



(12)发明专利申请

(10)申请公布号 CN 109801072 A

(43)申请公布日 2019.05.24

(21)申请号 201910066500.8

(22)申请日 2019.01.24

(71)申请人 易保互联医疗信息科技(北京)有限公司

地址 100027 北京市朝阳区新源里16号14层2座12B06

(72)发明人 金以东 李雪莉 王语莫 周大胜

(74)专利代理机构 北京科石知识产权代理有限公司 11595

代理人 李艳霞

(51)Int.Cl.

G06Q 20/38(2012.01)

G06K 9/00(2006.01)

G06K 9/62(2006.01)

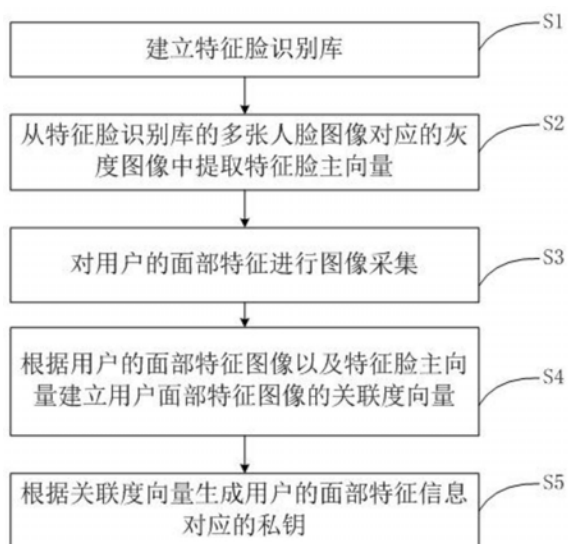
权利要求书2页 说明书9页 附图1页

(54)发明名称

基于面部特征的区块链电子钱包的私钥生成方法及系统

(57)摘要

本申请提供一种基于面部特征的区块链电子钱包的私钥生成方法及系统,私钥生成方法包括以下步骤:建立特征脸识别库;从特征脸识别库的多张人脸图像对应的灰度图像中提取特征脸主向量;对用户的面部特征进行图像采集;根据用户的面部特征图像以及特征脸主向量建立用户面部特征图像的关联度向量;根据关联度向量生成用户的面部特征信息对应的私钥。本申请基于强认证面部特征信息生成私钥,私钥与用户的面部特征信息关联性强,能够提升私钥的安全性,使私钥不会轻易被推算出具体的取值。另外,私钥不再需要存储,能够避免被盗用和违规使用的风险。当私钥丢失或忘记携带存储设备时也能够依据用户的面部特征信息进行重现。



1. 一种基于面部特征的区块链电子钱包的私钥生成方法,其特征在于,包括以下步骤:
建立特征脸识别库;
从特征脸识别库的多张人脸图像对应的灰度图像中提取特征脸主向量;
对用户的面部特征进行图像采集;
根据用户的面部特征图像以及特征脸主向量建立用户面部特征图像的关联度向量;
根据关联度向量生成用户的面部特征信息对应的私钥。
2. 根据权利要求1所述的私钥生成方法,其特征在于,所述步骤建立特征脸识别库的具体过程为:
随机采集U张不同的人脸图像;
对于各张人脸图像,均对应的将其转换为灰度图像,灰度图像的大小为m*n个像素;
将灰度图像的m*n个像素构成的矩阵转变为m*n维行向量;
将U张不同的人脸图像对应的行向量排列为矩阵A,矩阵A为U行m*n列的矩阵。
3. 根据权利要求2所述的私钥生成方法,其特征在于,所述步骤提取特征脸主向量的具体过程为:
对矩阵A中的每一列元素分别进行去中心化处理;
为去中心化处理后的矩阵建立协方差矩阵;
计算协方差矩阵的所有特征值以及各个特征值对应的特征向量;
对m*n个特征值进行排序,选取其中最大的多个特征值,并按照从大到小的顺序组成新的特征数组,同时将特征数组中各个特征值对应的特征向量组成新的特征向量矩阵;
计算去中心化处理后的矩阵在特征向量矩阵上的投影,得到特征脸主向量。
4. 根据权利要求3所述的私钥生成方法,其特征在于,所述步骤对矩阵A中的每一列元素分别进行去中心化处理的具体过程为:
计算每一列元素的平均值;

