第17卷 第1期
2007年1月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.17 No.1
Jan. 2007

基于指纹识别的网络身份认证系统

吴教育,曾东海
(广东科学技术职业学院 计算机工程技术学院,广东 广州 510640)

摘 要:指纹识别技术已经广泛地应用于公安、银行、证券等机关、企事业单位。介绍了指纹识别技术及其在身份认证方面的应用,提出了基于指纹识别的网络身份认证系统的一种解决方案,给出了系统的拓扑结构和软件体系结构。该系统针对不同的领域配以不同的应用软件,可应用于远程网络数据库的访问权限及身份的确认等,以提高网上业务活动的安全性。

关键词:指纹识别;指纹特征值;指纹身份认证系统
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2007)01-0170-02

Network ID Authentication System Based on Fingerprint Identification

WU Jiao-yu, ZENG Dong-hai
(Department of Computer Engineering and Technology, Guangdong Institute of Science and Technology, Guangzhou 510640, China)

Abstract: Fingerprint identification technology has been widely used in such enterprises and public institutions like public security organs, banks, securities business and so on. Introduces the fingerprint identification technology used in ID authentication, provides a solution for the network ID authentication system based on fingerprint identification, gives the system topology and software architecture. This system also gives the different application software for different field, may be applied in the long-distance network database access rights and the ID confirmation and so on, and enhances the security of on-line service activity.

Key words: fingerprint identification; fingerprint characteristic value; fingerprint ID authentication system

1 指纹识别技术

指纹识别技术,可称为人体密码,是模式识别领域中使用最早的,也是最为成熟的生物鉴定技术,它是集传感器技术、生物技术、电子技术、数字图像处理、模式识别于一体的高新技术[1]。

指纹识别技术的核心是指纹识别算法,可以把识别算法大致分为3个步骤:图像预处理、指纹特征提取和指纹特征比对[2]。多年来在各个公司及其研究机构产生了许多数字化的指纹识别算法,指纹识别算法最终都归结为在指纹图像上找到并比对指纹的特征。指纹比对分为两类:验证和辨识。验证是利用人员的ID,先从指纹库中将事先录入的指纹特征提取出来,然后与现场采集的指纹提取的指纹特征值进行一比一的比对,来证明该人员为所要识别的人。辩识是将现场采集到的指纹,提取指纹特征值,同指纹库中存储的指纹特征值逐一对比,从中找出与现场指纹相匹配的,并识别人员身份,辨识是一比多的匹配过程[3]。

在指纹识别的过程中,计算机必须对输入的指纹图像进行处理,以实现指纹的分类、定位、提取形态和细节特征,然后才根据所提取的特征进行指纹的比对和识别。指纹识别的过程如图1所示。

图1 指纹识别过程

由于计算机处理指纹时,只涉及了指纹的一些有限的信息,而且比对算法并不是精确匹配,其结果也不能保证100%准确。指纹识别系统的特定应用的重要衡量标志是识别率。主要由两部分组成:拒真率(FRR)和误识率(FAR)。可以根据不同的用途来调整这两个值。FRR和FAR是成反比的。用0~1.0或百分比来表达这个数[4]。

2 指纹身份认证

在日常生活中,无论你是到银行取钱,到网上交易,还是参加社保或医保,所有这些场合都需要身份的认证,而传统的身份认证技术由于受到证件伪造以及密码被窃取、破解等的威胁,逐渐表现得有些力不从心。现在,科技的发展让人们有了新的选择——应用指纹识别技术进行身份认证,即指纹身份认证。

指纹身份认证有以下优点[5]:

(1) 人的指纹具有唯一性和不变性。从目前研究的

收稿日期:2006-04-12
基金项目:广东省科技厅2001年火炬计划项目(C10203)
作者简介:吴教育(1964-),男,江西人,硕士,副教授,研究方向为计算机软件与应用、系统数据维护。

结果来看,世界上还没有完全相同的两枚指纹。且一个人的指纹从一出生就确定下来,不随年龄的改变而变化。

(2) 指纹的采集相对容易。目前已有多种类型的指纹采集仪器,只需用手指一按,就可以取得指纹图像。

(3) 指纹识别算法已经相当成熟。目前已有很多公司专门从事指纹识别算法的研究和供应,提供成熟的基于PC或更大型计算机系统的指纹识别算法和基于嵌入式系统的指纹识别算法。好的指纹识别算法的拒真率和误识率可以同时达到1%和0.1%以下。

