(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104408341 A
(43)申请公布日 2015.03.11

(21)申请号 201410641806.9

(22)申请日 2014.11.13

(71)申请人 西安交通大学
地址 710049 陕西省西安市碑林区咸宁西路28号

(72)发明人 沈超 蔡忠闽 左幸存 余天文 管晓宏

(74)专利代理机构 西安通大专利代理有限责任公司 61200
代理人 朱海临

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 3/01(2006.01)

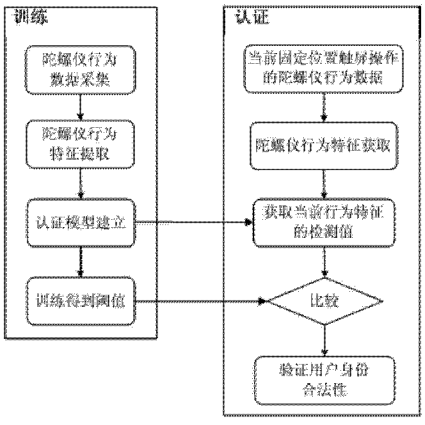
权利要求书2页 说明书5页 附图2页

(54)发明名称

基于陀螺仪行为特征的智能手机用户身份认证方法

(57)摘要

本发明公开了一种基于陀螺仪行为特征的智能手机用户身份认证方法，通过分析智能手机用户在触屏操作时所产生的陀螺仪行为数据，根据触屏操作的时间信息提取不同操作事件对应的传感器行为数据，生成传感器行为特征，并基于行为特征建立用户的身份认证模型，对智能手机用户进行身份认证。本发明方法的优点在于：操作简单，无需增加任何额外设备；在不改变用户习惯的基础上使用陀螺仪操作行为描述手机用户在认证过程中体现出的行为特性，以此作为用户身份判定的依据，能够有效防止污迹攻击和观察攻击，具有广泛的安全性和适用性。



CN 104408341 A

1. 一种基于陀螺仪行为特征的智能手机用户身份认证方法，其特征在于，由训练和认证两个部分构成，其中：

所述训练部分包括下述步骤：

(1) 陀螺仪采集并记录用户多次触屏操作过程中形成的行为数据，形成训练数据；

(2) 针对每次陀螺仪所记录的行为数据，提取触屏操作对应的陀螺仪行为数据；

(3) 针对触屏操作对应的陀螺仪行为数据，提取行为特征向量，在其中获取参考特征向量，计算行为特征向量与参考特征向量的距离，得到距离特征向量，形成训练特征集合；

(4) 采用单分类器建立用户的身份认证模型，将合法用户的训练特征集合标记为正类对身份认证模型进行训练，得到合法用户的身份判定阈值；

所述认证部分包括下述步骤：

(1) 在认证时，陀螺仪获取用户与训练相同的触屏操作产生的行为数据，提取触屏操作对应的陀螺仪行为数据；

(2) 针对触屏操作对应的陀螺仪行为数据，提取行为特征向量，与训练部分所述的认证模型训练时获得的参考特征向量进行距离度量，得到距离特征向量；

(3) 将该距离特征向量作为身份认证模型的输入，得到身份认证的检测值，并将该检测值与身份判定阈值进行比较，进而判定用户身份的合法性。

2. 根据权利要求 1 所述的基于陀螺仪行为特征的智能手机用户身份认证方法，其特征在于，所述提取触屏操作对应的陀螺仪行为数据是指针对每次触屏操作，提取触屏操作开始时和结束时的时间，得到触屏操作的时间区间，并将该时间区间与陀螺仪记录的行为数据时间戳进行匹配，得到每次触屏操作下对应的陀螺仪行为数据。

3. 根据权利要求 1 所述的基于陀螺仪行为特征的智能手机用户身份认证方法，其特征在于，所述针对触屏操作对应的陀螺仪行为数据，提取行为特征向量的具体方法是：提取针对触屏操作对应的陀螺仪行为数据，包括统计特征和距离特征，具体如下：

