一种高安全性生物智能卡及应用系统①

A High Security Biometric Smart Card and application system

李 超 辛 阳 杨义先 钮心忻
(北京邮电大学信息安全中心 北京 100876)
(北京邮电大学网络与交换技术国家重点实验室 北京 100876)

摘要:智能卡作为一种存储数据的可移动媒质广泛应用于许多系统,例如电子商务和移动商务等。智能卡中的数据是通过用户的个人身份识别码(PIN)来保护的。但是,PIN 作为一种口令存在着许多缺点,例如,它可能会被遗忘或者被盗窃,并且被破译。本文提出一种应用生物特征认证取代 PIN 认证的高可靠性的智能卡,以加强智能卡的安全性。整个数据处理过程和生物认证过程都是在智能卡中进行的,不会造成私密数据的泄漏。本文还设计了一套生物智能卡的应用系统模型。

关键词:智能卡 生物认证 生物证书

1 引言

传统的利用智能卡进行个人身份认证中,智能卡的合法性和有效性是通过基于公钥基础设施(PKI)的认证来确认的[1]。在 CHV_Key(卡持有者认证密钥,是同用户 PIN 密切相关的私钥)得到恰当的管理的情况下,这种电子认证的安全性是有保证的。但 PIN 码作为一种口令,可能很容易地被猜测出或通过字典攻击进行破解[2]。简单的口令很容易被破解从而影响到安全性,而复杂的却又难以记住。而且,口令无法进行唯一性确认,即当口令跟别人共享时,很难确定谁才是真正用户。

由于上述 PIN 的这些局限,利用生物认证[3]来管理 CHV_Key 相对 PIN 有很多安全和应用上的优点。生物认证是指通过个人的生理特征或行为模式如指纹、脸形、虹膜、声音等进行身份认证。这些生物特征不可能被丢失或遗忘,也很难被复制、共享和散布,并且它要求认证者在认证现场。由于时间、成本、试验条件的限制,伪造这些生物特征进而获取访问权限将很困难,与此同时,由于生物特征对于用户本身的唯一性,一旦用户通过生物特征进行的身份认证访问所需的数字内容,用户是无法否认自己曾经访问过该内容的。因此,生物认证是一种理想的候选方案来代替基于口令的认证方案,它能提供完善的认证机制来保护智能卡里的数据。

2 智能卡

Java 智能卡(Java 卡),能够运行利用 Sun Microsystems Java 程序语言编写的应用程序[4][5]。Java 卡技术使 Java 技术可在存储空间受限的智能卡等设备上运行,它提供平台独立性、存储和动态更新多种应用的能力,并与现行的智能卡标准兼容。Java 卡基于熟悉指令集的通用 32 位结构,其内存系统由 RAM(随机存储器),ROM(只读存储器)和 EEROM(电子擦除编程 ROM)。RAM 速度快,作为程序运行时的临时缓存。系统程序保存在 ROM 上,不能修改和升级。而应用程序则同卡的操作系统分离,保存在 EEROM 中,能够随时更新。

Java 卡运行环境(JCRE)结构见图 1。图 1 中,每个应用是一种应用服务如电子钱包、身份认证等。

3 生物识别技术

有一些生物特性识别(如指纹识别、人脸识别、虹膜识别、声音识别等等)已经在各种不同的应用使用了。每种生物识别方式都有其优缺点,没有哪种方式能够有效地符合各种应用的所有需求(举例来说,准确性、实用性、费用)。指纹识别是生物识别学中有效

① 国家自然科学基金(No. 90204017, 60372094)

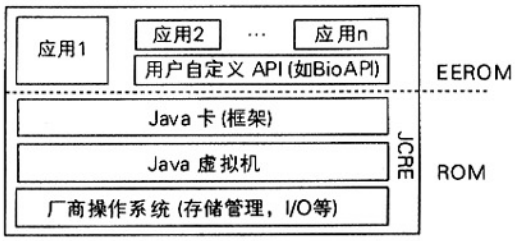

图 1　Java 卡的基本架构

性和可行性方面比较成熟的一种生物认证方法，尤其适合在智能卡应用中认证用户。综合各种因素的影响，生物智能卡原型的开发选择指纹识别作为卡内识别方式。下面简要的介绍在生物识别系统中具有是代表性指纹识别的完整过程，见图 2。

