



(12) 发明专利

(10) 授权公告号 CN 113360874 B

(45) 授权公告日 2022. 10. 25

(21) 申请号 202110626432.3

G06K 7/10 (2006.01)

(22) 申请日 2021.06.04

G06V 40/13 (2022.01)

(65) 同一申请的已公布的文献号

G06V 10/764 (2022.01)

申请公布号 CN 113360874 A

G06K 9/62 (2022.01)

(43) 申请公布日 2021.09.07

审查员 雷韵

(73) 专利权人 湖南大学

地址 410083 湖南省长沙市岳麓区麓山南路28号

(72) 发明人 刘璇 彭宇伟

(74) 专利代理机构 长沙正奇专利事务所有限责任公司 43113

专利代理师 王娟 马强

(51) Int.Cl.

G06F 21/32 (2013.01)

G06F 21/34 (2013.01)

权利要求书1页 说明书9页 附图4页

(54) 发明名称

用户生物特征信息认证方法及系统

(57) 摘要

本发明公开了一种用户生物特征信息认证方法及系统,利用无源RFID标签数据进行用户验证的双因素认证系统,系统首先验证用户的密码,然后识别用户的生物特征进行认证。本发明提出的方法对密码的识别可以达到较高的准确率(平均达到96.9%以上)和用户验证准确率(平均92.8%以上)。



1. 一种用户生物特征信息认证方法,其特征在于,包括以下步骤:

S1、对采集的RFID相位数据进行预处理,获得连续的相位数据;

S2、根据相位数据中的相位值和时间信息对标签数据进行异常检测,提取出用户输入的密码信号的特征部分;

S3、对所述特征部分进行特征提取,获得单个密码信号的特征向量;

S4、利用所有密码信号的特征向量训练分类器,获得区分不同密码的分类器模型;利用注册用户的特征向量训练分类器,获得区分不同用户的分类器模型;所述注册用户的特征向量是指密码信号的特征向量的组合。

2. 根据权利要求1所述的生物特征信息认证方法,其特征在于,步骤S1的具体实现过程包括:

取标签的前N个数据作为起始窗口,得到起始窗口内标签数据的相位均值,计算起始窗口内的所有标签相位和相位均值的差值,若某个标签数据的相位值与窗口内的相位均值的差值大于 $(\pi-1)$ 且小于 $(\pi+1)$, 则判定该标签数据发生了倒 π 现象,将该相位值加上 π 并对 2π 取余;当该差值大于 $(\pi+1)$ 时,判定为发生了周期环绕现象,若标签相位值大于起始窗口内相位均值,则将标签相位值减去 2π ,反之,则加上 2π 。

3. 根据权利要求2所述的生物特征信息认证方法,其特征在于,步骤S1的具体实现过程还包括:

处理完起始窗口内的标签数据后,在其余待处理的标签数据前设置一个大小为n个标签数据的滑动窗口,将滑动窗口内的标签作为正常数据,计算滑动窗口内标签数据的相位均值,然后计算待处理标签数据的相位值和滑动窗口内标签数据相位均值的差值,若该待处理的标签数据点的相位值与窗口内的相位均值的差值大于 $(\pi-1)$ 且小于 $(\pi+1)$, 则判定该标签数据发生了倒 π 现象,将该相位值加上 π 并对 2π 取余;当该差值大于 $(\pi+1)$ 时,判定为发生了周期环绕现象,若标签相位值大于滑动窗口内相位均值,则将标签相位值减去 2π ,反之,则加上 2π 。

4. 根据权利要求1所述的生物特征信息认证方法,其特征在于,步骤S2的具体实现过程包括:

1) 设置一个固定大小的滑动窗口,定义所述滑动窗口内标签的平均振幅 $A_i(k)$ 和标签的相位值基准度量 $x_m(i)$;

2) 通过每个标签在滑动窗口内的平均振幅,计算得到所述滑动窗口内的标签振幅和G函数,对于第k个滑动窗口,若该第k个滑动窗口的G函数 $G(k)$ 大于阈值threshold,则该第k个滑动窗口为异常窗口;

3) 获取所有异常窗口的中间窗口,取中间窗口内的标签数据作为特征部分。

5. 根据权利要求4所述的生物特征信息认证方法,其特征在于,步骤S3的具体实现过程包括:获得特征窗口内M个标签的相位值,计算M个标签中两两标签间的相位差;所有相位差组成的向量即单个密码信号的特征向量;其中,所述特征窗口即中间窗口。

6. 根据权利要求1~5之一所述的生物特征信息认证方法,其特征在于,步骤S4中,利用随机森林算法训练分类器。

7. 一种生物特征信息认证系统,其特征在于,包括计算机设备;所述计算机设备被配置或编程为用于执行权利要求1~6之一所述方法的步骤。

用户生物特征信息认证方法及系统

技术领域

[0001] 本发明涉及模式识别领域,特别是一种用户生物特征信息认证方法及系统。

背景技术

[0002] 随着现代高新技术的发展,对人员管理的手段越来越丰富,安全问题越来越受到人们的关注。各行业及个人对安全、保密、隐私的需求愈发强烈,用户验证技术显得尤为重要。用户验证的目的是验证一个用户是否确实是注册在系统中的合法用户。它在许多应用程序中是一项至关重要的任务,例如对区域或事件的访问控制、电子支付等。

[0003] 身份鉴别的方法主要有三类:(1)信息,如口令或密码;(2)持有物,如各类证件或ID卡;(3)生理特征或行为特征,如指纹、手形、声音、虹膜等。

[0004] 第一,基于信息的方法旨在使用传统的加密算法执行身份验证,并使用加密技术保护标签免受非法访问[4-8]。这种方法大多需要修改商用通信协议或标签硬件,难以应用于轻量级无源标签。无源设备有限的计算能力限制了诸如散列和加密等加密算法的执行。事实上,商用现货(COTS)无源RFID标签不支持强加密操作,目前的UHF标签没有加密能力。