统计特征是指每次触屏操作对应的陀螺仪行为数据的统计描述量，包括：

X 轴角速度的最大值、最小值、均值、中值、标准差、75％分位数与 25％分位数之差、峰度系数、偏度系数；

Y 轴角速度的最大值、最小值、均值、中值、标准差、75％分位数与 25％分位数之差、峰度系数、偏度系数；

Z 轴角速度的最大值、最小值、均值、中值、标准差、75％分位数与 25％分位数之差、峰度系数、偏度系数；

距离特征是指在相同触屏操作上陀螺仪行为数据与参考行为数据之间的距离度量，其具体计算步骤为：

1) 在相同触屏操作对应陀螺仪行为训练数据中，包括多组样本数据，采用动态时间规整计算每组样本数据与其它组样本数据之间的距离，累加后得到距离之和，选择距离之和最小的陀螺仪样本数据作为参考行为数据；

2) 采用动态时间规整计算在每次相同触屏操作上陀螺仪行为数据与参考行为数据之间的距离，得到距离特征。

4. 根据权利要求 1 所述的基于陀螺仪行为特征的智能手机用户身份认证方法，其特征在于，所述的参考特征向量的获取是指在触屏操作对应的陀螺仪行为数据中，采用曼哈

顿距离计算每个行为特征向量到其它行为特征向量的距离，形成该特征向量对应的距离向量，选择距离向量模最小的特征向量作为参考特征向量。

基于陀螺仪行为特征的智能手机用户身份认证方法

技术领域

[0001] 本发明涉及智能手机用户身份认证，特别涉及一种利用手机传感器数据的智能手机用户身份认证方法。

背景技术

[0002] 随着移动互联网的迅猛发展，智能手机已渗透到各行各业，影响着人们生活和工作的各个细节。智能手机记录和存储着移动用户愈来愈多的重要数据（如账户密码）和隐私信息（如短信和视频）。特别是近年来手机支付相关应用的大量使用以及隐私泄漏事件的频繁发生，使得人们对智能手机的安全保护问题越来越关注。

[0003] 安全有效的身份认证是进行智能手机安全保护的核心问题，是指用户在访问智能手机系统或者访问不同保护级别的系统资源时，系统确认该用户的身份是否合法的过程。目前用于智能手机的身份验证方式主要有三种：1)PIN密码，2)图形密码，3)指纹。对于PIN密码的方式而言，易于实现且简单方便，但是容易被遗忘或被盗取；对于图形密码（用户需要在3x3的点阵上按照一定顺序连接若干点作为密码）的方式而言，易于记忆，但触屏痕迹和手指运动容易被观察造成猜测攻击；对于指纹识别方式而言，虽然准确度高，但是需要特殊的硬件支持。

发明内容

[0004] 利用智能手机用户在触屏操作过程中所展现的动作行为作为身份认证的依据可以作为替换或增强PIN密码/图形密码/指纹认证的一种很好的手段，同时由于手机传感器（如加速度计或陀螺仪）作为智能手机中所固有的内置设备，能够直接地、准确地对用户触屏操作过程中的动作行为进行反映和测量，因此可以采用用户在触屏操作时所引起的手机陀螺仪行为数据对用户的动作行为进行测量，并以此作为用户身份认证的依据。与前述三种当前流行的认证方式相比，使用陀螺仪行为特征进行身份认证：不会遗忘和丢失，不易被他人窃取和伪造；操作简单，不需要特殊的硬件支持，且成本很低，容易大范围推广；此外，能够有效防止污迹攻击和观察攻击，具有广泛的安全性和适用性。

[0005] 本发明的目的是提供一种基于手机传感器数据的智能手机用户身份认证方法，特别是利用用户在触屏操作过程中被陀螺仪记录的行为特征来判断用户身份合法性的方法。