$$\mu_j = \frac{\sum_{k=1}^U a_{k,j}}{U}$$
 式中,k=1,2,3,...,U,j=1,2,3,...,m*n; μ_j 表示矩阵A中第j列元素的平均值;
将矩阵A中的每一元素均减去该元素所在列的平均值,得到去中心化处理后的矩阵。
5. 根据权利要求3所述的私钥生成方法,其特征在于,所述步骤根据用户的面部特征图像以及特征脸主向量建立用户面部特征图像的关联度向量的具体过程为:
将用户的面部特征图像转变为灰度图像,所述灰度图像的大小为m*n个像素;
将灰度图像的m*n个像素构成的矩阵转变为m*n维行向量z;
计算m*n维行向量z在特征向量矩阵P上的投影,得到该用户的特征脸主向量y:

$$y = z \times P,$$
 式中, $\times$ 表示矩阵乘法,该用户的特征脸主向量y表示1行h列的行向量;
计算用户面部特征图像的关联度向量x:

$$x = (DD^T)^{-1} D y^T,$$
 式中,T表示矩阵的转置。
6. 根据权利要求5所述的私钥生成方法,其特征在于,所述步骤根据关联度向量生成用

户的面部特征信息对应的私钥的具体过程为：

对关联度向量 x 中的每个元素计算其四舍五入后的整数 e_g ：

$$e_g = \text{round}(x_g \cdot 10^\tau), g = 1, 2, \dots, U,$$

式中， round 表示按四舍五入规则取整； τ 表示可调参数，其为非负整数；

按照预设顺序排列生成用户的面部特征信息对应的私钥。

7. 根据权利要求1~6任一项所述的私钥生成方法，其特征在于，所述步骤对用户的面部特征进行图像采集前，还包括以下步骤：利用活体认证方法确认为用户本人。

8. 一种基于面部特征的区块链电子钱包的私钥生成系统，其特征在于，包括：

识别库建立模块，用于根据随机采集的多张不同的人脸图像建立特征脸识别库；

提取模块，用于从特征脸识别库中的人脸图像对应的灰度图像中提取特征脸主向量；

图像采集模块，用于采集用户的面部特征图像。

关联度向量建立模块，用于根据用户的面部特征图像和特征脸主向量建立用户面部特征图像的关联度向量；

生成模块，用于根据关联度向量生成用户的面部特征信息对应的私钥。

9. 根据权利要求8所述的私钥生成系统，其特征在于，所述关联度向量建立模块包括：

矩阵转变模块，用于将用户的面部特征图像转变的灰度图像的 $m \times n$ 个像素构成的矩阵转变为 $m \times n$ 维行向量；

关联度向量计算模块，利用 $m \times n$ 维行向量在特征向量矩阵上的投影以及特征脸主向量计算得到用户面部特征图像的关联度向量。

10. 一种基于面部特征的区块链电子钱包的私钥生成装置，其特征在于，包括：

处理器，

所述处理器能够从区块链上调用智能合约，

所述智能合约包括计算机程序，

所述计算机程序在所述处理器上运行时，执行以下步骤：

建立特征脸识别库；

从特征脸识别库中的多张人脸图像对应的灰度图像中提取特征脸主向量；

对用户的面部特征进行图像采集；

根据用户的面部特征图像以及特征脸主向量建立用户面部特征图像的关联度向量；

根据关联度向量生成用户的面部特征信息对应的私钥。

11. 一种基于区块链的个人电子钱包，其特征在于，包括私钥，所述私钥由权利要求1~7任一项所述的私钥生成方法生成，所述私钥生成方法作为智能合约存储在区块链上。

基于面部特征的区块链电子钱包的私钥生成方法及系统

技术领域

[0001] 本申请属于信息安全技术领域,具体涉及一种基于面部特征的区块链电子钱包的私钥生成方法及系统。

背景技术

[0002] 基于区块链的电子钱包技术中,非对称加密技术对交易的安全性、可靠性有着至关重要的影响。非对称加密技术中,公钥与私钥通过加密算法生成,公钥用于加密、私钥用于解密。一般情况下,电子钱包用户的公钥与私钥在注册时生成,且保持不变。私钥由用户自身持有,不能透露给其他人,否则其交易的安全性将受到极大地威胁。

[0003] 现有技术中公钥与私钥基于加密算法的条件随机生成,并存储于某数据库或设备中。虽然私钥的存储环境可能是安全的、保密的,但是仍然不能完全避免私钥被窃取的风险。如果私钥存储在某一运营商的中心化数据库内,则还可能面临运营商违规查看用户私钥的风险。基于区块链的个人电子钱包的最大优势是去中心化的存储方式,如果私钥由运营商中心化储存,则不能充分发挥区块链的特点与优势。