因此,指纹身份认证是目前最安全、最可靠的身份鉴定方法,是具有法律权威的验证手段,已经广泛应用在电子商务、公安、保险、医疗等领域,比如,在网上贸易中进行交易时的终端客户身份确认;在银行业务中用来确认银行柜员身份和银行储户身份;在考试管理中,用于考生身份的确认;在公安刑侦领域用于确认犯罪嫌疑人;在医疗保险方面用于献血输血管理、个人医疗档案管理、保险受益人确认等等。

3　网络环境下的指纹身份认证系统

近年来,互联网络带给人们的方便与利益,正在快速增长之中,但也因此产生了很多的问题,尤其在信息安全方面。由于指纹特征数据可以在计算机网络上进行传输和验证,网络指纹身份认证系统可以极大地提高网上业务活动的安全性。下面给出了对基于网络的指纹身份认证系统的解决方案。

(1) 系统的拓扑结构。

系统的拓扑结构如图2所示。

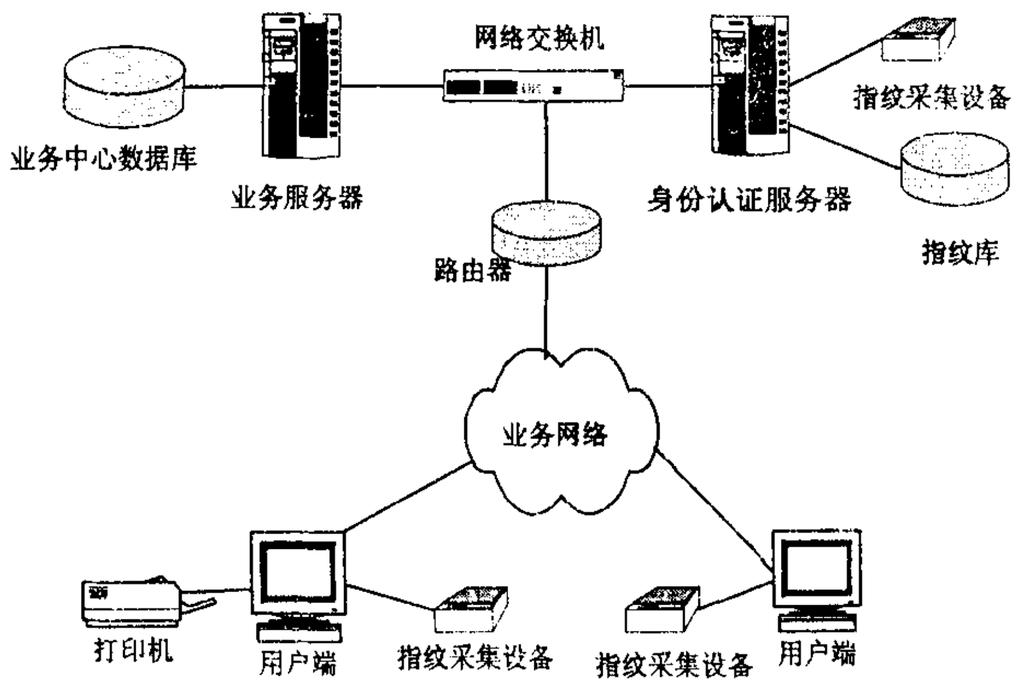

图2　系统的拓扑结构

①身份认证服务器:是身份认证的服务器端,负责认证操作,根据认证策略最终决定认证是否通过;负责处理在身份认证过程中所需的所有数据资料和信息;负责对认证记录进行分析,完成对网络的全局监控,提供正常和异常操作警告和报告。负责指纹库的建立、管理和维护。

②用户端:主要负责获取用户ID和采集用户指纹数据,并提取指纹特征值,将用户ID和指纹特征值加密传送到身份认证服务器。

③业务服务器:负责完成相应的业务操作,需根据具体应用领域安装相应的业务应用模块。

当用户要访问业务服务器的信息资源时,必须通过用户ID和指纹进行身份认证。首先,用户在用户端用ID进行系统登录,由指纹采集设备采集用户的指纹数据,并在用户端进行用户指纹数据的处理,获得指纹特征值;然后,通过网络将用户ID和指纹特征值传送到身份认证服务器,身份认证服务器根据用户ID从指纹库取出该用户的指纹模板与用户端传送来的指纹特征值进行比对认证,如果认证通过就允许用户进行有关的业务操作,否则禁止用户进行操作。

