2018 年全国大学生信息安全竞赛

作品简介

作品名称：基于指纹、指静脉的活体身份认证的复杂口令管理系统

电子邮箱：elaine.whw@gmail.com

提交日期：2018年6月4日

基于指纹、指静脉的活体身份认证的复杂口令管理系统

摘要：随着云存储、大数据等新兴互联网技术的不断发展，人们的安全意识和隐私保护意识的不断提高，信息安全越来越为信息化建设中急需解决的重大技术问题。其中，密码学是保障信息安全的核心和基础。然而，在传统密码学中的密钥使用与管理过程中，存在密钥长度、复杂度与用户记忆的矛盾、人机接口隐患这些难以调和的缺陷。因此需要一种复杂口令管理系统，在实现电子身份与物理身份紧密绑定的同时，帮助用户管理复杂口令。本作品设计开发了一种基于指纹、指静脉的活体身份认证的复杂口令管理系统，用户仅需提供其生物特征与简单密钥就可以方便、安全地管理诸多复杂长密钥。本系统引入生物特征密码技术，将生物特征与传统密码学相结合，利用生物特征的独特性、不易伪造、无需记忆等优势，有效弥补了上述传统密码学的缺陷。本系统的创新性工作包括：（1）使用指纹与指静脉双生物特征识别技术验证用户身份，具有活体识别的特性，不易伪造；（2）使用简单口令加密生物特征点，抵御多数据库比对攻击；（3）使用模糊金库增加存储数据的安全性；（4）使用国产SM系列密码算法。

一、选题背景

随着互联网的大面积普及和数字化进程的不断推进，信息安全越来越成为信息化建设中急需解决的重大技术问题，它与国家安全、社会安全、经济安全等均紧密相关。而信息安全的核心与基础——密码技术，应如何改进以适应更严格的安全要求，是目前一个急需解决的重要问题。目前，在基于传统密码学的密钥保护和管理方面存在以下缺陷：

第一，密钥的长度、复杂度与用户记忆能力的矛盾。一般来讲，密钥长度越长、生成越随机，安全性越高。但随之，用户对随机复杂长密钥的记忆难度也大大提高，这无疑增加了密钥管理的困难程度。

第二，人机接口隐患。基于传统密码学的身份认证系统完全依赖于与密码系统匹配的密钥，并且无法保障密钥使用者的数字身份与物理身份的统一，一旦密钥被窃或丢失，作为安全保障的密码系统也将随之失效。

而生物特征的独特性、不易伪造、无需记忆等优势，使得它的引入有望解决以上问题。生物特征密码技术是一种将生物特征与密码学相结合的技术，它解决了生物特征的模糊性与密码学的精确性之间的矛盾，使生物特征可参与到密钥的

保护或生成中，在解决传统密钥易遗忘、与用户存在人机接口隐患问题的同时，可以一定程度上保护生物特征模板。

基于指纹、指静脉的活体身份认证的复杂口令管理系统正是为了解决传统密码学中密钥保护与管理的两个安全问题提出的。针对第一个安全问题，本系统对用户提供的生物特征采用模糊金库(Fuzzy Vault)算法，将用户的复杂长密钥作为模糊金库的多项式系数进行安全存储，当用户需要时可以利用指纹、指静脉特征以及简单口令将其恢复；针对第二个安全问题，本系统应用指纹、指静脉双生物特征相结合，实现活体识别的同时将用户的物理身份与电子身份严格绑定。

二、作品设计与实现

本系统的整体架构如图1所示。在用户需要调出复杂秘密信息时，提供指纹指静脉图像，系统经过图像处理模块提取特征点信息，并与模糊金库中的点集进行比对。系统利用拉格朗日插值法和纠错码恢复秘密信息，只有用户的生物特征与注册时提供的生物特征足够相似才能恢复出正确的复杂秘密信息。之后，通过加密模块对秘密信息进行加密。接着，由数据传输模块将加密后的长口令从服务器端发送到客户端。客户端接受到密文信息后，通过解密模块对密文进行解密，并呈现给用户。至此，各个模块分工明确，协同合作完成了口令安全管理的流程。