[0004] 实际应用过程中,运营商通过采集用户的面部特征,与数据库或设备中记录的面部特征数据进行比对,生成核验结果。在用户通过验证后将其面部信息与对应的私钥直接进行关联。然而,私钥往往与用户的面部特征信息关联性弱,一旦私钥丢失或忘记携带存储端,则无法再现,只能重新生成私钥。另外,当用户存储私钥的手机、平板电脑等设备失窃时,用户的私钥将面临被盗用的风险。

[0005] 由上述可见,无论客户端进行存储还是运营商处进行存储,私钥都不能有效地避免被盗用的风险,也就无法避免交易安全受到的威胁。

发明内容

[0006] 为至少在一定程度上克服相关技术中存在的问题,本申请提供了一种基于面部特征的区块链电子钱包的私钥生成方法及系统。

[0007] 根据本申请实施例的第一方面,本申请提供了一种基于面部特征的区块链电子钱包的私钥生成方法,其包括以下步骤:

[0008] 建立特征脸识别库;

[0009] 从特征脸识别库的多张人脸图像对应的灰度图像中提取特征脸主向量;

[0010] 对用户的面部特征进行图像采集;

[0011] 根据用户的面部特征图像以及特征脸主向量建立用户面部特征图像的关联度向量;

[0012] 根据关联度向量生成用户的面部特征信息对应的私钥。

[0013] 上述私钥生成方法,所述步骤建立特征脸识别库的具体过程为:

[0014] 随机采集U张不同的人脸图像;

[0015] 对于各张人脸图像,均对应的将其转换为灰度图像,灰度图像的大小为 $m \times n$ 个像

素；

[0016] 将灰度图像的 $m \times n$ 个像素构成的矩阵转变为 $m \times n$ 维行向量；

[0017] 将 U 张不同的人脸图像对应的行向量排列为矩阵 A ，矩阵 A 为 U 行 $m \times n$ 列的矩阵。

[0018] 上述私钥生成方法，所述步骤提取特征脸主向量的具体过程为：

[0019] 对矩阵 A 中的每一列元素分别进行去中心化处理；

[0020] 为去中心化处理后的矩阵建立协方差矩阵；

[0021] 计算协方差矩阵的所有特征值以及各个特征值对应的特征向量；

[0022] 对 $m \times n$ 个特征值进行排序，选取其中最大的多个特征值，并按照从大到小的顺序组成新的特征数组，同时将特征数组中各个特征值对应的特征向量组成新的特征向量矩阵；

[0023] 计算去中心化处理后的矩阵在特征向量矩阵上的投影，得到特征脸主向量。

[0024] 上述私钥生成方法，所述步骤对矩阵 A 中的每一列元素分别进行去中心化处理的具体过程为：

[0025] 计算每一列元素的平均值；

$$[0026] \quad \mu_j = \frac{\sum_{k=1}^U a_{k,j}}{U},$$

[0027] 式中， $k=1, 2, 3, \dots, U$ ， $j=1, 2, 3, \dots, m \times n$ ； μ_j 表示矩阵 A 中第 j 列元素的平均值；

