刷脸支付的方法和装置

技术领域

[01]本说明书一个或多个实施例涉及电子信息技术，尤其涉及刷脸支付的方法和装置。

背景技术

[02]刷脸支付是一种以人脸识别为核心的新型支付方式。刷脸支付的过程非常简单，用户不需要带钱包、银行卡或手机，支付时只需要用户面对POS（销售点）机的屏幕，刷脸支付系统就会自动将用户面部信息与该用户的个人账户相关联，并完成针对该用户的交易扣款，整个交易过程十分便捷。

[03]但是，目前的刷脸支付过程中，用户需要等到刷脸支付的交易扣款成功后，才能离开，增加了用户的等待时间。因此，希望能有改进的方案，能够减少用户在刷脸支付过程中的等待时间。

发明内容

[04]本说明书一个或多个实施例描述了刷脸支付的方法和装置，能够减少用户的等待时间。

[05]根据第一方面，提供了一种刷脸支付的方法，包括：检测到刷脸支付触发事件；获取人脸图像；根据获取的所述人脸图像进行用户的身份核验；在所述用户的身份核验通过后，获取所述用户的风险数据；利用所述用户的风险数据判断交易的支付风险是否可控，如果可控，通知用户可离开。

[06]在本说明书的一个实施例中，所述检测到刷脸支付触发事件包括如下中的任一项：检测到刷脸机具的屏幕上出现人脸；检测到对刷脸支付按钮的点击输入，该刷脸支付按钮位于刷脸机具的屏幕上；检测到通过物理键盘输入的对应于刷脸支付的按键操作；检测到人脸的眼部注视刷脸机具的屏幕；检测到刷脸机具的屏幕上出现对应于刷脸支付的人体动作；检测到对应于刷脸支付的语音口令。

[07]在本说明书的一个实施例中，在所述获取人脸图像之后，并在所述根据获取的人脸图像进行用户的身份核验之前，进一步执行如下中的任一项：根据所获取的人脸图像，进行注意力识别，如果确定注意力在所述刷脸机具的屏幕上，则继续执行所述根据获取

的所述人脸图像进行用户的身份核验；判断当前是否获取了至少两个人脸图像，如果是，则计算每一个人脸图像对应的人脸相对于所述刷脸机具的屏幕的空间位置数据，利用计算出的空间位置数据计算每一个人脸图像对应的概率，将概率值最大的人脸图像确定为所述用户的人脸图像，并根据该用户的人脸图像进行所述用户的身份核验；检测刷脸机具的屏幕上是否出现人体躯干，如果是，则判断该人体躯干与获取的人脸图像是否属于同一个用户，如果属于，则继续执行所述根据获取的所述人脸图像进行用户的身份核验。

[08]在本说明书的一个实施例中，所述根据获取的所述人脸图像进行所述用户的身份核验，包括：根据所获取的所述人脸图像进行活体检测；如果所述活体检测通过，则根据所获取的所述人脸图像进行人脸识别，判断能否识别出对应于所述人脸图像的用户身份，如果能，则所述用户的身份核验通过。

[09]在本说明书的一个实施例中，所述获取所述用户的风险数据包括：获取 N 个维度的用户风险数据；其中，N 为正整数；以及对每一个维度的用户风险数据均进行归一化处理，得到该维度的用户风险向量；则，所述利用所述风险数据判断交易的支付风险是否可控，包括：利用如下计算式，计算用户风险值：

$$R^u(X^u)=\left(\prod_{n=1}^{N}x_n^u\right)^{\frac{1}{aN}}，\ 其中0\le x_n^u\le 1，\ 常量a>1$$

[10]其中，$R^u(X^u)$表征所述用户风险值，x_n^u表征第 n 个维度的用户风险向量，n 为 1 至 N 中的任意一个整数；判断所述用户风险值是否大于第一预定值，如果是，则确定所述交易的支付风险可控。