[0006] 为达到以上目的，本发明是采用如下技术方案实现的：

[0007] 一种基于陀螺仪行为特征的智能手机用户身份认证方法，其特征在于，由训练和认证两个部分构成，其中：

[0008] 所述训练部分包括下述步骤：

[0009] (1)陀螺仪采集并记录用户多次触屏操作过程中形成的行为数据，形成训练数据；

[0010] (2)针对每次陀螺仪所记录的行为数据，提取触屏操作对应的陀螺仪行为数据；

[0011] (3)针对触屏操作对应的陀螺仪行为数据，提取行为特征向量，在其中获取参考

特征向量，计算行为特征向量与参考特征向量的距离，得到距离特征向量，形成训练特征集合；

[0012] (4) 采用单分类器建立用户的身份认证模型，将合法用户的训练特征集合标记为正类对身份认证模型进行训练，得到合法用户的身份判定阈值；

[0013] 所述认证部分包括下述步骤：

[0014] (1) 在认证时，陀螺仪获取用户与训练相同的触屏操作产生的行为数据，提取触屏操作对应的陀螺仪行为数据；

[0015] (2) 针对触屏操作对应的陀螺仪行为数据，提取行为特征向量，与训练部分所述的认证模型训练时获得的参考特征向量进行距离度量，得到距离特征向量；

[0016] (3) 将该距离特征向量作为身份认证模型的输入，得到身份认证的检测值，并将该检测值与身份判定阈值进行比较，进而判定用户身份的合法性。

[0017] 上述方法中，所述提取触屏操作对应的陀螺仪行为数据是指针对每次触屏操作，提取触屏操作开始时和结束时的时间，得到触屏操作的时间区间，并将该时间区间与陀螺仪记录的行为数据时间戳进行匹配，得到每次触屏操作下对应的陀螺仪行为数据。

[0018] 所述针对触屏操作对应的陀螺仪行为数据，提取行为特征向量的具体方法是：提取针对触屏操作对应的陀螺仪行为数据，包括统计特征和距离特征，具体如下：

[0019] 统计特征是指每次触屏操作对应的陀螺仪行为数据的统计描述量，包括：

[0020] X 轴角速度的最大值、最小值、均值、中值、标准差、75％分位数与 25％分位数之差、峰度系数、偏度系数；

[0021] Y 轴角速度的最大值、最小值、均值、中值、标准差、75％分位数与 25％分位数之差、峰度系数、偏度系数；

[0022] Z 轴角速度的最大值、最小值、均值、中值、标准差、75％分位数与 25％分位数之差、峰度系数、偏度系数；

[0023] 距离特征是指在相同触屏操作上陀螺仪行为数据与参考行为数据之间的距离度量，其具体计算步骤为：

[0024] 1) 在相同触屏操作对应陀螺仪行为训练数据中，包括多组样本数据，采用动态时间规整计算每组样本数据与其它组样本数据之间的距离，累加后得到距离之和，选择距离之和最小的陀螺仪样本数据作为参考行为数据；

[0025] 2) 采用动态时间规整计算在每次相同触屏操作上陀螺仪行为数据与参考行为数据之间的距离，得到距离特征。

[0026] 所述的参考特征向量的获取是指在触屏操作对应的陀螺仪行为数据中，采用曼哈顿距离计算每个行为特征向量到其它行为特征向量的距离，形成该特征向量对应的距离向量，选择距离向量模最小的特征向量作为参考特征向量。

[0027] 本发明方法的优点在于：陀螺仪行为特征无需记忆和携带，不易被他人窃取和伪造；操作简单，无需增加任何额外设备；在不改变用户习惯的基础上使用陀螺仪操作行为描述手机用户在认证过程中体现出的行为特性，以此作为用户身份判定的依据，能够有效防止污迹攻击和观察攻击，具有广泛的安全性和适用性。此外，采用距离度量的特征表示方法可有效降低行为波动的影响，显著地提高身份认证的鲁棒性。