[0028] 将矩阵 A 中的每一元素均减去该元素所在列的平均值，得到去中心化处理后的矩阵。

[0029] 上述私钥生成方法，所述步骤根据用户的面部特征图像以及特征脸主向量建立用户面部特征图像的关联度向量的具体过程为：

[0030] 将用户的面部特征图像转变为灰度图像，所述灰度图像的大小为 $m \times n$ 个像素；

[0031] 将灰度图像的 $m \times n$ 个像素构成的矩阵转变为 $m \times n$ 维行向量 z ；

[0032] 计算 $m \times n$ 维行向量 z 在特征向量矩阵 P 上的投影，得到该用户的特征脸主向量 y ：

$$[0033] \quad y = z \times P,$$

[0034] 式中， $\times$ 表示矩阵乘法，该用户的特征脸主向量 y 表示1行 h 列的行向量；

[0035] 计算用户面部特征图像的关联度向量 x ：

$$[0036] \quad x = (DD^T)^{-1} D y^T,$$

[0037] 式中， T 表示矩阵的转置。

[0038] 上述私钥生成方法，所述步骤根据关联度向量生成用户的面部特征信息对应的私钥的具体过程为：

[0039] 对关联度向量 x 中的每个元素计算其四舍五入后的整数 e_g ：

$$[0040] \quad e_g = \text{round}(x_g \cdot 10^t), g=1, 2, \dots, U,$$

[0041] 式中， round 表示按四舍五入规则取整； t 表示可调参数，其为非负整数；

[0042] 按照预设顺序排列生成用户的面部特征信息对应的私钥。

[0043] 上述私钥生成方法，所述步骤对用户的面部特征进行图像采集前，还包括以下步骤：利用活体认证方法确认为用户本人。

[0044] 根据本申请实施例的第二方面，本申请提供了一种基于面部特征的区块链电子钱包的私钥生成系统，其包括：

[0045] 识别库建立模块，用于根据随机采集的多张不同的人脸图像建立特征脸识别库；

- [0046] 提取模块,用于从特征脸识别库中的人脸图像对应的灰度图像中提取特征脸主向量;
- [0047] 图像采集模块,用于采集用户的面部特征图像。
- [0048] 关联度向量建立模块,用于根据用户的面部特征图像和特征脸主向量建立用户面部特征图像的关联度向量;
- [0049] 生成模块,用于根据关联度向量生成用户的面部特征信息对应的私钥。
- [0050] 上述私钥生成系统,所述关联度向量建立模块包括:
- [0051] 矩阵转变模块,用于将用户的面部特征图像转变的灰度图像的 $m \times n$ 个像素构成的矩阵转变为 $m \times n$ 维行向量;
- [0052] 关联度向量计算模块,利用 $m \times n$ 维行向量在特征向量矩阵上的投影以及特征脸主向量计算得到用户面部特征图像的关联度向量。
- [0053] 根据本申请实施例的第三方面,本申请提供了一种基于面部特征的区块链电子钱包的私钥生成装置,其包括:
- [0054] 处理器,
- [0055] 所述处理器能够从区块链上调用智能合约,
- [0056] 所述智能合约包括计算机程序,
- [0057] 所述计算机程序在所述处理器上运行时,执行以下步骤:
- [0058] 建立特征脸识别库;
- [0059] 从特征脸识别库中的多张人脸图像对应的灰度图像中提取特征脸主向量;
- [0060] 对用户的面部特征进行图像采集;
- [0061] 根据用户的面部特征图像以及特征脸主向量建立用户面部特征图像的关联度向量;
- [0062] 根据关联度向量生成用户的面部特征信息对应的私钥。
- [0063] 根据本申请实施例的第四方面,本申请提供了一种基于区块链的个人电子钱包,其包括私钥,所述私钥由上述任一项所述的私钥生成方法生成,所述私钥生成方法作为智能合约存储在区块链上。
- [0064] 根据本申请的上述具体实施方式可知,至少具有以下有益效果:本申请私钥生成方法基于强认证生物特征信息生成私钥,私钥与用户的面部特征信息关联性强,能够提升私钥的安全性,使私钥不会轻易被推算出具体的取值。本申请生成的私钥用于基于区块链的个人电子钱包中,私钥不再需要存储,能够避免被盗用和违规使用的风险。本申请能够强化区块链个人电子钱包的去中心化特性。不需要存储介质,当私钥丢失或忘记携带存储设备时也能够依据用户的面部特征信息进行重现。
- [0065] 应了解的是,上述一般描述及以下具体实施方式仅为示例性及阐释性的,其并不能限制本申请所欲主张的范围。

附图说明

- [0066] 下面的所附附图是本申请的说明书的一部分,其示出了本申请的实施例,所附附图与说明书的描述一起用来说明本申请的原理。
- [0067] 图1为本申请具体实施方式提供的基于面部特征的区块链电子钱包的私钥生成方

法的流程图。

[0068] 图2为本申请具体实施方式提供的一种基于面部特征的区块链电子钱包的私钥生成系统的结构示意图。

[0069] 图3为本申请具体实施方式提供的一种基于区块链的个人电子钱包的应用状态示意图。

具体实施方式

[0070] 为使本申请实施例的目的、技术方案和优点更加清楚明白,下面将以附图及详细叙述清楚说明本申请所揭示内容的精神,任何所属技术领域技术人员在了解本申请内容的实施例后,当可由本申请内容所教示的技术,加以改变及修饰,其并不脱离本申请内容的精神与范围。

