学校编码：10384　　分类号_____密级_____
学　　号：23020101153046　　UDC_____

厦门大学

硕士学位论文

指纹的匹配算法及集成方案的研究

Research of Fingerprint Matching Algorithm and Integrated Scheme

郑智强

指导教师姓名：郑建德　教授
专业名称：计算机软件与理论
论文提交日期：2013 年 5 月
论文答辩日期：2013 年　月
学位授予日期：2013 年　月

答辩委员会主席：_____
评　阅　人：_____

2013 年　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人(签名)：郭翔强

2013年05月31日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1。经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2。不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人(签名)：郑翔强

2013年05月31日

摘 要

随着国家信息化建设的推进与发展，信息安全成为信息化平台与信息系统必须要考虑与面对的问题。用户在享用信息化带来的工作效率提升的同时，伴随着个人信息被盗用，个人隐私被的风险。这些风险多数源自于身份认证过程中存在安全漏洞。现代数字身份认证手段存在着易复制、被盗取等诸多问题。目前，数字身份认证技术所面临的问题的最佳解决方案是采用生物特征的身份认证技术；而指纹作为最古老的的生物特征之一，具有易采集、难伪造、普遍性的优点，被广泛应用于现代身份认证当中。对指纹的匹配算法，研究人员已经作了大量的工作；但是，指纹识别算法的识别速度和识别率一直难以共存。另外，传统的生物认证技术存在生物模板泄露等危险，如何安全有效地使用指纹识别技术是当下研究的一个热点。

厦门大学信息安全实验室对身份认证技术和指纹识别技术做了大量的研究，先后提出了手机令牌认证技术与基于矢量三角形的匹配算法。本文在前人研究的基础之上，继续对指纹匹配算法与认证技术进行研究，将二者结合在一起，构建一种安全的指纹识别技术与令牌认证技术的集成方案。本文的主要工作有如下三点：

1. 本文论述了当前基于指纹的识别技术现状，并对比了各种识别算法的优缺点。由于指纹特征点的特殊性，标准遗传算法存在容易早熟等问题。本文在前人的研究基础之上提出了一种基于自适应收敛遗传算法的快速指纹匹配算法，通过实验证实了该算法在时间与识别率上都有所提高。

2. 本文研究了指纹匹配算法与传统认证的集成，论述了当前指纹用于身份认证的不同方案。本文在手机令牌认证技术的基础之上提出了一种安全的集成方案，方案中使用手机令牌技术解锁指纹识别认证。

3. 本文介绍了 Windows 7 系统的安全机制并研究了 Windows 7 系统的登录认证机制。本文将指纹认证与令牌认证的集成方案向下兼容地应用在 Windows 7 系统的登入认证当中，加强了 Windows 7 系统身份认证的安全性。

关键词：指纹匹配算法；令牌认证技术；多因素认证

Abstract

With the promotion and development of national information construction, information security has become an assignable problem in information platform and information systems, which should be handled. Users enjoy the efficiency of the information technology. But the mistake of authentication may lead to privacy breaches, identity theft and fraud. The traditional digital authentication is weak for the easiness to copy and reuse. With the development of biometric technology, it is considered to be one of the best solutions for the problems faced by the traditional identity authentication technology. Fingerprint is one of the oldest bio-feature. It is easy to collect, difficult to counterfeit and almost people have one. It is widely used for the modern identity authentication. Currently there are a lot of researches on fingerprint recognition algorithm. However, the recognition speed and the recognition rate are difficult to co-exist. In addition, the traditional biometric authentication technology has the problem of leaking biometric feature template which is hard to rebuild. How to using fingerprint recognition technology safe and effectively is a hot point this moment.

Information Security Lab of Xiamen University has made a lot of research on authentication technology and fingerprint recognition technology. This article continues to study fingerprint recognition technology and mobile token authentication technology, and the cooperation of the two makes a secure framework to use fingerprint recognition technology. The main contributions of the thesis are summarized as below:

This paper discusses the current status of identification technology based on fingerprint, and compares the advantages and disadvantages of various recognition algorithm. Because of the nature of the fingerprint minutia, standard genetic algorithm based recognition algorithm has problems such as premature. The thesis proposes a fast fingerprint recognition algorithm based on adaptive convergence of genetic algorithm based on the previous study, the experiments show that the algorithm can improve the time and performance.

This paper studies the integration of fingerprint recognition algorithm with traditional authentication, comparing biometric crypto technology with traditional

solutions. This paper proposes a secure way to using fingerprint based on the mobile token authentication technology, which uses mobile token technology to unlock fingerprint certification.

At last, this thesis describes the system's security mechanisms in Windows 7 and Windows 7 system login authentication mechanism. And we use the integrated to program a new authentication method for Windows 7 system login, which strengthen the security of the Windows 7 system authentication.