附图说明

[0028] 下面结合附图及具体实施方式对本发明做进一步的详细描述。

[0029] 图 1 是本发明方法的总体流程示意图。

[0030] 图 2 是本发明方法中触屏操作对应的陀螺仪行为数据提取的具体流程示意图。

[0031] 图 3 是本发明方法中陀螺仪行为距离特征向量提取方法的具体流程示意图。

[0032] 图 4 是采用本发明进行智能手机用户身份认证的实验操作的截屏照片。

[0033] 图 5 是采用本发明进行智能手机用户身份认证的实验结果图。

具体实施方式

[0034] 参见图 1，一种基于陀螺仪行为特征的智能手机用户身份认证方法，可用于触屏设备操作者身份合法性进行认证，实现对触屏设备内部存储的个人和敏感信息的安全防护。本发明包含身份认证模型训练和操作者身份认证两个部分，具体的实施步骤如下：

[0035] 1) 身份认证模型训练部分包括下述步骤：

[0036] (1) 陀螺仪采集并记录用户多次在固定触屏位置的点击和滑动操作（触屏操作）过程中的陀螺仪行为数据，得到训练数据集；陀螺仪行为数据的格式为：{水平向右方向 (X 轴）的角速度，垂直向上方向 (Y 轴）的角速度，屏幕正面法线方向 (Z 轴）的角速度，时间戳}。

[0037] (2) 针对每次陀螺仪所记录的行为数据，提取触屏操作对应的陀螺仪行为数据（参见图 2)。具体为：

[0038] 第一步，提取触屏操作时手指接触和离开触摸屏的时间，得到触屏操作的时间区间；

[0039] 第二步，将每个触屏操作的时间区间与陀螺仪行为数据的时间戳进行匹配，得到每个触屏操作下对应的陀螺仪行为数据。

[0040] (3) 针对触屏操作对应的陀螺仪行为数据，提取行为特征向量，在其中获取参考特征向量，计算行为特征向量与参考特征向量的距离，得到距离特征向量，形成训练特征集合（参见图 3)。具体为：

[0041] 第一步，针对训练数据集中每次触屏操作过程中触屏操作对应的陀螺仪行为数据，提取陀螺仪行为特征向量，具体为触屏操作引起智能手机晃动所衍生出的一系列陀螺仪行为测量，包括统计特征和距离特征两类。其中，统计特征是指每个触屏操作对应的陀螺仪行为数据的统计描述量，包括 X 轴、Y 轴、Z 轴角速度的最大值、最小值、均值、中值、标准差、75％分位数与 25％分位数之差、峰度系数、偏度系数；距离特征是指在相同触屏操作上的陀螺仪行为数据与参考行为数据之间的距离度量，其具体计算步骤为：首先，在相同触屏操作对应陀螺仪行为训练数据中，采用动态时间规整计算每个陀螺仪样本数据与其它陀螺仪样本数据之间的距离，累加后得到距离之和，选择距离之和最小的陀螺仪样本数据作为参考行为数据；然后，采用动态时间规整计算在每个相同触屏操作上陀螺仪行为数据与参考行为数据之间的距离，得到距离特征；

[0042] 假设合法用户训练采集了 n 组数据，分别用 DTW（动态时间规整）计算某组数据和其他 n-1 组数据向量的距离之和。选取和其他 n-1 组数据欧式距离最小的一组作为参考样本；

[0043] 第二步，采用欧式距离计算每次触屏操作过程中陀螺仪行为特征向量与训练集中其它陀螺仪行为特征向量的距离，得到维度为 (P-1) 的距离向量（其中 P 表示训练集中触屏操作过程的次数）；计算训练集中每个距离向量的模，选择模值最小的陀螺仪行为向量作为参考行为特征向量；