[0071] 本申请的示意性实施例及其说明用于解释本申请,但并不作为对本申请的限定。另外,在附图及实施方式中所使用相同或类似标号的元件/构件是用来代表相同或类似部分。

[0072] 关于本文中所使用的“第一”、“第二”、…等,并非特别指称次序或顺位的意思,也非用以限定本申请,其仅为了区别以相同技术用语描述的元件或操作。

[0073] 关于本文中所使用的方向用语,例如:上、下、左、右、前或后等,仅是参考附图的方向。因此,使用的方向用语是用来说明并非用来限制本创作。

[0074] 关于本文中所使用的“包含”、“包括”、“具有”、“含有”等等,均为开放性的用语,即意指包含但不限于。

[0075] 关于本文中所使用的“及/或”,包括所述事物的任一或全部组合。

[0076] 关于本文中的“多个”包括“两个”及“两个以上”;关于本文中的“多组”包括“两组”及“两组以上”。

[0077] 关于本文中所使用的用语“大致”、“约”等,用以修饰任何可以细微变化的数量或误差,但这些微变化或误差并不会改变其本质。一般而言,此类用语所修饰的细微变化或误差的范围在部分实施例中可为20%,在部分实施例中可为10%,在部分实施例中可为5%或是其他数值。本领域技术人员应当了解,前述提及的数值可依实际需求而调整,并不以此为限。

[0078] 某些用以描述本申请的用词将于下或在此说明书的别处讨论,以提供本领域技术人员在有关本申请的描述上额外的引导。

[0079] 实施例一

[0080] 图1是本申请一实施例提供的一种基于面部特征的区块链电子钱包的私钥生成方法的流程图。如图1所示,基于面部特征的区块链电子钱包的私钥生成方法包括以下步骤:

[0081] S1、建立特征脸识别库,其具体过程为:

[0082] S11、随机采集U张不同的人脸图像。

[0083] S12、对于各张人脸图像,均对应地将其转换为灰度图像,灰度图像的大小为 $m \times n$ 个像素。其中,U的取值可以根据实际应用场景进行设定; m 表示图像像素的行数, n 表示图像像素的列数。

[0084] S13、将灰度图像的 $m \times n$ 个像素构成的矩阵转变为 $m \times n$ 维行向量 a 。

[0085] S14、将U张不同的人脸图像对应的行向量a排列为矩阵A,即矩阵A为U行m*n列的矩阵;矩阵A的形式可以为:

$$[0086] \quad A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m*n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m*n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{U,1} & a_{U,2} & \cdots & a_{U,m*n} \end{bmatrix}。$$

[0087] 通常情况下,m*n大于U,例如大小为100*100的图像共有10000个像素,而特征脸识别库的数据量即U为数十至数百张。

[0088] S2、从特征脸识别库的U张人脸图像对应的灰度图像中提取特征脸主向量,其具体过程为:

[0089] S21、对矩阵A中的每一列元素分别进行去中心化处理,其过程为:

[0090] 采用以下公式计算每一列元素的平均值:

$$[0091] \quad \mu_j = \frac{\sum_{k=1}^U a_{k,j}}{U}$$

[0092] 式中,k=1,2,3,...,U,j=1,2,3,...,m*n; μ_j 表示矩阵A中第j列元素的平均值。

[0093] 将矩阵A中的每一元素均减去该元素所在列的平均值,得到去中心化处理后的矩阵。

[0094] S22、为去中心化处理后的矩阵建立协方差矩阵C,其中协方差矩阵C的形式可以为:

$$[0095] \quad C = \begin{bmatrix} \text{cov}(b_1, b_1) & \text{cov}(b_1, b_2) & \cdots & \text{cov}(b_1, b_{m*n}) \\ \text{cov}(b_2, b_1) & \text{cov}(b_2, b_2) & \cdots & \text{cov}(b_2, b_{m*n}) \\ \vdots & \vdots & \ddots & \vdots \\ \text{cov}(b_{m*n}, b_1) & \text{cov}(b_{m*n}, b_2) & \cdots & \text{cov}(b_{m*n}, b_{m*n}) \end{bmatrix}$$

[0096] 其中,cov表示协方差函数,

$$[0097] \quad \text{cov}(b_i, b_j) = \frac{\sum_{k=1}^U (b_{i,k} - \mu_i)(b_{j,k} - \mu_j)}{U-1}$$