[0005] 第二,基于持有物的方法是利用反映在反向散射信号中的标签的电路特性差异来识别和验证标签。一种基于物理层信号的读写器认证解决方案,即仲裁器(Arbitrator)[9],可以有效地防止对标签的非法访问。Han等人提出了一种新的基于内部相似性的物理层识别系统GenePrint[10]。Yang使用额外的相位偏移作为一种新的指纹,称为Tagprint[11],用于识别一对读写器和标签。Chen等人提出了一种名为Eingerprint的新型指纹[12],EingerPrint使用存储在标签电路中的电能作为指纹,用于商品RFID系统中的无源标签认证。Wang等人提出了一种验证方法Hu-Fu[13],作者观察到两个相邻标签之间的电感耦合现象[14,15],当两个标签放在一起并产生耦合效应时,就可以达到验证的目的。

[0006] 第三,前两种传统方法是对用户的间接验证,这些解决方案的目标是验证设备本身(即标签),其本质特征导致其存在不可避免的缺陷,加密算法可能被攻击或标签可能被攻击者窃取,系统的安全性无法得到保证。近年来,主流的用户身份验证方法都是基于不同的生物特征或行为特征(如指纹、人脸、声音等)进行身份识别。与传统认证技术相比,生物特征认证技术(尤其是指纹认证)因其普适性、唯一性、持久性和防伪等特点,提供了更优异的认证性能。RF-Mehndi[16]使用标签的物理特征和持有者的生物特征来验证标签阵列的用户有效性。当用户触摸个人卡上的金属导体时,结合标签的物理层信息和用户的身体阻抗实现验证。虽然RF-Mehndi结合了标签的物理特征和用户生物特征信息,但仍然无法摆脱个人卡的影响,个人卡仍然会丢失,给用户带来麻烦。

[0007] 本发明所用到的名词解释如下:

[0008] 相位:相位是某一物理量随着时间(或位置)作余弦(或正弦)变化时,决定该量在任一时间(或位置)状态的一个数值。对于一个波而言,相位反映了在特定的时刻波在其周期循环中的位置,是一种波是否在波峰、波谷或它们之间的某点的标度,也是描述信号波形变化的度量,通常以度(角度)作为单位,也称作相角。当信号波形以周期的方式变化时,波

形循环一周即为 360° 。

[0009] Impinj商用设备:Impinj是全球领先的超高频Gen 2RFID解决方案供应商。基于公司的先进技术与业界诸多合作伙伴一起推出众多的产品和解决方案,包括高性能的标签芯片,读写器,读写器芯片,软件,天线和系统集成。

发明内容

[0010] 本发明所要解决的技术问题是,针对现有技术不足,提供一种用户生物特征信息认证方法及系统,提高用户认证识别准确率。

[0011] 为解决上述技术问题,本发明所采用的技术方案是:一种用户生物特征信息认证方法,包括以下步骤:

[0012] S1、对采集的RFID相位数据进行预处理,获得连续的相位数据;

[0013] S2、根据相位数据中的相位值和时间信息对标签数据进行异常检测,提取出用户输入的密码信号的特征部分;

[0014] S3、对所述特征部分进行特征提取,获得单个密码信号的特征向量;

[0015] S4、利用所有密码信号的特征向量训练分类器,获得区分不同密码的分类器模型;利用注册用户的特征向量训练分类器,获得区分不同用户的分类器模型。

[0016] 本发明由于只使用异常部分的中间窗口,提取的都是较为稳定的特征部分,舍弃了波动较大的数据异常部分,所以使得用户认证辨识系统具有较好的用户验证性能,提高了用户认证识别准确率。

[0017] 步骤S4中,利用随机森林算法训练分类器。本发明在进行密码识别和用户认证时,使用随机森林算法训练分类模型,较其他方法来说,能够处理很高纬度的数据,当用户使用的密码长度较长时也能有良好的性能表现,具有较快的模型训练速度。

[0018] 步骤S1的具体实现过程包括:取标签的前N个数据作为起始窗口,得到起始窗口内标签数据的相位均值,计算起始窗口内的所有标签相位和相位均值的差值,若某个标签数据的相位值与窗口内的相位均值的差值大于 $(\pi-1)$ 且小于 $(\pi+1)$,则判定该标签数据发生了倒 π 现象,将该相位值加上 π 并对 2π 取余;当该差值大于 $(\pi+1)$ 时,判定为发生了周期环绕现象,若标签相位值大于起始窗口内相位均值,则将标签相位值减去 2π ,反之,则加上 2π 。在大量实验的验证下,本步骤的阈值设置符合本发明的使用场景,能够很好的检测出起始窗口内的异常标签数据,从而得到一个稳定连续的标签相位,进一步提高了分类器的辨识精度。

[0019] 步骤S1的具体实现过程还包括:处理完起始窗口内的标签数据后,在其余待处理的标签数据前设置一个大小为n个标签数据的滑动窗口,将滑动窗口内的标签作为正常数据,计算滑动窗口内标签数据的相位均值,然后计算待处理标签数据的相位值和滑动窗口内标签数据相位均值的差值,若该待处理的标签数据点的相位值与窗口内的相位均值的差值大于 $(\pi-1)$ 且小于 $(\pi+1)$,则判定该标签数据发生了倒 π 现象,将该相位值加上 π 并对 2π 取余;当该差值大于 $(\pi+1)$ 时,判定为发生了周期环绕现象,若标签相位值大于滑动窗口内相位均值,则将标签相位值减去 2π ,反之,则加上 2π 。利用已经处理完毕的正常标签数据去检测未处理的标签数据,可以使得检测结果更加准确,并且由于待处理标签数据与滑动窗口内的标签是连续的,可以有效区分出由于触摸导致的标签信号变化和倒 π 或周期环绕现象,进一步提高了用户认证识别准确率。