[0044] 第三步，采用曼哈顿距离计算每次触屏操作过程中陀螺仪行为特征向量与参考行为特征向量的差值向量，作为每次触屏操作过程中陀螺仪行为数据的距离特征向量，形成陀螺仪行为训练特征集；

[0045] (4) 采用单类分类器建立合法用户的身份认证模型，将合法用户的训练特征集合标记为正类对身份认证模型进行训练，得到合法用户的身份判定阈值 σ（σ 根据模型训练的精度进行选取）；

[0046] 2) 操作者身份持续认证部分，包括下述步骤：

[0047] (1) 在认证时，陀螺仪获取用户与训练相同的触屏操作产生的行为数据，提取触屏操作对应的陀螺仪行为数据；

[0048] (2) 针对触屏操作对应的陀螺仪行为数据，提取行为特征向量，与训练部分所述的认证模型训练时获得的参考特征向量进行距离度量，得到距离特征向量；

[0049] (3) 将该距离特征向量作为身份认证模型的输入，得到身份认证的检测值，并将该检测值与的合法用户身份判定阈值 σ 进行比较，若检测值大于阈值，则判定的当前用户为非法用户；若检测值小于阈值，则判定当前用户为合法用户；

[0050] 根据本发明进行智能手机用户身份认证的实验

[0051] 本发明以智能手机用户的身份认证为例进行了实验验证，具体步骤如下：

[0052] 第一步，生成训练数据。实验要求 10 名用户分别按照图 4 的方式在智能手机上进行触屏操作，重复 30 次，每次包括 3 个触屏点击操作和 4 个触屏滑动操作，采集和记录这些用户进行上述操作时陀螺仪行为数据。在图 4 所示的方式中，用户在点一、二、三上进行触屏点击操作，在点四、五、六、七、八之间进行触屏滑动操作。

[0053] 第二步，在每次触屏操作过程中提取触屏操作对应的陀螺仪行为数据。针对每个用户，提取触屏操作开始时和结束时的时间，得到每个触屏操作对应的时间区间；将每个触屏操作的时间区间与陀螺仪行为数据的时间戳进行匹配，提取每个触屏操作下对应的陀螺仪行为数据。

[0054] 第三步，生成距离特征向量。针对每个用户，提取每次触屏操作过程中陀螺仪行为特征向量，并选取参考特征向量，比对行为特征向量和参考特征向量后得到距离特征向量，形成训练特征集合。

[0055] 第四步，身份认证模型构建。针对每个用户，将该用户的训练特征数据标记为正类，采用单分类支持向量机构建合法用户的身份认证模型，并利用训练特征集对模型进行学习。

[0056] 第五步，生成测试数据。针对每个用户，要求其按照图 4 的方式进行触屏操作，重复 20 次，得到测试数据集。

[0057] 第六步，用户身份合法性的认证。选择某一用户作为合法用户，针对其中的每一条测试样本，生成距离特征向量，将其作为该用户身份认证模型的输入，得到身份认证的检测值，并将该检测值与阈值 σ（σ 设定为 0.55）比较，若检测值小于阈值 σ，则判定该用户为

非法用户；反之，则判定该用户为合法操作。

[0058] 第七步，选择剩余用户依次作为合法用户，重复上述第六步的过程，得到所用的用户平均认证结果。

[0059] 针对所有用户，测试本发明方法对智能手机用户身份进行认证的准确度。图5是本实施例智能手机用户的平均受试者工作特征(Receiver Operating Characteristic,ROC)曲线，横坐标是错误接受率(False-Acceptance Rate,FAR)，表示行身份认证时被判为合法用户的非法用户样本数占测试的非法用户样本总数的百分比，用来衡量非法用户被错误地判别为合法用户通过验证的概率；纵坐标是错误拒绝率(False-Rejection Rate,FRR)，表示进行身份认证时被判为非法用户的合法用户样本数占测试的合法用户样本总数的百分比，用来衡量合法用户被错误地判别为非法用户拒绝通过验证的概率。