[0098] 式中, b_i 表示去中心化处理后的矩阵的第i列的列向量, b_j 表示去中心化处理后的矩阵的第j列的列向量。

[0099] S23、计算协方差矩阵C的所有特征值 $\lambda_1, \lambda_2, \cdots, \lambda_{m*n}$ 以及各个特征值对应的特征向量 $p_1, p_2, \cdots, p_{m*n}$ 。

[0100] 可以理解的是,由于协方差矩阵C是m*n阶方阵,因此协方差矩阵C有m*n组特征值和特征向量。

[0101] S24、对m*n个特征值进行排序,选取其中最大的h个特征值,并按照从大到小的顺序组成新的特征数组 Λ ,同时将特征数组 Λ 中各个特征值对应的特征向量组成新的特征向量矩阵P。

[0102] 其中,特征数组 Λ 可以为:

$$[0103] \quad \Lambda = [\lambda_1, \lambda_2, \cdots, \lambda_h]。$$

[0104] 特征向量矩阵P可以为:

$$[0105] \quad P = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{h,1} \\ p_{1,2} & p_{2,2} & \cdots & p_{h,2} \\ \vdots & \vdots & \ddots & \vdots \\ p_{1,m*n} & p_{2,m*n} & \cdots & p_{h,m*n} \end{bmatrix} \circ$$

[0106] S25、计算去中心化处理后的矩阵在特征向量矩阵P上的投影,得到特征脸主向量D,即:

$$[0107] \quad D = A \times P$$

[0108] 式中, $\times$ 表示矩阵乘法,特征脸主向量D表示U行h列的矩阵;特征脸主向量D的形式可以为:

$$[0109] \quad D = \begin{bmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,h} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,h} \\ \vdots & \vdots & \ddots & \vdots \\ d_{U,1} & d_{U,2} & \cdots & d_{U,h} \end{bmatrix} \circ$$

[0110] S3、对用户的面部特征进行图像采集。

[0111] 为保证采集的面部图像为用户本人的图像,在进行用户面部特征的图像采集之前,先通过活体认证来确认是由用户本人进行的操作。

[0112] 具体地,活体认证方法采用现有的人脸识别技术,通过检测用户的眨眼、张嘴、摇头或点头等组合动作来验证用户是否为真实活体本人操作。

[0113] S4、根据用户的面部特征图像以及特征脸主向量建立用户面部特征图像的关联度向量,其具体过程为:

[0114] S41、将用户的面部特征图像转变为灰度图像。其中,灰度图像的大小为m*n个像素。

[0115] S42、将灰度图像的m*n个像素构成的矩阵转变为m*n维行向量z。

[0116] S43、计算m*n维行向量z在特征向量矩阵P上的投影,得到该用户的特征脸主向量y,即:

$$[0117] \quad y = z \times P$$

[0118] 式中, $\times$ 表示矩阵乘法,该用户的特征脸主向量y表示1行h列的行向量。

[0119] S44、计算用户面部特征图像的关联度向量x,即:

$$[0120] \quad x = (DD^T)^{-1}Dy^T,$$

[0121] 式中,T表示矩阵的转置。

[0122] 关联度向量x表示U行1列的列向量,其形式可以为:

$$[0123] \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_U \end{bmatrix} \circ$$

[0124] S5、根据关联度向量x生成用户的面部特征信息对应的私钥,其具体过程为:

[0125] S51、对关联度向量 x 中的每个元素计算其四舍五入后的整数 e_g ,具体地,可以采用以下公式得到:

[0126] $e_g = \text{round}(x_g \cdot 10^\tau)$, $g=1, 2, \dots, U$,

[0127] 式中,round表示按四舍五入规则取整; τ 表示可调参数,其为非负整数,可以取值为1,2,……。

[0128] S52、按照预设顺序排列生成用户的面部特征信息对应的私钥。

[0129] 具体地,当 $x = [1.25, 10.05, 0.03, \dots, 3.54]^T$, T 表示矩阵的转置, $\tau=1$ 时,生成的用户面部特征信息对应的私钥为:

[0130] 131000……35。

[0131] 本申请私钥生成方法基于强认证生物特征信息生成私钥,私钥与用户的面部特征信息关联性强,能够提升私钥的安全性,使私钥不会轻易被推算出具体的取值。

[0132] 实施例二

[0133] 如图2所示,在以上私钥生成方法的基础上,本申请还提供了一种基于面部特征的区块链电子钱包的私钥生成系统,其包括识别库建立模块1、提取模块2、图像采集模块3、关联度向量建立模块4和生成模块5。