[0020] 步骤S2的具体实现过程包括：

[0021] 1) 设置一个固定大小的滑动窗口，定义所述滑动窗口内标签的平均振幅 $A_i(k)$ 和标签的相位值基准度量 $x_m(i)$ ；

[0022] 2) 通过每个标签在滑动窗口内的平均振幅，计算得到所述滑动窗口内的标签振幅和G函数，对于第k个滑动窗口，若该第k个滑动窗口的G函数 $G(k)$ 大于阈值threshold，则该第k个滑动窗口为异常窗口；

[0023] 3) 获取所有异常窗口的中间窗口，取中间窗口内的标签数据作为特征部分。步骤S2通过使用滑动窗口，计算窗口内每个标签的平均振幅和9个标签的振幅和G函数，将单个的标签相位变化给结合到一起，避免了单个标签会由于某个触摸动作导致的相位变化不大，而使得异常检测失败，也能接受小部分的标签的特征遗失（由于触摸导致标签内部芯片功率太低而无法激活标签工作，阅读器也就无法获得标签信号），增强了本发明方法的鲁棒性。

[0024] 步骤S3的具体实现过程包括：获得特征窗口内M个标签的相位值，计算M个标签中两两标签间的相位差；所有相位差组成的向量即单个密码信号的特征向量；其中，所述特征窗口即中间窗口。本步骤中计算了M个标签之间的两两相位差，当其中一个标签相位发生了变化，会导致M个相位差发生变化。用户之间的微小生物特征差异会导致标签信号发生变化，并且由于耦合作用的存在而进一步将这些细微的差异放大，有助于用户的区分。

[0025] 本发明还提供了一种用户生物特征信息认证系统，其包括计算机设备；所述计算机设备被配置或编程为用于执行上述方法的步骤。

[0026] 与现有技术相比，本发明所具有的有益效果为：本发明既克服了传统密码容易被盗并且安全性能低的缺点，还克服了因使用专有设备的用户验证方法而带来的额外部署开销和高额使用成本。实验表明，本发明的方法对识别用户输入的密码的TPR (True Positive Rate, 真阳性率) 可以达到96.9%以上。当不同用户使用同一个密码时，本发明的方法也可以以一个较低的FPR (False Positive Rate, 假阳性率) 来区分不同的用户，因此本发明的方法可以有效地抵御冒充攻击和密码泄露等问题。本发明的方法实现了平均92.8%以上的用户认证识别准确率。本发明利用商用impinj读写器设备进行实验，可以很轻松的扩展到RFID商用市场。

附图说明

[0027] 图1 (a) 为相位周期环绕，图1 (b) 为相位的倒 π 现象；

[0028] 图2为滑动窗口检测异常信号图；

[0029] 图3为系统示意图；

[0030] 图4为标签的耦合作用示意图；

[0031] 图5为系统的整体工作流程图；

[0032] 图6为系统识别不同密码的TPR结果图；

[0033] 图7为不同用户使用同一密码的FPR结果图。

具体实施方式

[0034] 本发明实施例提供了一种基于RFID的利用标签物理层信息和用户生物特征信息

认证的个性化方案。本发明提供的是一种基于无源RFID的用户认证系统,利用商用impinj读写器设备进行实验,可以很轻松的扩展到RFID商用市场。本发明创造性地提出用九个标签(标签之间的耦合作用是距离越近作用越强,应该尽可能的使用较小的标签阵列,而使标签间的距离都较小。若使用2*2的标签阵列,密码数量太少,不满足使用需求;使用3*3大小的标签阵列刚好可以表示1~9的密码数字,比较契合人们日常使用密码输入的场景,且此时的9个标签也处在较强的耦合距离之内)组成一个密码阵列,其中一个标签作为一个密码按钮,用户只需要触摸标签的表面一次就可以输入一个密码,如图3所示。当用户连续触摸多个标签时,可以获得用户的密码序列,实现用户认证密码的功能。

[0035] 在本发明触摸的过程中,本发明也巧妙地将自己的生物特征信息整合到标签信号中。当用户触摸其中一个标签时,由于其指尖的阻抗会影响标签的相位信息,从而形成独特的相位特性。如图4所示,由于标签之间存在耦合效应,标签相互影响。标签阵列中的9个标签靠得越近,标签的耦合效果越强。当一个标签被碰触时,不仅它自己的信号会发生变化,其他八个标签的信号也会因为耦合效应而发生变化。这些信号的变化与使用者的身体阻抗高度相关,不同的用户有不同的身体阻抗,正常情况下人体的阻抗约为300-1000 Ω ,导致标签相位信号的不同变化。用户触摸其中一个标签就会使其余八个标签的信号发生变化,用户密码和用户的生物特征信息巧妙地结合在一起,增强了系统的抗攻击能力,结合用户生物特征信息可以区分使用相同密码的不同用户。

[0036] 本发明首先对采集的RFID相位数据进行预处理,获得一个连续的相位数据,然后根据相位值和时间信息对标签数据进行异常检测,提取出用户输入密码动作的特征部分,通过特征提取算法对提取出来的特征部分进行有效的特征提取,最后对所有的合法注册用户数据进行训练和建模。本发明使用impinj商用RFID阅读器进行数据采集,先识别区分出用户输入的密码序列,如果数据库中存在合法的用户密码序列,然后进一步进行用户认证,这种分成两阶段的验证方法可以有效地提升用户验证精度。

[0037] 为解决上述技术问题,本发明所采用的技术方案是:

[0038] 本发明通过从RFID设备获取到标签的数据后,将数据传送到PC机进行处理。处理的工作流程如图5所示,本发明可以看出,它包含四个主要步骤:数据采集、数据预处理和异常检测、特征提取、用户认证。

[0039] 第一步是数据采集工作,本发明系统的信号数据采集分为注册阶段和验证阶段。在注册阶段,每个用户设置自己的密码并触摸与其密码对应的标签。用户需要进行多次触摸密码序列数据采集工作,收集其身份特征信息,身份特征信息与用户的密码及其身体阻抗有关。从用户触摸的密码中提取出单个密码的特征,用户的密码序列就可以组合起来形成用户的特征向量。不同用户的阻抗和密码会导致每个人获得唯一的身份信息。在验证阶段,用户只需触摸该标签阵列一次,即可验证其在注册阶段设置的输入密码。然后,后台PC机可以获得标签的相关信号数据,并完成认证。