[0060] 从图示的实验结果可以看出，本发明方法能够准确地对智能手机用户的身份进行认证。当FAR为8.32％时，FRR为3.75％；当FAR为2.14％时，FRR为7.28％；当FAR与FRR相等时，身份认证的平均等错误率为5.78％。上述结果验证了本发明的可行性和有效性，表明该方法可作为一种高效的智能设备使用者的身份安全认证技术。

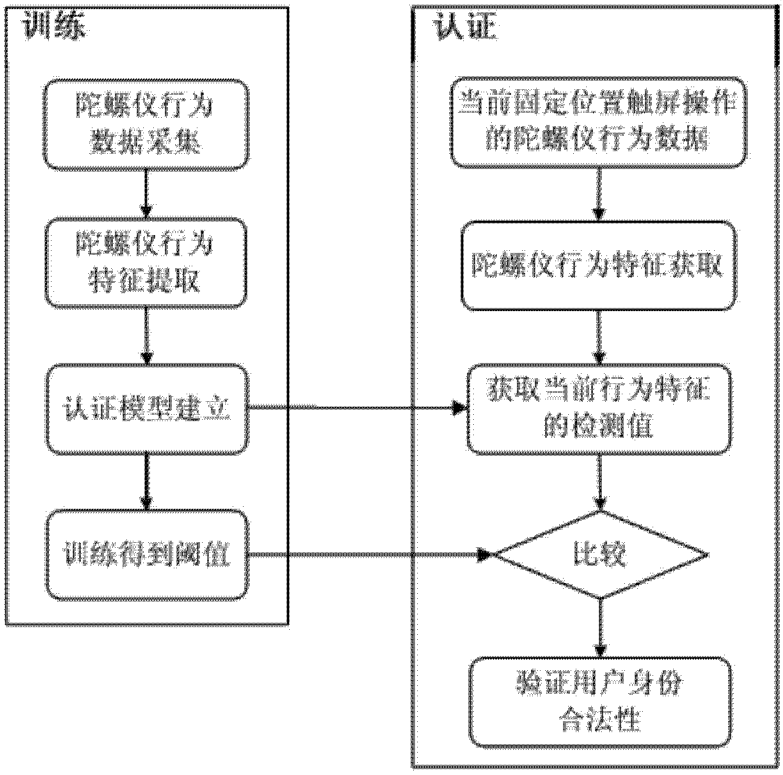

训练
陀螺仪行为数据采集
陀螺仪行为特征提取
认证模型建立
训练得到阈值
认证
当前固定位置触屏操作的陀螺仪行为数据
陀螺仪行为特征获取
获取当前行为特征的检测值
比较
验证用户身份合法性