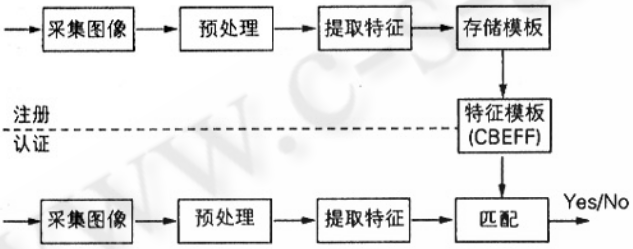

图 2　指纹识别过程

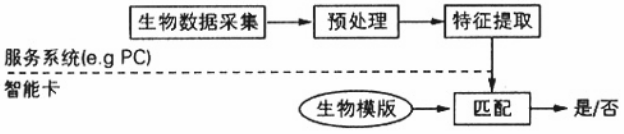

图 3　生物智能卡的工作流程

在注册步骤中，首先，采集注册用户的指纹图像，然后对其进行预处理，然后提取指纹特征，最后这些指纹特征按照模版标准化为通用生物识别交换文件格式（CBEFF）或其他类型的格式[6]，并作为注册用户的生物模版储存。特征是包含位置、方向、类型等的指纹的唯一特征。[7][8]指纹的匹配是通过比对特征和特征模版来实现的。

在认证步骤中，获得验证者的指纹特征过程和注册步骤是一样。最后，指纹验证器比较输入的特征和注册的特征模板之间的相似度。为了纠正在指纹图像获取和传输中发生的图像失真，在提取指纹特征之前必须对图像进行预处理。提取特征实际上就是找出指纹特征的过程。通过比对验证者的指纹特征与注册过的指纹特征来核实验证者的身份。然而，在特征的提取过程中可能会产生错误的特征或者伪特征，而丢失正确的特征，这会影响到指纹比对结果。因此注册时，我们建议使用多个指纹图像生成一个特征模版，这样能有效率地抛弃错误的特征而且弥补一些被丢失的特征。

4　生物智能卡设计

为了实现生物特征认证和智能卡的结合，智能卡必须有开放的操作系统，比如 Java 卡。本文提出了一种生物智能卡设计原型，使用拥有 32 位处理器的 Java 卡实现生物认证。整个生物认证是通过发行者自定义的 APIs（如图 1 所示的 BioAPI）实现的。智能卡的其它应用，比如应用 2・・・应用 n 等也基于 BioAPI 开发的。智能卡的工作流程如图 3 所示。

在设计原型中，采用 FipSecTM 算法作为卡内指纹比对算法，是由 FhG－SIT 提出的卡内上基于特征匹配的识别算法。该算法需要两位小数的数值，只有浮点数才能支持这种精确度。Java 卡的处理器并不支持浮点运算，成为生物智能卡实现的主要障碍。为了解决该问题，Y. S. Moon 等定义了一套非整数计算的 API，用于指纹图像的处理的计算。本原型设计中采用了其定义的计算 API，解决卡内处理器的计算能力所造成的问题。

为了增强智能卡的安全性，智能卡中存储的生物特征模板数据必须防止被篡改或者破坏。数字签名是一种有效的用于保证数据完整性的手段。X. 509 公钥证书是 ISO/IEC/ITU 定义的一种用数字签名保护用户公钥的一种典型的数字证书。

