服务器,服务器 OS 采用 Solarise 10 64 位 UNIX 操作系统,数据库管理系统采用 Oracle 10g, WEB 应用服务器软件采用 Weblogic 10,客户端主要采用装有 Windows 系列操作系统的 PC 机。

系统在实验环境下,使用了 2000 枚指纹样本作为考生指纹和管理员指纹进行测试,各个功能模块的具体测试结果数据如表 1。

表1 系统测试结果

测试模块	测试结果
考生指纹采集	平均时间为 0.5 s, FAR 在 2 000 枚的范围内为 0%, FRR < 0.2%
管理员指纹登录	平均时间为 0.10 s, FAR 在 2 000 枚的范围内为 0%, FRR < 0.1%
管理员指纹 RSA 加解密	增加了时间开销,但是安全系数增加了 3 倍
考生指纹数据下载并写入到指纹识别设备	不分县区下载时间为 30 s,分县区下载平均时间为 5 s,写入指纹识别时间为 40 s
现场端考生指纹匹配	平均时间为 0.3 s, FAR 在 30 枚的范围内为 0%, FRR < 0.1%

通过对测试结果分析,系统能正确完成考生指纹的采集,指纹模板库的建立,考生指纹的匹配,系统管理员的指纹认证以及指纹特征值在网络上的安全传输,各模块的性能指标都符合基本要求。

与传统的 ID + 密码安全机制相比较,将指纹认证应用到考试管理系统上更大程度上保障了应用系统的安全;与使用 IC 卡存储考生指纹作为身份认证相比较,本方案将活体指纹存储在指纹数据库,减少了制作 IC 卡的步骤,节约了时间和成本,方便了考试管理人员和考生,提高了工作效率,在理论上和应用上都是可行的。

### [参考文献]

- [1] 尹义龙, 宁新宝, 张晓梅. 自动指纹识别技术的发展与应用[J]. 南京大学学报: 自然科学版, 2002, 1: 1-1.
- [2] 王卫东, 平西建. 自动指纹识别技术研究[J]. 信息工程大学学报, 2005, (5): 217-219.
- [3] SEONJOO KIM, DONGJAE LEE, JAIHEI KIM. Algorithm for detection and elimination of false minutiae in fingerprint images. Audio-and Video-Based Biometric Person Authentication, Third International Conference, AVBAP2001[C]. Sweden: Halmstad, 2001: 235-240.
- [4] 罗希平, 田捷. 自动指纹识别中的图像增强和细节匹配算法[J]. 软件学报, 2002, 13(5): 946-955.
- [5] 杨琴, 夏德麟, 晏蒲柳. 一种基于指纹识别的网络通信安全平台[J]. 计算机工程, 2001, (3): 129-134.

[责任编辑: 黄建军]