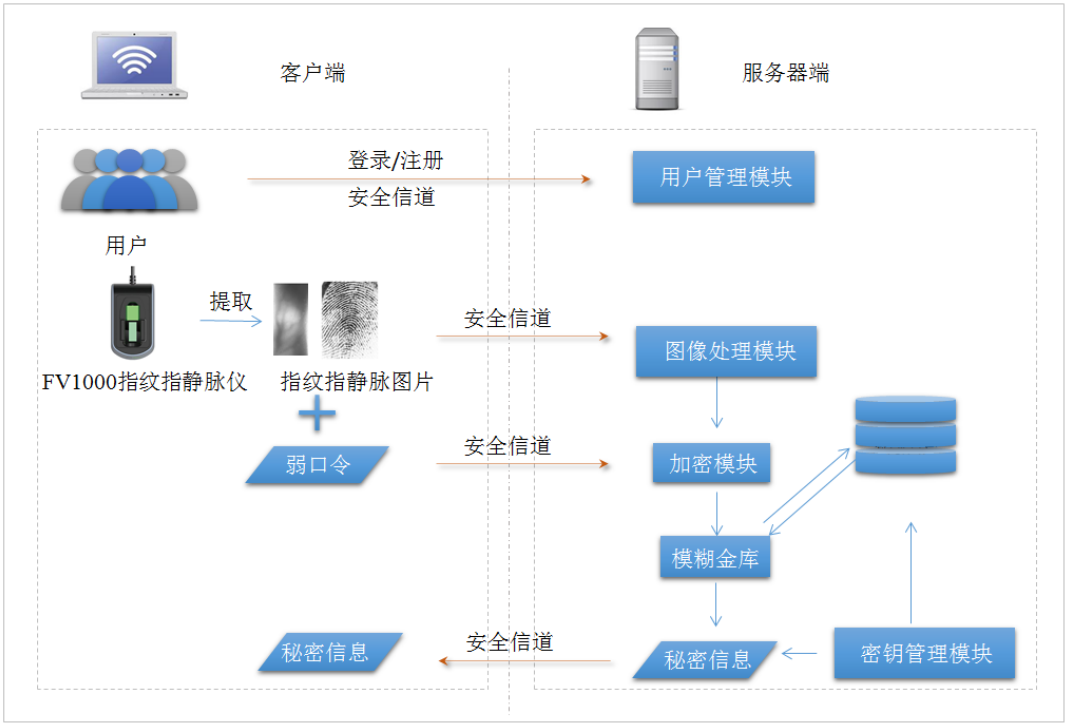


图 1　总体架构图

具体实现过程分为以下几个阶段：

1. 硬件选择。由于我们需要同时采集指纹与指静脉，经过研究比较，我们选择了中控智慧公司研发的 FV1000 指纹指静脉采集仪，开发平台选择了 1 台基于 Windows 操作系统的笔记本电脑。

2. 完成对硬件的系统控制。我们通过 Python 实现对采集的指纹图像与指静脉图像的提取，并作为本系统运行时的输入。

3. 完成指纹、指静脉图像预处理，并提取、筛选特征点。对于采集仪采集到的初始指纹、指静脉图像，经图像归一化、图像分割、图像增强、二值化、细化等预处理操作后得到特征点，并去除不稳定的伪特征点。

4. 模糊金库算法实现。注册阶段，将用户需要管理的复杂口令信息拆分后作为模糊金库加密算法中的多项式系数进行运算；用户身份验证通过后的解密阶段，用拉格朗日插值法恢复出多项式系数，并用 CRC 纠错码消除生物特征的模糊性带来的误差，最后还原出用户原始的复杂口令信息。

5. 采集足够多的指纹、指静脉图像作为测试用例。我们总共采集了 50 人的共计 400 根手指的指纹、指静脉图像，每根手指采集 10 次，最终得到初始图像 4000 组。

6. 客户端应用开发。我们选用 HTML 编写客户端界面。

7. 性能测试。在此阶段，我们先后在客户端进行了用户登入系统、注册、添加复杂秘密信息、删除复杂秘密信息、恢复复杂秘密信息、修改复杂秘密信息这几个功能的测试。经过测试，本系统的以上功能全部能够正常运行。

本系统作为一个基于双生物特征活体身份认证的复杂口令管理系统，能够实现对用户身份的活体认证，并通过模糊金库算法对用户的复杂口令信息进行保护，与此同时本系统能够保证全过程的数据传输安全性以及存储安全性。在简化用户复杂口令记忆的同时极大提高了口令管理系统的安全性和可靠性。

三、测试与分析

3.1 环境搭建

测试环境主要分为服务器端部分和客户端部分。服务器端部分需要搭建python服务器，完成python matlab模块装载。客户端部分需要打开浏览器输入服务器IP和端口，安装FV1000指纹指静脉仪设备驱动，并正确安装指纹指静脉采集

程序。实物测试环境如图2所示。

图 2　实物测试图

3.2　功能测试

用户第一次使用该系统时，需要创建账号,创建账号时需要输入用户名和密码，用户名不能与已有用户名重复。再次确认密码后，即可成功注册进入系统。之后，用户只要正确输入账号和密码，点击登录即可进入功能界面。功能界面如图3所示：