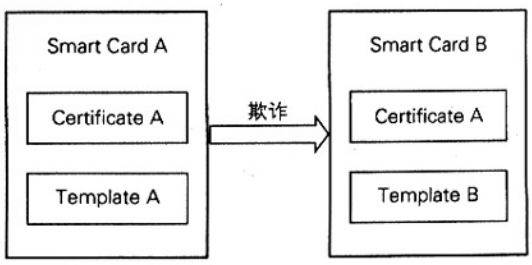

图 4 一种通过攻击智能卡进行身份欺诈的方法

本设计原型中，智能卡中保存了用户的 X. 509 公钥证书、经过数字签名的生物特征模板和用户的私钥。生物模板与公钥证书之间的对应关系（比如用户

ID 和模板的对应关系)的安全性并没有保证。因此必须考虑伪造证书或生物模板和破坏智能卡所带来的威胁。例如,如果卡 A 中的模板(即模板 A)被黑客用模板 B 替换,那么,B 就能使用卡 A 并假冒 A 使用其私钥,如图 4 所示。模板和用户 ID 数据必须同时被数字签名,以其保证与公钥证书之间的对应关系,从而防止通过篡改智能卡来假冒。为了验证模板的发行者的合法性和智能卡中验证模板的合法性,Yoshiaki Isobe 提出了通过 X.509 证书验证生物特征模板的方法,创建了一种新的经过数字签名的生物模板——生物证书。但是 Yoshiaki Isobe 提出的生物证书有许多缺点,如没有证书的有效期和主体等,这对于数字证书来说是不合理的。经过改进的生物证书模板结构如图 5 所示。在 X.509 证书中,证书信息包括版本、序列号、发行者名称和有效性等。生物证书中,版本是指证书的版本号;证书序列号用于区分不同的证书;主体身份直接与生物模板数据相关联;有效性是指证书有效的时间期限。X.509 证书身份信息是指 PKI 公钥证书的身份信息如 X.509 证书发行者姓名和序列号等。发行者及其唯一标识指生物证书发行者名称及其身份信息。模板数据是用户的生物特征模板,在该原型中标准化为通用生物识别交换文件格式(CBEFF)。

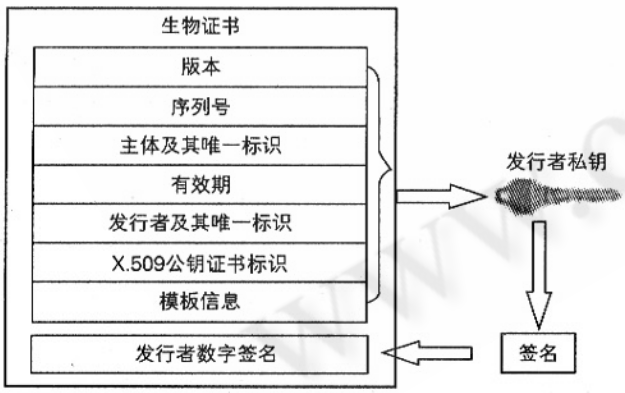

图 5 生物证书的结构

5 智能卡应用系统

首先用户需要在系统注册机构 CA 进行注册:注册时 CA 为用户生成一对公私钥并颁发一个 X.509 公钥证书。然后采集用户指纹并产生一个指纹模板,并按照图 5 所示的生物证书格式为用户产生一个生物证书。最后将用户公钥证书、生物证书和私钥集成在智能卡中并颁发给用户。

在用户使用生物智能卡进行身份认证阶段:用户通过指纹采集仪输入指纹,然后将指纹直接传入生物智能卡中,在智能卡内将输入的指纹和生物证书中模板进行比对,以进行身份认证。如果生物认证通过,智能卡则允许读卡内私钥,进行相关操作。在进行指纹比对前,需要对生物模板进行合法性检查,其验证方法和验证 PKI 公钥证书方法一致。

本文还设计并实现了一种生物智能卡认证应用系统模型,图 6 所示。在使用系统服务的时候,服务端产生一个随机数发送给客户端;客户端采集用户指纹,在并生物智能卡内比对成功后释放出用户私钥,利用私钥对随机数的哈希值进行签名并发送给服务端;在服务端使用用户公钥验证经过用户签名的随机数哈希值,以确定用户是否为合法用户。

分析以上生物智能卡网络认证系统,不难发现用户通过输入指纹后,在卡内实现身份认证,认证通过后才能释放用户私钥,从而保护了用户私钥的安全。同时,服务端和客户端进行随机数的挑战应答验证了用户是否为合法用户。

与原来使用普通智能卡存放用户私钥的系统相比,该系统的优点显而易见:用户无需记卡的 PIN 码,用户私钥只有经过生物认证后才能释放,而且非法用户无法篡改用户模板和私钥,用户私钥保护的更加安全。系统通过挑战应答方式进一步确认用户身份,多层次保护了系统的安全。该系统唯一的缺点就是目前生物智能卡系统实现比较复杂,成本较高。

基于生物智能卡认证应用系统模型,我们开发了一套生物智能卡应用系统。该系统主要包括用户注册终端、智能卡发行机构、证书发行机构、用户客户端和服务端等六部分。各部分具体功能流程参考图 7 所示。

6 结论

本文提出了一种新的在智能卡实现生物认证的生物智能卡体系结构和生物智能卡应用系统,还提出一种保护卡内生物模板信息的生物证书模板,并基于该结构开发出了生物认证 Java 卡系统原型和应用系