[0134] 其中,识别库建立模块1用于根据随机采集的多张不同的人脸图像建立特征脸识别库。

[0135] 提取模块2用于从特征脸识别库中的人脸图像对应的灰度图像中提取特征脸主向量。

[0136] 图像采集模块3用于采集用户的面部特征图像。

[0137] 关联度向量建立模块4用于根据用户的面部特征图像和特征脸主向量建立用户面部特征图像的关联度向量。

[0138] 生成模块5用于根据关联度向量生成用户的面部特征信息对应的私钥。

[0139] 具体地,识别库建立模块1包括随机采集模块、灰度转换模块和矩阵构建模块。其中,随机采集模块用于随机采集 U 张不同的人脸图像。灰度转换模块用于将 U 张不同的人脸图像转换为灰度图像,灰度图像的大小用 $m \times n$ 个像素表示。矩阵构建模块用于将 U 张不同的人脸图像对应的灰度图像的像素构成 U 行 $m \times n$ 列的矩阵 A 。

[0140] 具体地,提取模块2包括去中心化模块、协方差矩阵建立模块、特征值和特征向量计算模块、特征向量矩阵构建模块和特征脸主向量计算模块。

[0141] 其中,去中心化模块通过将矩阵 A 中的每一元素均减去该元素所在列的平均值,得到去中心化处理后的矩阵。协方差矩阵建立模块通过计算去中心化处理后的矩阵中各列向量之间的协方差,建立协方差矩阵。特征值和特征向量计算模块用于计算协方差矩阵的所有特征值及其对应的特征向量。特征向量矩阵构建模块利用协方差矩阵的所有特征值中按序排列的最大的多个特征值所对应的特征向量组成特征向量矩阵。

[0142] 特征脸主向量计算模块通过计算去中心化处理后的矩阵在特征向量矩阵上的投影,得到特征脸主向量。

[0143] 具体地,关联度向量建立模块4包括矩阵转变模块和关联度向量计算模块。其中,矩阵转变模块用于将用户的面部特征图像转变的灰度图像的 $m \times n$ 个像素构成的矩阵转变为 $m \times n$ 维行向量。关联度向量计算模块利用 $m \times n$ 维行向量在特征向量矩阵上的投影以及特征脸

主向量计算得到用户面部特征图像的关联度向量。

[0144] 具体地,生成模块5包括取整模块和排序生成模块。其中,取整模块用于对关联度向量中的每个元素计算其四舍五入后的整数。排序生成模块用于按照预设顺序排列生成用户的面部特征信息对应的私钥。

[0145] 需要说明的是:上述实施例提供的私钥生成系统仅以上述各程序模块的划分进行举例说明,实际应用中,可以根据需要而将上述处理分配由不同的程序模块完成,即将私钥生成系统内部结构划分成不同的程序模块,以完成以上描述的全部或者部分处理。另外,上述实施例提供的私钥生成系统与私钥生成方法实施例属于同一构思,其具体实现过程详见方法实施例,这里不再赘述。

[0146] 本申请私钥生成系统基于强认证生物特征信息生成私钥,私钥与用户的面部特征信息关联性强,能够提升私钥的安全性,使私钥不会轻易被推算出具体的取值。

[0147] 基于上述私钥生成系统中各模块的硬件实现,为了实现本申请实施例提供的私钥生成方法,本申请实施例还提供了一种基于面部特征的区块链电子钱包的私钥生成装置,其包括:处理器和用于存储能够在处理器上运行的计算机程序的存储器。其中所述处理器用于运行所述计算机程序时,执行如下步骤:

[0148] 建立特征脸识别库;

[0149] 从特征脸识别库中的多张人脸图像对应的灰度图像中提取特征脸主向量;

[0150] 对用户的面部特征进行图像采集;

[0151] 根据用户的面部特征图像以及特征脸主向量建立用户面部特征图像的关联度向量;

[0152] 根据关联度向量生成用户的面部特征信息对应的私钥。

[0153] 在示例性实施例中,本申请实施例还提供了一种计算机存储介质,是计算机可读存储介质,例如,包括计算机程序的存储器,上述计算机程序可由私钥生成系统中的处理器执行,以完成上述私钥生成方法中的所述步骤。计算机可读存储介质可以是磁性随机存取存储器(FRAM,ferromagnetic random access memory)、只读存储器(ROM,Read Only Memory)、可编程只读存储器(PROM,Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM,Erasable Programmable Read-OnlyMemory)、电可擦除可编程只读存储器(EEPROM,Electrically Erasable Programmable Read-Only Memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM,Compact Disc Read-OnlyMemory)等存储器。