由于身份认证操作是在服务器端完成,用户端获取的身份认证信息(用户ID和指纹特征值)需在网络上进行传输。在传输过程中,用户的身份认证信息可能会被非法用户窃取或破坏。为使用户的身份认证信息安全到达服务器,在传输前需对身份认证信息进行加密处理。

(2) 系统的软件体系结构。

系统的软件体系结构如图3所示。

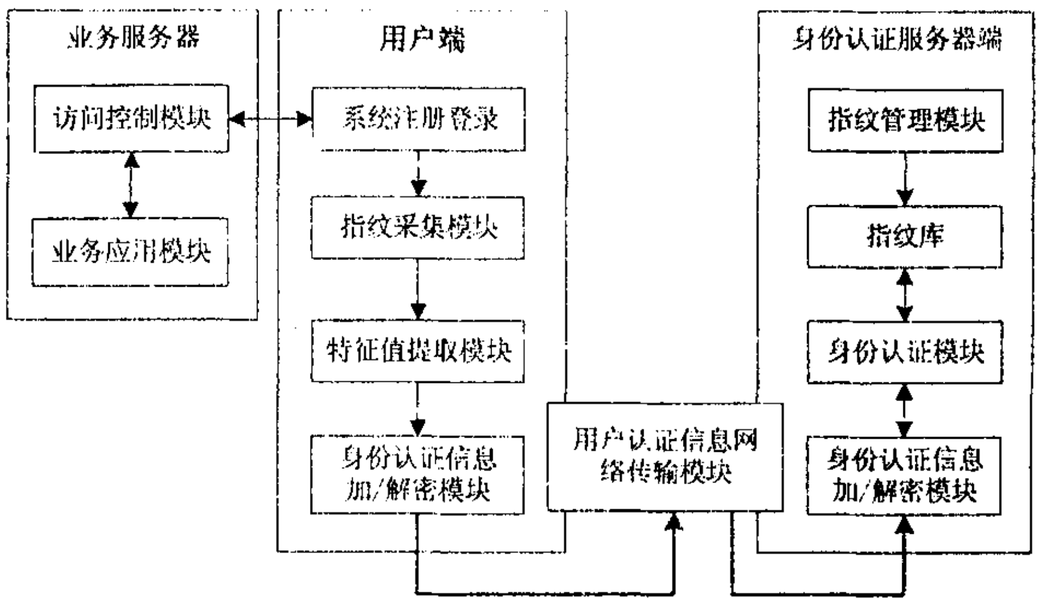

图3　系统的软件体系结构

系统注册登录模块:为用户提供系统注册、登录界面。

①指纹采集模块:负责采集用户指纹数据。

②特征值提取模块:负责对采集到的指纹图像进行预处理,提取其特征值。

③身份认证信息加/解密模块:在用户端负责将提取到的用户ID和指纹特征值进行加密处理,在服务器端负责对传输到服务器的已加密的身份认证信息进行解密处理。

④用户认证信息网络传输模块:负责已加密的用户身份认证信息在网络上的安全传输。

⑤身份认证模块:负责根据用户ID和指纹特征值进行用户身份认证,负责认证信息管理及认证记录分析。

⑥指纹管理模块:负责指纹库的建立,指纹库中应包括所有合法用户的指纹模板;负责指纹库的管理和维护,比如指纹库的更新、查询等。对身份认证方式和策略进行设定和管理,根据用户、用户组、用户任务和应用软件的不同组合,实现对用户的访问权限进行分配和设定。

⑦访问控制模块:监控用户的登录状态,在业务服务器上控制用户对业务服务器资源的访问权限,完成业务应用模块与身份认证模块之间的连接、交互及数据交换等。

(下转第176页)

新实例时,需要重新计算原训练集 D 中每个元素的新类型支持概率 θ' 值,有了额外的时间开销,时间开销为 $N(\sum_{i=1}^{m}[(n+i)(m-i)])$ 级。在空间和时间的额外开销方面,都在可接受范围,所以该算法是可行的。

在增量学习算法中,反复用训练数据检验,这使得样本实例属性值之间的条件相关性不断弱化,减小其负面影响。因而,在朴素贝叶斯分类算法的基本限制和明显缺陷方面,增量学习算法都对其有不错的完善。

5 结束语

如何改善朴素贝叶斯分类算法,提高其在入侵检测系统中的性能,仍然是目前一个比较重要的课题。除了文中所述的方法外,还有很多诸如贝叶斯分类算法与决策树结合[3]、贝叶斯分类算法与信念网络结合[1]等等的方法。但各种方法不是降低实例属性值之间的条件依赖程度,就是提高用先验知识来预测后验数据的准确率。增量学习策略是一种相对简便实用的弥补方法,而怎样选择新实例加入到训练集 D 中,更好地完备训练集 D 来改善文中算法,仍然值得做深入的研究工作。

参考文献:

[1] Lee Wenke, Stolfo S J, Mok K W. A Data Mining Framework for Building Intrusion Detection Models[C]//Proceedings of the 1999 IEEE Symposium on Security and Privacy. Los Alamos, CA: IEEE Computer Society Press, 1999: 120 - 132.