[0040] 第二步是数据预处理和异常检测,由于标签信号的基本特征,相位是一个周期函数,存在着周期围绕现象和倒 π 现象。为了获得可用的相位特性,本发明需要在得到标签信号后对数据进行预处理。将标签信息进行相位展开和消除倒 π 现象。图1(a)为相位周期环绕,图1(b)为相位的倒 π 现象。当用户触摸标签时,本发明发现标签阵列中的一些标签无法反馈标签信号。在图2中,两个相邻的标签数据由虚线连接。被圆圈包围的两条数据之间缺

少大量信号数据。这是因为在用户触摸标签之后,由于用户的阻抗和标签耦合的影响,标签功率变得相对较小,无法达到激活标签的阈值。因此,在该触摸阶段,标签数据不能被读取器读取,不能读取到标签的相位信号。本发明将利用这一现象作为验证用户身份的一项特征。为了保留这一特征,将不进行插值和数据平滑处理。

[0041] 从RFID系统采集到的原始数据可能伴随着倒 π 现象和相位环绕现象的发生,如图1(a)和图1(b)所示,这些都会对后来数据处理的准确性带来困扰,所以需要对其进行数据处理。倒 π 现象就是连续相位值中可能出现的异常的正负 π 相位值之差,原始数据采集到的相位值与真实的相位值相差一个 π 值,在图像中表现为连续的波形图出现尖刺情况,如图1(b)所示,发生倒 π 现象的异常点被圆圈圈出,处理之后的数据用矩形圈出表示。

[0042] 本发明使用滑动窗口对倒 π 现象进行处理:首先,我们取标签的前十个数据点(若数据量少于十个,则可能会由于异常点过多使得窗口内相位均值偏向异常点,而对异常数据判断错误,过多的数据量也是不需要的,经过实验论证,10个数据点就已经可以很好地检测出异常点并得到初始的正常标签数据)作为我们的起始窗口,因为此时的标签数据是较稳定的,无用户动作的。我们找出此窗口中的异常点,即标签相位值较窗口平均值的差值在 $(\pi-1, \pi+1)$ 内的点。本发明将异常点认定为发生了倒 π 的标签数据,对倒 π 现象的修正方法为将其相位值加上 π 并对 2π 取余,这是因为标签相位是一个周期函数,其值为0到 2π 。接下来对除前十个数据以外的标签数据进行处理,在待处理数据前设定一个滑动窗口,此时的窗口大小设定为6个标签数据(因为起始窗口内的数据已经处理完毕,此6个数据均为正常标签数据,可以满足检测出异常点的需求),比较标签相位值与窗口平均值的差值是否在设定的阈值内判断其是否发生了倒 π 现象,对发生了倒 π 现象的相位值进行修正,处理完倒 π 现象使标签相位值变得相对连续。

[0043] 相位周期环绕现象[1]是由于相位角处在0到 2π 的固定范围值而产生超过最大值 2π 周期性跳变为0的过程,与真实相位相比存在着不同程度的相位周期模糊性。往往通过恢复失去的相位周期性,得到解决相位环绕的过程,如图1(a)所示,发生周期环绕现象的异常点被圆圈圈出,处理之后的数据用矩形圈出表示。在这一过程中与处理倒 π 原理相似,本发明使用滑动窗口的方法对数据进行异常检测,只是阈值设定与处理倒 π 的不同,当待处理标签相位值与窗口内标签相位平均值的差值大于 $(\pi+1)$ 时,判定为发生了周期环绕现象,若标签相位值大于窗口相位均值,则将标签相位值减去 2π ,反之,则加上 2π 。对于发生了周期环绕现象的数据根据不同情况进行加 2π 或者是减 2π 的处理。

[0044] 经过数据预处理后,本发明得到了一个连续可用的标签相位信号,需要进一步提取与用户身份信息相关的相位特征。本发明发现,当用户触摸标签的那一刻和用户移除手指的那一刻,标签信号的变化相对复杂、混乱,相位特征不稳定。然而,在触摸过程中,标签的相位信号趋于稳定。因此,本发明提出了一种使用G函数的滑动窗口异常检测算法来提取中间部分稳定的标签相位信号。

[0045] 基于滑动窗口的检测方法对连续的用户数据进行异常信号检测,其具体算法如下:

[0046] 1) G函数检测:我们提出一种基于滑动窗口的异常检测方法,在一段连续的用户触摸标签阵列活动中检测出单个触摸动作并提取出稳定有效的特征窗口。我们首先设置了一个固定大小的滑动窗口来检测异常的标签数据(在此处窗口大小设置为0.5s),标签数据包

含时间信息和相位值。分别定义了窗口内标签的平均振幅 $A_i(k)$ 和标签的相位值基准度量 $x_m(i)$ (i) :

$$[0047] \quad A_i(k) = \frac{\sum_{j=1}^l |x_j - x_m(i)|}{l};$$

$$[0048] \quad x_m(i) = \frac{\sum_{j=1}^l |x_j|}{l};$$

[0049] 其中 $A_i(k)$ 表示第i个标签在第k个窗口中的平均振幅,l表示固定长度的滑动窗口中标签数据量, x_j 表示第j个数据的相位值, $x_m(i)$ 表示标签在第一个窗口中的平均相位值,作为计算振幅的相位基准。接下来,我们定义每个窗口内的标签振幅和为 $G(k)$ [3],则 $G(k)$ 可由 $A_i(k)$ 计算得到:

$$[0050] \quad G(k) = \sum_{i=1}^9 A_i(k);$$

[0051] 2) 阈值比较:我们通过每个标签在滑动窗口内的平均振幅计算得到窗口内的标签振幅和 G 函数,接下来我们经验的设置阈值 $\text{threshold}=1.5$,若 $G(k)$ 大于阈值 threshold ,则将第k个窗口标记为异常窗口。用户的单次触摸是一个连续的动作,所以经过阈值比较过后我们可以得到一个连续的异常窗口序列,如图2所示,异常窗口被虚线划分出来。该连续的异常部分则为用户触摸标签时引起的标签信号变化。