[0154] 实施例三

[0155] 如图3所示,本申请还提供了一种基于区块链的个人电子钱包,其包括上述任一私钥生成方法生成的私钥,私钥生成方法作为智能合约存储在区块链上。当用户需要获取私钥时,只需要从区块链上调用智能合约,利用私钥生成方法即可重新生成用户面部特征对应的私钥。

[0156] 采用本申请基于面部特征的区块链电子钱包的私钥生成方法,私钥不再需要记录,能够避免被盗用和违规使用的风险。该方法能够强化区块链个人电子钱包的去中心化特性。不需要存储介质,当私钥丢失或忘记携带存储设备时也能够依据用户的面部特征信息进行重现。另外,基于强认证生物特征的私钥生成方法能够有效地提升私钥的安全性,使

私钥不能轻易被推算出具体的取值。

[0157] 以上所述仅为本申请示意性的具体实施方式,在不脱离本申请的构思和原则的前提下,任何本领域的技术人员所做出的等同变化与修改,均应属于本申请保护的范围。

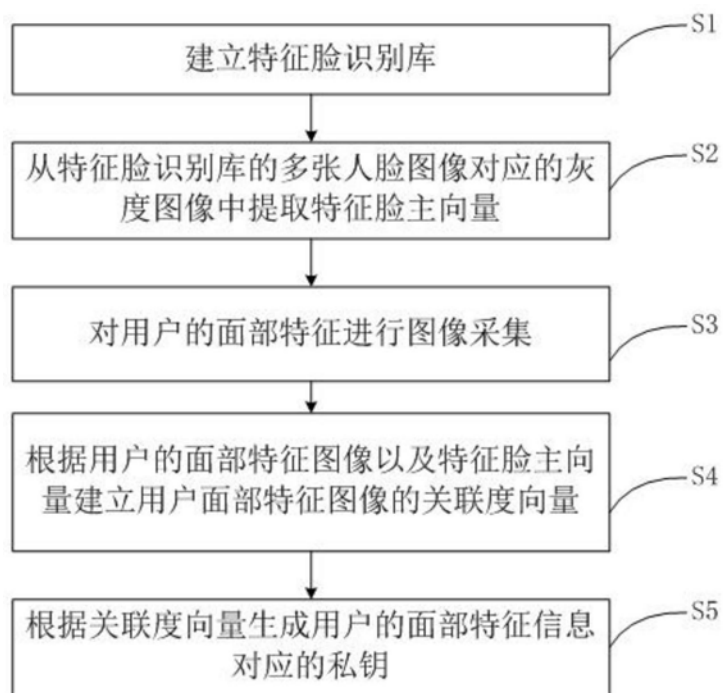


图1



图2

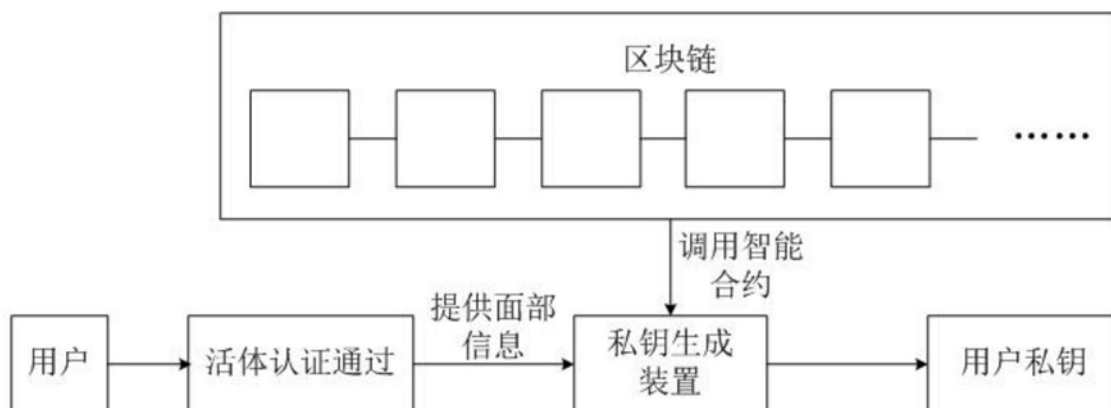


图3