图 3　功能界面

我们分别对添加秘密信息、删除秘密信息、恢复秘密信息、修改秘密信息、查看操作日志等功能进行了测试，均可正常运行。

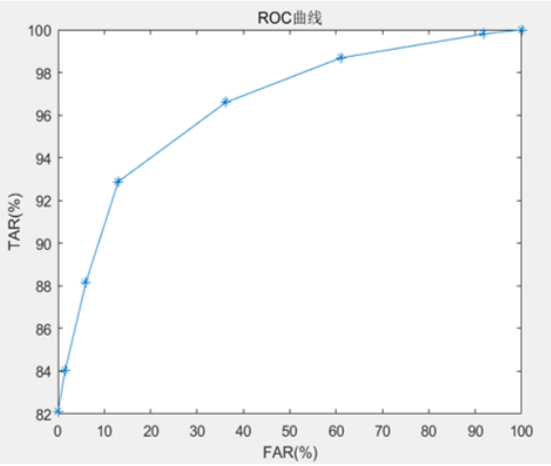
3.3 性能测试

对于每根手指，随机选取 5 张图像进行系统注册，并从剩余的图像数据集中，

构造 5000 对正样本样例，5000 对负样本样例，用于测试我们系统的识别性能。由于指纹指静脉采集过程中手指位置的偏差、光线明暗等因素的影响，同一手指每次采集到的特征点位置可能会产生一定的偏移。在模糊金库解密过程中，我们定义了一个阈值 m，若输入的点(x,y)与模糊金库中的点(x_0,y_0)的直线距离不大于 m，则判定该点匹配。设置合理的阈值可以提高识别精度，为此我们分别设置模糊金库判断阈值为 4，12，20，28，36，44，52，60 进行测试。测试结果如图 4(a)所示，我们根据以上结果计算 TAR 与 FAR，并绘制 ROC 曲线如图 4(b)所示:

Threshold:4			Threshold:12		
	TRUE	FALSE		TRUE	FALSE
Positive	4105	895	Positive	4202	798
Negative	0	5000	Negative	78	4922
Threshold:20			**Threshold:28**		
	TRUE	FALSE		TRUE	FALSE
Positive	4409	591	Positive	4644	356
Negative	303	4697	Negative	651	4349
Threshold:36			**Threshold:44**		
	TRUE	FALSE		TRUE	FALSE
Positive	4830	170	Positive	4934	66
Negative	1813	3187	Negative	3050	1950
Threshold:52			**Threshold:60**		
	TRUE	FALSE		TRUE	FALSE
Positive	4990	10	Positive	5000	0
Negative	4588	412	Negative	5000	0

(a)模糊金库不同阈值性能测试图



(b) ROC曲线图

图 4 模糊金库性能测试图

经计算，系统 EER 为：9.498%。当阈值设置小于 4 时，系统误识率为 0,正确识别正样本的概率达到了 82%。

四、创新点总结

本系统基于指纹与指静脉双生物特征身份认证与模糊金库技术，实现了复杂口令的生成、相关信息的安全存储、复杂口令的定时更新与友好的用户界面，这都保证了用户复杂口令的安全性和复杂口令管理过程的简易性。作品主要创新性如下。

1. 使用指纹与指静脉双生物特征识别技术验证用户身份。指纹特征识别的发展研究已经相对成熟，但由于其简单性存在被人窃取与伪造指纹的风险。于是我们结合指纹与指静脉实现双生物特征的认证识别，增加了系统的安全性。指静脉作为新兴的生物特征识别技术具有活体识别、高安全性、非接触性三大特点，指静脉不易伪造，采集设备安全卫生，易于被用户接受。

2. 使用简单口令加密生物特征点。在利用用户的生物特征点进行计算之前，首先用简单口令对其进行加密。这就避免了攻击者同时获得多个模糊金库后采用对比攻击的风险。由于简单口令不同，自然加密后的用户特征点就不同，攻击者的比对方案不能奏效。

3. 使用模糊金库增加存储数据的安全性。数据库中不会直接存储与用户生物特征有关的信息，这样就防止了黑客利用攻击数据库来伪造生物特征信息；数据库也不会存放明文或密文形式的用户复杂口令，解决黑客利用灌库攻击破解用户复杂口令的隐患。

4. 使用国产密码算法。由于信息安全是国家安全的关键环节，为确保密码算法的自主可控，降低敏感信息泄露和信息系统遭受攻击的风险，我们在系统中大量应用国产密码算法，例如 SM3 杂凑算法、SM4 分组密码算法等。国产密码算法的使用对于国家安全有着重要的意义，也为我们设备的商业化打下基础。

五、未来工作

目前，基于指纹、指静脉的活体身份认证的复杂口令管理系统能够通过客户端连接的指纹指静脉采集仪获取用户的手指指纹、静脉信息，并将相关数据通过安全信道传输到服务端，实现了复杂口令管理的功能，且其性能表现良好。未来工作会在以下几个方向中继续发展：

1. 结合基于生物特征的密钥生成算法，得到安全性更高的复杂密钥。本系统作为复杂口令管理系统，默认用户已有复杂长密钥，否则为其随机生成复杂长密钥，并进行之后的生物特征密钥绑定。随机生成复杂密钥过程的安全性仍有待提高，未来可以考虑结合模糊提取等生物特征密钥生成算法，借由用户的固有生物特征来生成复杂密钥信息。

2. 寻求嵌入性更好的指纹指静脉采集设备。本系统所采用的采集设备体积较大，对移动电子设备的嵌入性较弱。未来我们将寻求体积更小、性能更优的采集设备，以便将系统拓展到移动终端。

3. 与一些具体的登录系统相结合，实现身份认证过程的自动化。目前，本系统在用户复杂密钥恢复成功后将其通过安全信道发送回客户端，由用户自行输入到登录系统中。未来可以与具体的登陆系统相结合，无需用户手动输入，即可由本系统自动实现身份认证。