[0052] 3) 获取特征窗口:得到异常窗口后我们发现,在连续的异常窗口中,中间窗口内的标签相位值较为稳定,而前一两个异常窗口和最后一两个异常窗口内的标签相位值变化剧烈。这是由于用户刚触摸标签时和触摸后刚拿开手指时手指动作较大且指尖与标签表面的接触面积变化大,导致标签的信号波动较大。不稳定的标签数据显然不能作为我们的特征数据来提取用户的生物特征信息,为了避免使用到这些不稳定的标签数据,我们取中间窗口内的标签数据作为特征数据,如图2所示,矩形部分为我们获得的特征窗口。

[0053] 第三步是特征提取,将上一步本发明得到的特征部分进行特征提取。本发明计算九个标签之间的两两标签相位差,可以得到36个有效的特征值并作为单个密码的特征向量。

[0054] 下面是特征值的具体计算方法:

[0055] 1) 获得特征窗口内9个标签的相位值, A'_i 表示第i个标签在特征窗口内的平均相位值:

$$[0056] \quad [A'_1, A'_2, A'_3, A'_4, A'_5, A'_6, A'_7, A'_8, A'_9];$$

[0057] 2) 计算9个标签中两两标签间的相位差:

$$[0058] \quad \Delta A_{ij} = |A'_i - A'_j|;$$

[0059] 3) 因为 ΔA_{ij} 和 ΔA_{ji} 是相等的,并且 $\Delta A_{ii}=0$,所以从9个标签中我们可以得到36个有效的特征值,将这36个特征值组成用户单次触摸标签,即输入单个密码的特征向量 F :

$$[0060] \quad F = [\Delta A_{12}, \dots, \Delta A_{19}, \Delta A_{23}, \dots, \Delta A_{29}, \Delta A_{34}, \dots, \Delta A_{89}].$$

[0061] 最后一步是身份验证,本发明采用监督学习下的决策树学习进行分类,利用上述提取的特征,选用随机森林算法[5]构建分类器模型,进行不同密码区分训练和用户认证识别训练。本发明利用Weka[17]中的分类模型功能将在注册阶段收集的用户信息训练成验证模型。收集用户数据,提取特征信息,然后利用分类模型来确定该用户是否为合法用户。

[0062] 本发明实验系统中所使用的硬件如下:Impinj Speedway读写器、圆极化Laird

S9028PCR天线和内置Monza4芯片的AZ-9629型号无源标签。阅读器可以扩展配置四个定向天线,通过天线来发射和接收无线电信号。当读写器接通电源后,无源标签可以接收到与读写器相连天线发射的电磁波,从磁场中获得工作所需的能量,并通过反射信号与读写器进行通信。RFID设备主要由读写器和天线组成,本发明的PC机通过网线与读写器自身的Ethernet端口相连,可以获取到天线采集的用户输入密码的信息。

[0063] 本发明实验系统是基于Java的开发环境,在eclipse软件中导入OctaneSDKJava-1.24.1.0的jar包,利用Impinj产品提供的高度集成的环境编写控制读写器功能代码。本发明用户认证系统所需采集的信息包括标签的EPC、时间戳和相位等主要信息。然后将采集的信息通过Matlab应用程序对其进行预处理和数据分析,最终本发明将提取出来的特征向量运用机器学习算法进行训练和测试。

[0064] 如图3,本发明实施例9个RFID无源标签形成的标签阵列固定在天线上方,连接到阅读器的天线读取标签数据,最后数据由计算机处理。RFID读写器通过天线发送电磁波信号,然后天线接收并提取来自用户输入密码动作的后向散射信号,完成数据的采集工作。

[0065] 如图6所示,经过大量实验,本发明对识别用户输入的密码的TPR (True Positive Rate,真阳性率)可以达到96.9%以上。如图7所示,当不同用户使用同一个密码时,我们的方法也可以以一个较低的FPR (False Positive Rate,假阳性率)来区分不同的用户,这表明我们可以有效地抵御冒充攻击和密码泄露等问题。最终,我们的方法实现了平均92.8%以上的用户认证识别准确率。

[0066] 本发明介绍的是一种基于RFID的用户生物特征信息认证方法及系统,它是一种利用无源RFID标签数据进行用户验证的双因素认证系统,系统首先验证用户的密码,然后识别用户的生物特征进行认证。本发明的系统是一个由九个无源标签阵列和一个商用RFID读写器组成的用户识别系统,用户触摸阵列表面的标签,类似于输入密码的操作。当用户触摸其中一个标签时,由于其指尖的阻抗会影响标签的相位信息,从而形成独特的相位特性。用户密码和用户的生物特征信息巧妙地结合在一起,增强了系统的抗攻击能力。首先,本发明对信号数据进行预处理,以获得展开的连续的相位信息,然后使用滑动窗口来检测出信号的异常部分,并提取出稳定的用户动作数据和有效的特征,利用机器学习随机森林算法构建分类器模型,对用户进行认证识别。实验结果表明,本发明的方法具有较好的用户验证准确率,能够有效区分合法用户和非法用户,综合用户认证精度达到92.8%。

[0067] 参考文献:

[0068] [1]Zuo,Chao,et al."Temporal phase unwrapping algorithms for fringe projection profilometry:A comparative review."Optics and Lasers in Engineering 85 (2016):84-103.

[0069] [2]Azami,Hamed,Karim Mohammadi,and BehzadBozorgtabar."An improved signal segmentation using moving average and Savitzky-Golay filter."Journal of Signal and Information Processing 3.01 (2012):39.