Keywords: fingerprint matching algorithm; token authentication technology; multi-factor authentication

目录

Contents

第一章 绪论

1.1 研究背景和意义

数字身份认证中，用户的身份信息是用一组特定的数据来表示，计算机识别用户的数字身份，进而对用户身份认证与授权。信息系统在认证用户成功之后，根据用户权限设置，赋予用户相应的权限进行系统资源的访问与使用。有效和安全的身份认证技术是信息安全保障的关键。目前常用的单因素认证有如下三种：

1. 基于知识的认证

系统通过提供固定的问题的方式索取用户所知的身份信息。1981 年，Lamport 提出了基于用户名与密码的远程登入协议[1] 。这个远程协议中，用户认证时将输入用户名与密码作为身份凭证，服务器端查询存储在服务器的用户名与密码进行比对，进而确认用户是否合法。方案的优点是实现难度较小，且成本较低。在目前的网络应用中，这一类型的认证技术被广泛的使用。这一类型的认证技术最主要的问题在于安全性较低，容易遭受猜测或者字典攻击。人为记忆的用户名与密码熵值较低，因而攻击者可以进行猜测攻击，另外，用户容易忘记密码。Shimizu[2] 等人使用单向门陷函数对用户名与用户密码进行处理，存储用户密码的哈希值。

2. 基于令牌的认证

令牌是指用户所持有的，用来证明用户身份的物理硬件。用户通过令牌与待认证系统进行身份认证。这种认证的特点之一在于，系统只对用户的令牌认证而非用户本身，因此令牌认证属于对用户所有物的认证。通常地，令牌认证可以分为静态令牌认证与动态令牌认证。静态令牌认证中，系统通过获取用户令牌中的唯一标识码认证用户。常见的静态令牌如小区门禁系统中的开门钥匙。动态令牌认证则在认证的过程中交互的数据是变化的。在实现上，有一种是动态口令卡，如早期的网银卡中就使用这种技术——系统给出需要输入的口令卡中的数据的坐标，用户通过查询该坐标输入口令；还有一种动态令牌可以进行计算，这些令牌包括基于事件同步、基于时间同步以及挑战应答三种方式与信息系统进行交互

计算。这一类认证技术主要在于被盗用的风险较高。由于系统是对于物理硬件的认证，非法用户在盗用令牌之后就成为“合法用户”而随意对系统进行操作。

3. 基于生物特征的认证

数字身份认证技术大多数是以存储的数字信息作为认证的凭证，因此易于伪造和丢失。近年来，随着传感器的发展，计算机通过传感器可获得的数据越来越多，包括生物特征。生物特征识别技术就是利用人体固有的生理特性（如脸型、掌纹、虹膜）和行为特征（如声音、笔迹、步态）来进行个人身份的鉴定。这些生物特征具有如下的优点：首先，生物特征具有稳定性与唯一性；其次，相比于数字认证中的数字信处，生物特征具有便捷性，用户不需要携带额外的物件；再则，生物特征不易于被伪造，由于生物特征本身在结构方面比较复杂，攻击者很难去模仿复制，又与用户相随，因此，攻击者也不便去窃取。因此，基于生物特征的认证技术是数字身份认证不足的最佳解决方案。各国已经对生物认证技术的使用已经有了高度的重视；在英美等国的个人身份证明文件中已经嵌入了所有者的面部图像与可选的所有者指纹或者虹膜特征，共同倡导国际民用航空组织的提议。鉴于生物认证技术的广阔应用前景，Microsoft、IBM、NOVEL 等公司发起并成立了 BioAPI 联盟，制定生物特征识别应用程序接口工业标准。根据国际生物识别组织发布的 2009 至 2014 年的生物识别市场及产业发展预测调查报告[3]，未来几年内，全球市场产值总额将从 2009 年的 34.2 亿美元增长至 2014 年的 93.7 亿美元。

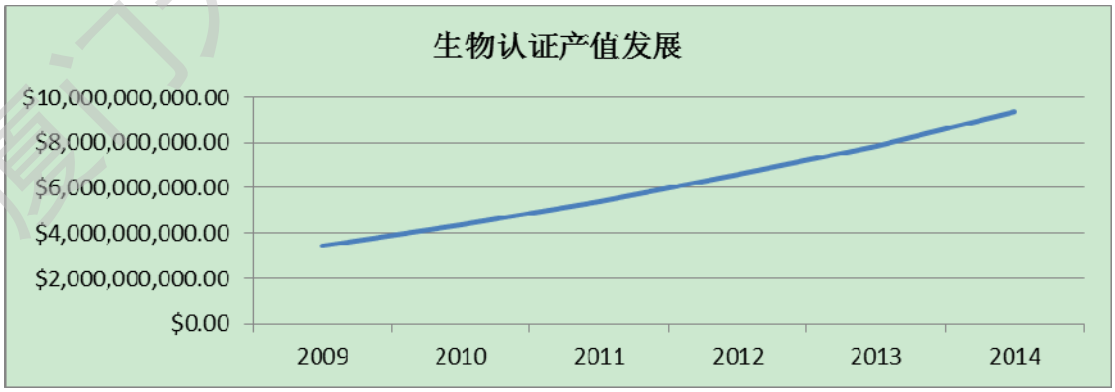

图 1.1 生物认证产值发展

指纹是最古老的生物特征之一。据记载，大约在 4000 多年前指纹的独特性