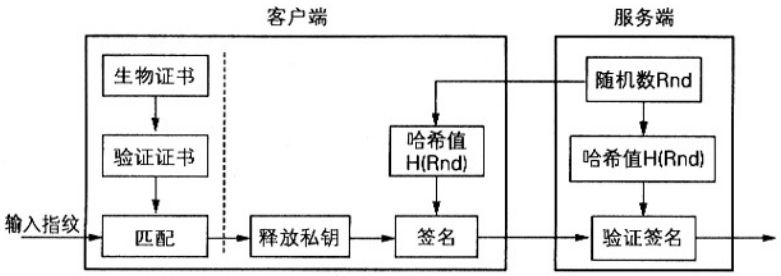

图 6　一种生物智能卡认证应用系统模型

统模型。整个生物认证程序都在智能卡内部运行，防止了隐私数据泄漏出智能卡，因此生物智能卡具有很高的安全性和鲁棒性。不过由于生物识别算法比较复杂，智能卡的计算能力有限，生物智能卡的设计和实现还有待于进一步的深入研究。

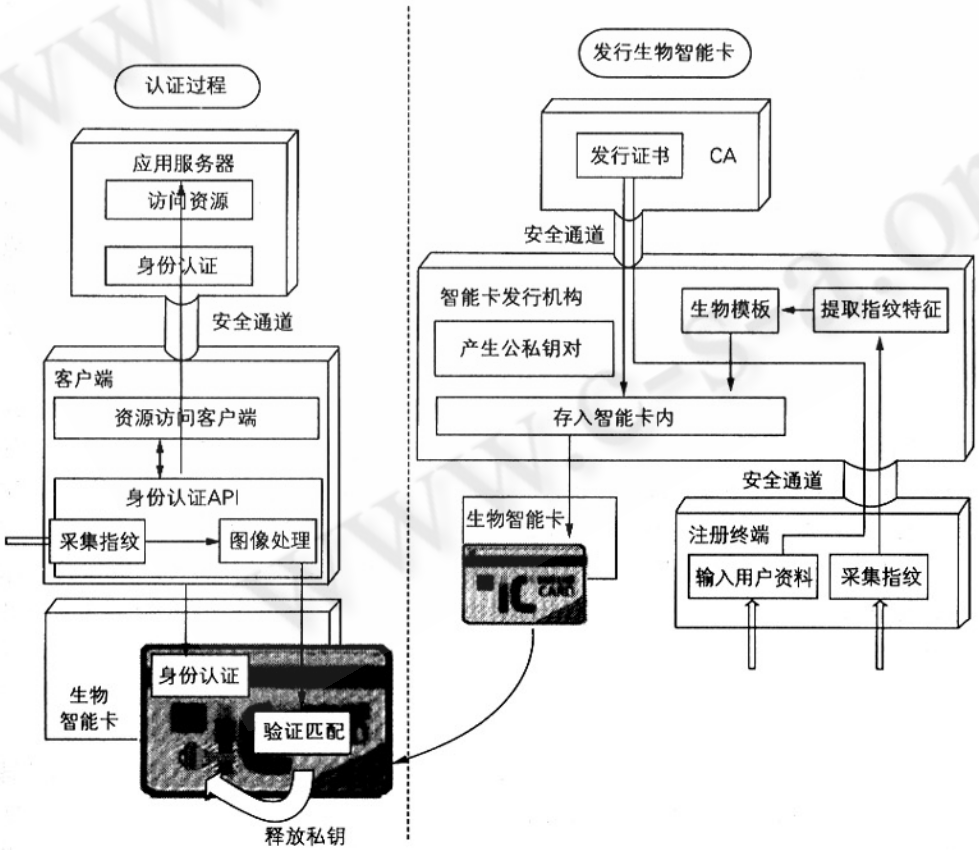

图 7　基于生物智能卡的生物认证应用系统

参考文献

1 W. Ford, M. S. Baum: Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption. Prentice – Hall, Inc (1997).

2 D. V. Klein: Foiling the Cracker: A Survey of, and Improvements to, Password Security. in Proc. 2nd USENIX Workshop Security (1990) 5 – 14.

3 A. K. Jain, R. Bolle, S. Pankanti, eds: Biometrics: Personal Identification in Networked Society. Norwell, MA: Kluwer (1999).

4 Sun Microsystems, Inc, http://java. sun. com/product/javacard.

5 Veridicom, http://www.veridicom.com.

6 F. Podio, J. Dunn, eds: Common Biometric Exchange File Format (CBEFF), NISTIR 6529 (2000).

7 D. Maio, D. Maltoni, S. Rizzi: An Efficient Approach to On – line Fingerprint Verification. Proceedings VIII Int. Symp. on Artijicial Intelligence, Mexico, (1995).

8 D. Maio, D. Maltoni: Direct Gray – Scale MinutiaeDetection in Fingerprints. IEEE Transactions on Pattern Analysis Machine Intelligence, V. 19, No. 1, (1997) 25 – 29.