[0070] [3]Narudin,Fairuz Amalina,et al."Evaluation of machine learning classifiers for mobile malware detection."Soft Computing 20.1 (2016):343-357.

[0071] [4]Tao Li,Wen Luo,Zhen Mo,Shigang Chen."Privacy-preserving RFID authentication based on cryptographical encoding."IEEE Conference on Computer

Communications (INFOCOM) 2012:2174-2182.

[0072] [5] Li Lu, Jinsong Han, Renyi Xiao, Yunhao Liu. "ACTION: Breaking the Privacy Barrier for RFID Systems." IEEE Conference on Computer Communications (INFOCOM) 2009:1953-1961.

[0073] [6] Min-Te Sun, Kazuya Sakai, et al. "Private and Secure Tag Access for Large-Scale RFID Systems." IEEE Trans. Dependable Secur. Comput. 13(6):657-671 (2016).

[0074] [7] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, Daniel W. Engel. "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems." International Conference on Security in Pervasive Computing (SPC) 2003:201-212.

[0075] [8] Qingsong Yao, Yong Qi, Jinsong Han, et al. "Randomizing RFID Private Authentication." IEEE International Conference on Pervasive Computing and Communications (PerCom) 2009:1-10.

[0076] [9] Han Ding, Jinsong Han, Yanyong Zhang, et al. "Preventing Unauthorized Access on Passive Tags." IEEE Conference on Computer Communications (INFOCOM) 2018:1115-1123.

[0077] [10] Jinsong Han, Chen Qian, Panlong Yang, et al. "GenePrint: Generic and Accurate Physical-Layer Identification for UHF RFID Tags." IEEE/ACM Trans. Netw. 24(2):846-858 (2016).

[0078] [11] Lei Yang, Pai Peng, Fan Dang, et al. "Anti-counterfeiting via federated RFID tags' fingerprints and geometric relationships." IEEE Conference on Computer Communications (INFOCOM) 2015:1966-1974.

[0079] [12] Xingyu Chen, Jia Liu, Xia Wang, et al. "Eingerprint: Robust Energy-related Fingerprinting for Passive RFID Tags." 17th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2020:1101-1113.

[0080] [13] Ge Wang, Haofan Cai, Chen Qian, et al. "Towards Replay-resilient RFID Authentication." Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, MobiCom 2018:385-399.

[0081] [14] Jinsong Han, Chen Qian, Xing Wang, et al. "Twins: Device-Free Object Tracking Using Passive Tags." IEEE/ACM Trans. Netw. 24(3):1605-1617 (2016).

[0082] [15] Lei Yang, Yekui Chen, Xiang-Yang Li, et al. "Tagoram: real-time tracking of mobile RFID tags to high precision using COTS devices." The 20th Annual International Conference on Mobile Computing and Networking, MobiCom 2014:237-248.

[0083] [16] Cui Zhao, Zhenjiang Li, Ting Liu, et al. "RF-Mehndi: A Fingertip Profiled RF Identifier." IEEE Conference on Computer Communications, INFOCOM 2019:1513-1521

[0084] [17] G. Holmes, A. Donkin, and I. Witten. "WEKA: A Machine

LearningWorkbench.”In IEEE ANZIS,1994.

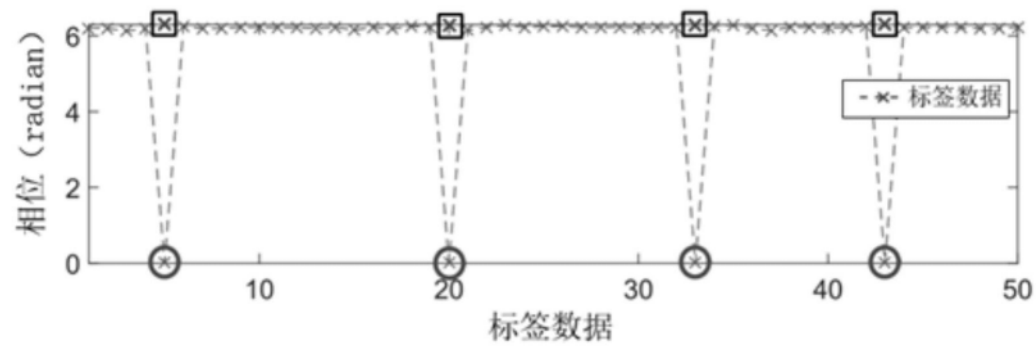


图1 (a)

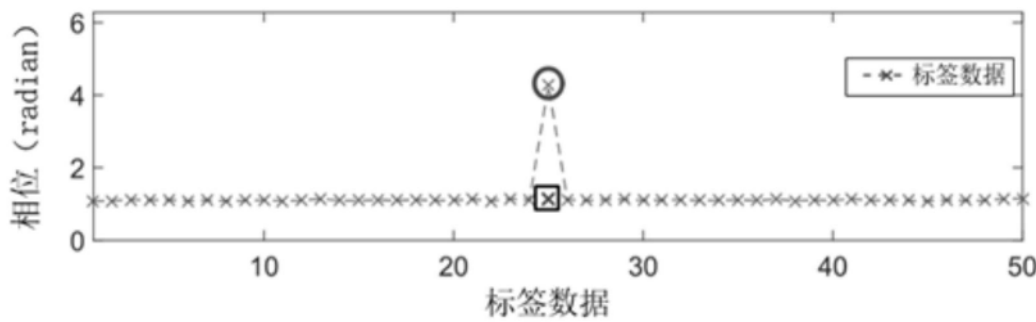


图1 (b)