图 1

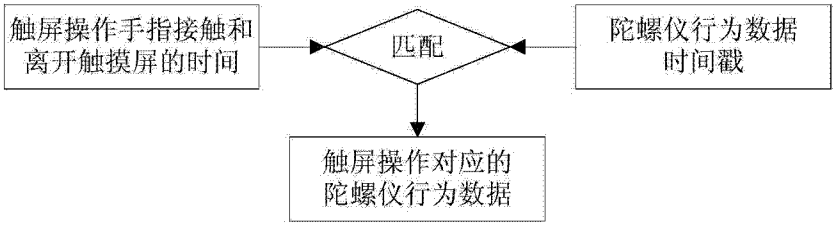

触屏操作手指接触和离开触摸屏的时间
匹配
陀螺仪行为数据时间戳
触屏操作对应的陀螺仪行为数据

图 2

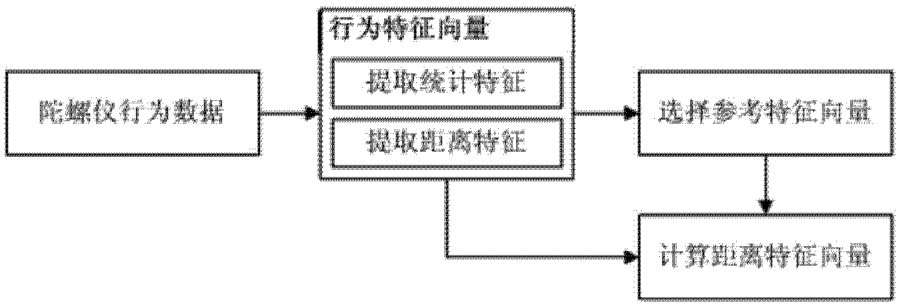

陀螺仪行为数据
行为特征向量
提取统计特征
提取距离特征
选择参考特征向量
计算距离特征向量

图 3

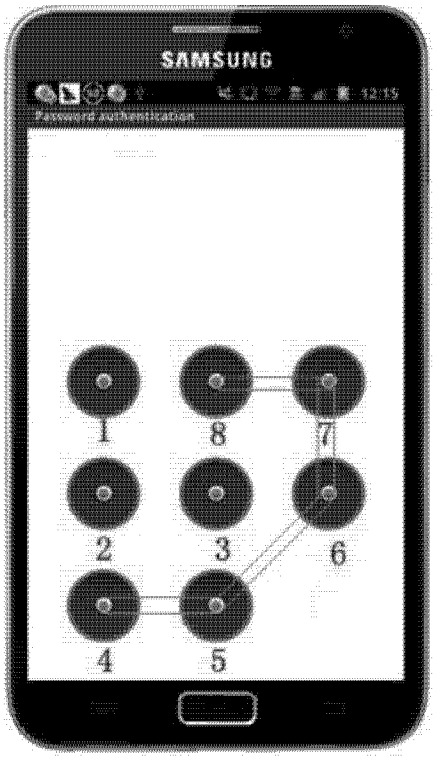


图 4

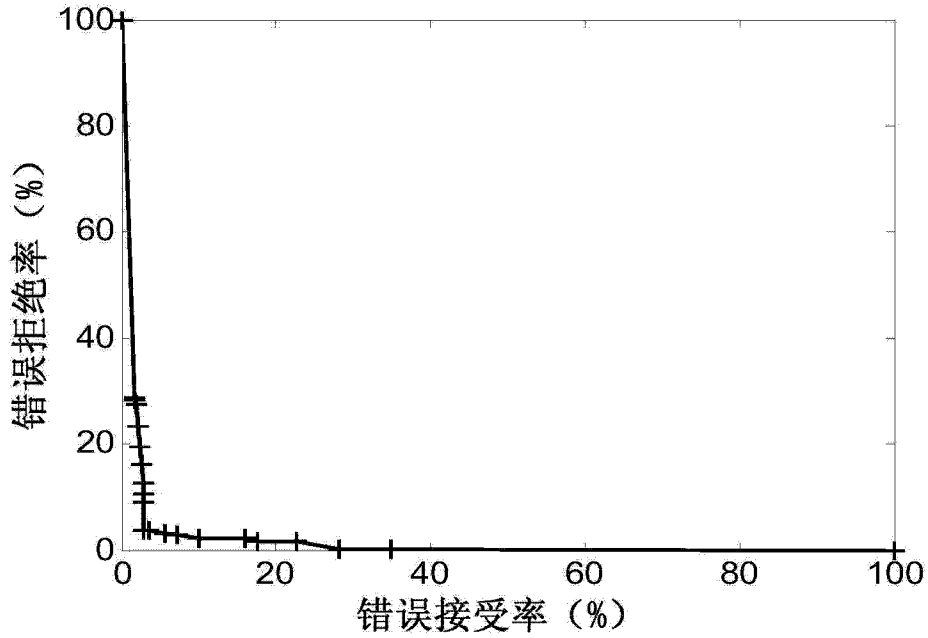


图 5