[2] Firedman N, Geiger D. Bayesian network classifier[J]. Machine Learning, 1997, 29: 103 - 130.

[3] 张王番. 多种策略改进朴素贝叶斯分类器[J]. 微机发展, 2005, 15(4): 35 - 37.

[4] Han Jiawei, Kamber M. 数据挖掘概念与技术[M]. 范 明, 孟小峰, 等译. 北京: 机械工业出版社, 2005.

[5] 张 琨, 徐永红, 王 珩, 等. 用于入侵检测的贝叶斯网络[J]. 小型微型计算机系统, 2003, 24(5): 913 - 915.

[6] Yager R R. An extension of the naive Bayesian classifier[J]. Information Sciences, 2006, 176: 577 - 588.

[7] 宫秀军, 刘少辉, 史忠植. 一种增量贝叶斯分类模型[J]. 计算机学报, 2002, 25(6): 645 - 650.

(上接第 171 页)

该系统针对不同的领域配以不同的应用软件,可应用于远程网络数据库的访问权限及身份的确认、银行储蓄防冒领及通存通兑的加密方法、保险行业中投保人的身份确认、期货证券提款人的身份确认、医疗卫生系统中医疗保险人的身份确认等领域。可以说,指纹识别技术实现了身份鉴定领域的世纪革命,解决了困扰身份识别多年的问题。

4 结束语

随着硬件技术的提高和互联网的广泛应用,指纹身份认证系统的开发和应用将得到进一步的拓宽,指纹身份认证的普及应用指日可待。

参考文献:

[1] 戴平阳. 指纹识别技术研究进展[J]. 厦门大学学报: 自然科学版, 2002, 41(6): 750 - 755.

[2] 卢朝阳, 张岗山, 刘 琳. 指纹识别系统性能评价方法[J]. 西安电子科技大学学报: 自然科学版, 2002, 29(6): 804 - 808.

[3] 于秀霞. 指纹识别技术及其应用[J]. 长春大学学报, 2005, 15(2): 30 - 32.

[4] 李海雄, 刘国清. 活体指纹识别系统及其应用[J]. 计算技术与自动化, 2003, 22(4): 68 - 70.

[5] 刘 旭, 田 捷. 自动指纹识别算法在嵌入式系统上的实现[J]. 计算机工程与应用, 2002(21): 120 - 124.

(上接第 173 页)

(5)分组长度太大,为保证安全性, n 至少也要 600 bits 以上,使运算代价很高,尤其是速度较慢,较对称密码算法慢几个数量级;且随着大数分解技术的发展,这个长度还在增加,不利于数据格式的标准化[4]。

5 结 论

主要对公钥密码 RSA 算法的安全性、攻击方法进行了探讨和分析,并对 RSA 的发展前景进行了简单介绍。在公开的密钥加密算法中,RSA 已经作为标准几乎在各种信息安全需求中给出很好的解决方案,其最大的优点是密钥空间大,缺点是长密钥带来巨大的计算量,导致加密速度慢。随着解密方法的进步和计算硬件技术的不断发展,RSA 算法应用显得越来越笨拙。RSA 加密算法是目前应用最广泛的公钥加密算法,特别适用于通过 Internet 传送数据[5]。不管怎样,RSA 算法还是会在将来很长一段时间继续成为公开密钥加密算法的主流。

参考文献:

[1] 朱文余, 孙 琦. 计算机密码应用基础[M]. 北京: 科学出版社, 2003.

[2] Stinson D R. 密码学原理与实际[M]. 冯登国译. 北京: 电子工业出版社, 2003.

[3] Menezes A J, van Oorschot P C. 应用密码学手册[M]. 胡磊等译. 北京: 电子工业出版社, 2005.

[4] 周玉洁, 冯登国. 公开密钥密码算法及其快速实现[M]. 北京: 国防工业出版社, 2002.

[5] Spillman R. 经典密码学与现代密码学[M]. 叶阮健等译. 北京: 清华大学出版社, 2004.