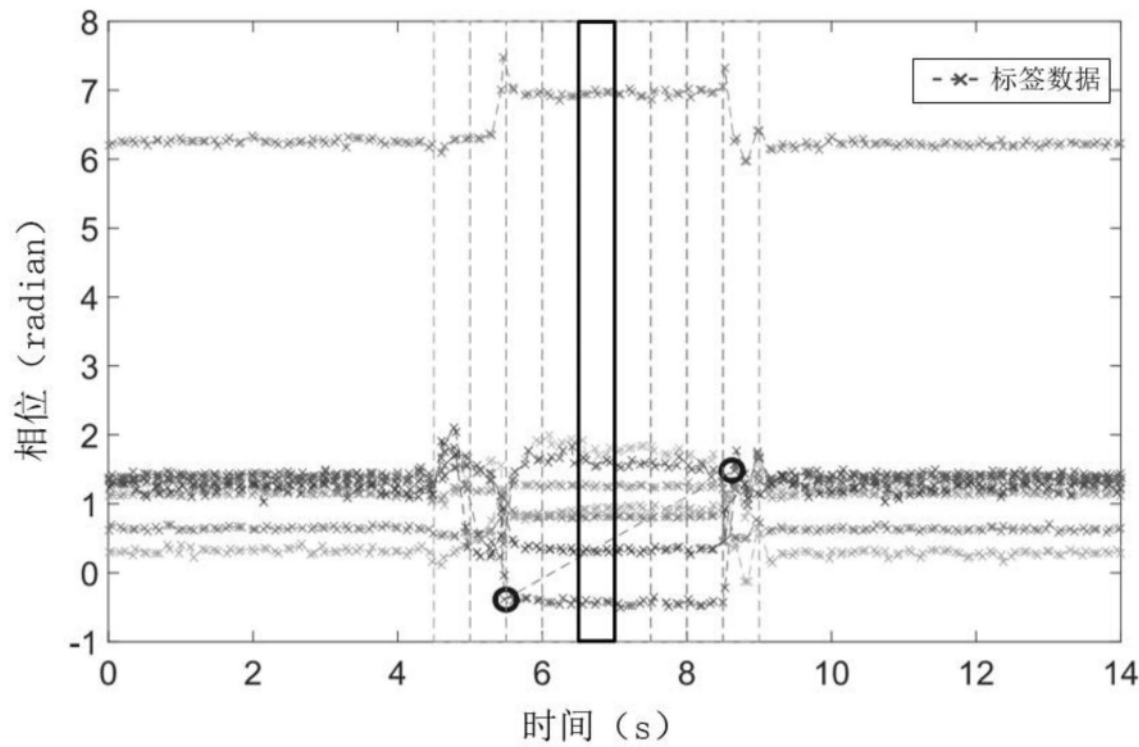


图2

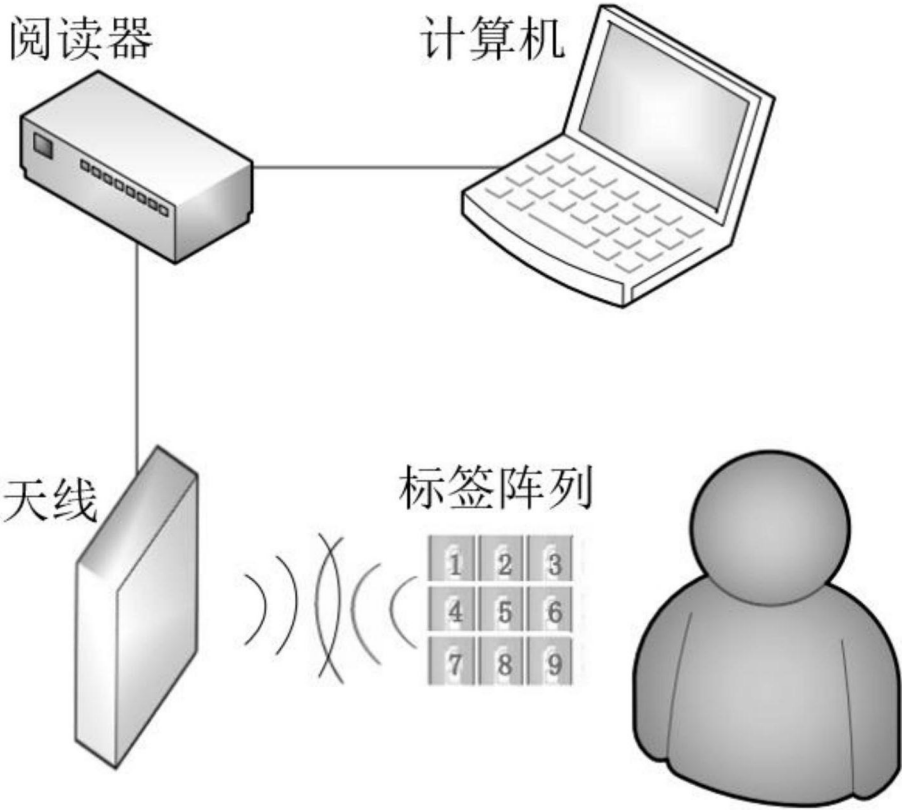


图3

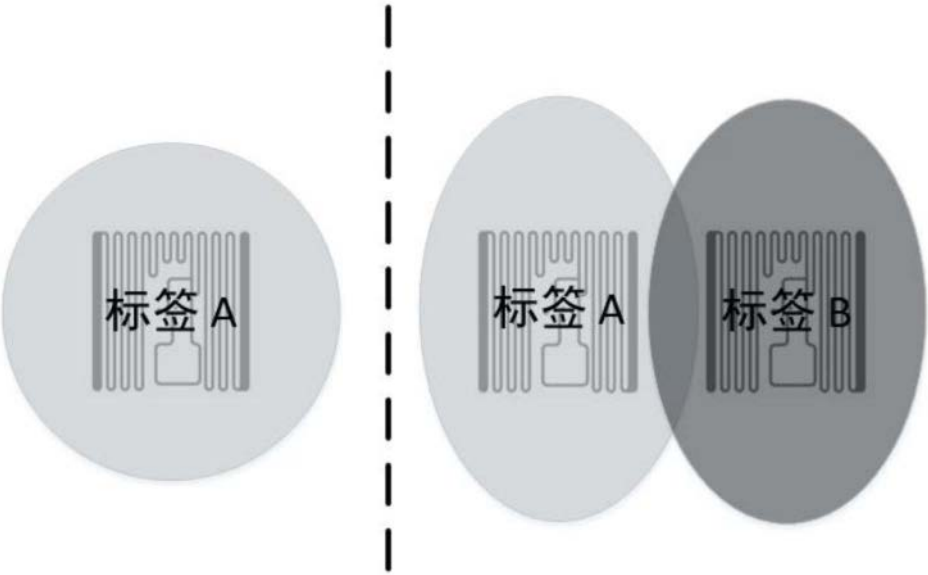


图4

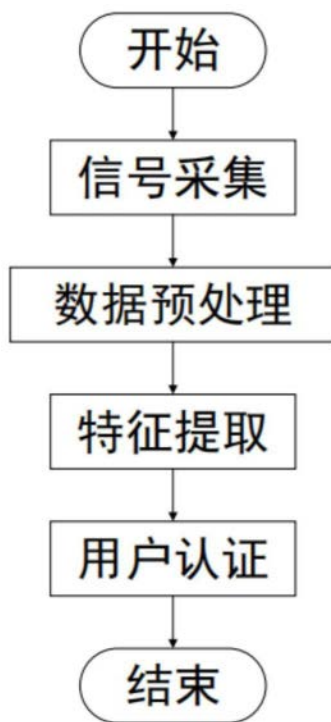


图5

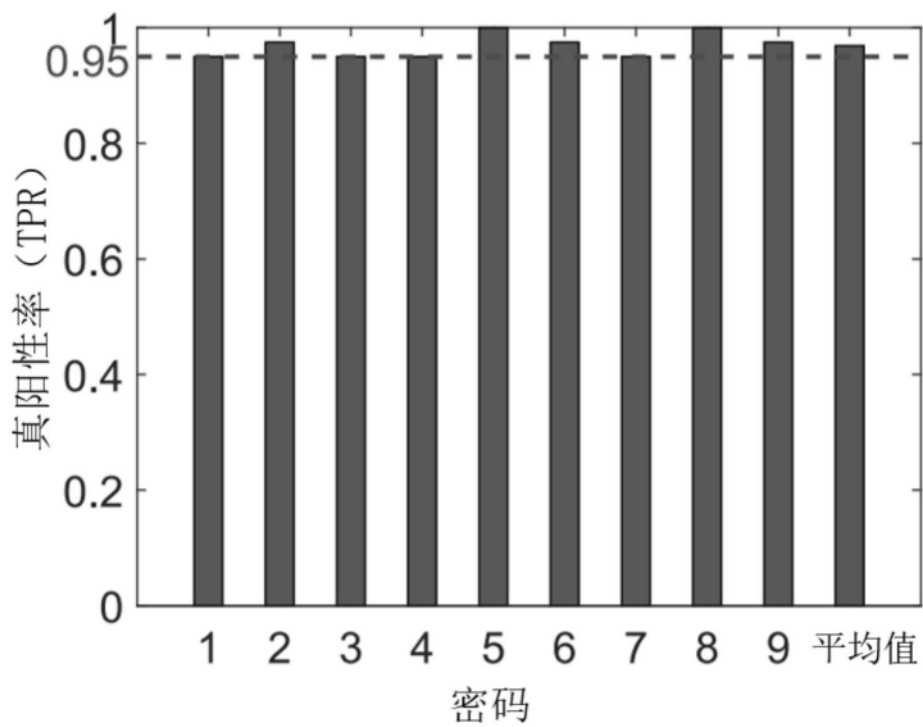


图6

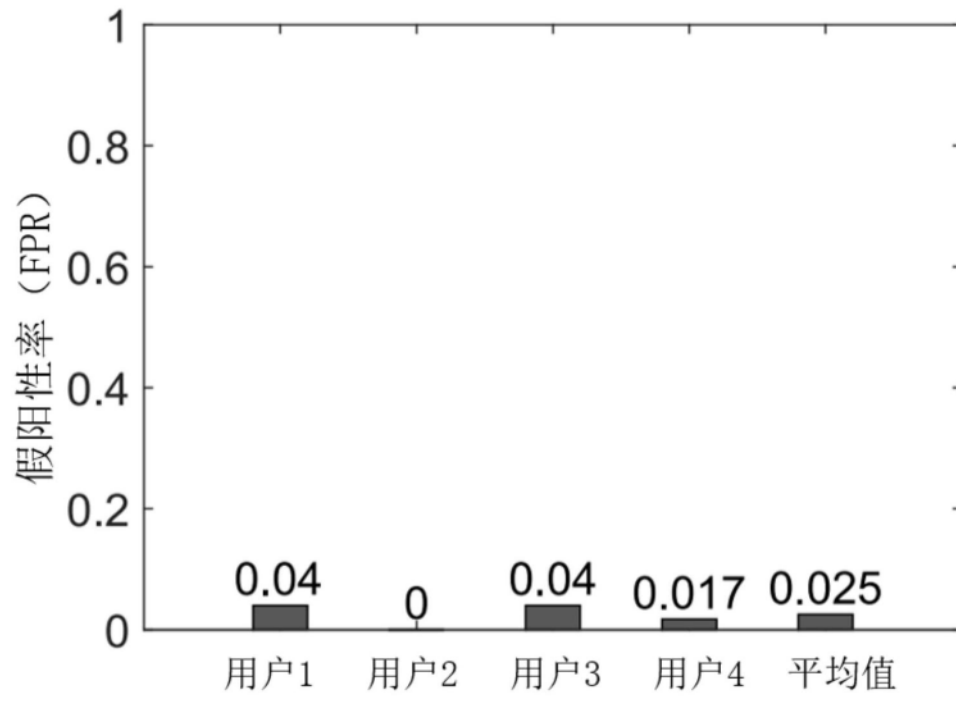


图7