[11]在本说明书的一个实施例中，在所述通知所述用户可离开之前，进一步包括：获取刷脸机具的风险数据；利用所述刷脸机具的风险数据判断交易的支付风险是否可控，如果是，则继续执行所述通知所述用户可离开。

[12]在本说明书的一个实施例中，所述获取刷脸机具的风险数据，包括：获取 M 个维度的刷脸机具风险数据；其中，M 为正整数；以及对每一个维度的刷脸机具风险数据均进行归一化处理，得到该维度的刷脸机具风险向量；则，所述利用所述刷脸机具的风险数据判断交易的支付风险是否可控，包括：利用如下计算式，计算机具风险值：

$$R^d(X^d)=\prod_{m=1}^{M}x_m^d，$$

[13]其中，$R^d(X^d)$表征所述机具风险值，x_m^d表征第 m 个维度的机具风险向量，x_m^d的值

为 0 或 1，m 为 1 至 M 中的任意一个整数；判断所述机具风险值是否为 1，如果是，则确定所述交易的支付风险可控。

[14]在本说明书的一个实施例中，所述刷脸机具的风险数据包括如下中的任一项：所述刷脸机具的软件环境的风险数据、所述刷脸机具的硬件环境的风险数据以及通信网络风险数据。

[15]在本说明书的一个实施例中，在所述通知所述用户可离开之前，进一步包括：获取商户的风险数据；利用所述商户的风险数据判断交易的支付风险是否可控，如果是，则继续执行所述通知所述用户可离开。

[16]在本说明书的一个实施例中，所述获取商户的风险数据，包括：获取 I 个维度的商户风险数据；其中，I 为正整数；以及对每一个维度的商户风险数据均进行归一化处理，得到该维度的商户风险向量；则，所述利用所述商户的风险数据判断交易的支付风险是否可控，包括：利用如下计算式，计算商户风险值：

$$R^m(X^m)=\left(\prod_{i=1}^{I}x_i^m\right)^{\frac{b}{I}}，\ 其中0\le x_i^m\le 1，\ 常量b>1$$

[17]其中，$R^m(X^m)$表征所述商户风险值，x_i^m表征第 i 个维度的商户风险向量，i 为 1 至 I 中的任意一个整数；判断所述商户风险值是否大于第二预定值，如果是，则确定所述交易的支付风险可控。

[18]在本说明书的一个实施例中，所述商户的风险数据包括如下中的任一项：商户的历史行为数据、所述用户的信用状态数据、所述商户的服务等级数据。

[19]在本说明书的一个实施例中，所述用户的风险数据包括如下中的任一项：所述用户的历史行为数据、所述用户的消费能力统计数据、所述用户的信用状态数据以及所述用户的芝麻信用分数。

[20]在本说明书的一个实施例中，在利用所述风险数据判断出交易的支付风险可控之后，进一步包括：利用所述用户的账户信息进行扣款处理；如果扣款不成功，则从预先设立的刷脸付资金池的账户中进行扣款；和/或，在利用所述风险数据判断出交易的支付风险不可控之后，进一步包括：利用所述用户的账户信息进行扣款处理，如果扣款不成功，则通知用户扣款失败，如果扣款成功，则通知用户可离开。

[21]根据第二方面，提供了一种刷脸支付的装置，包括：刷脸支付启动模块，配置为在

检测到刷脸支付触发事件后，获取人脸图像；身份核验模块，配置为根据获取的所述人脸图像进行用户的身份核验；风险控制模块，配置为在所述用户的身份核验通过后，获取所述用户的风险数据；利用所述用户的风险数据判断交易的支付风险是否可控；通知模块，配置为在所述风险控制模块判断出交易的支付风险可控之后，通知所述用户可离开。

[22]在本说明书的一个实施例中，所述刷脸支付启动模块被配置为在检测到如下中的任一项时，确定检测到刷脸支付触发事件：检测到刷脸机具的屏幕上出现人脸；检测到对刷脸支付按钮的点击输入，该刷脸支付按钮位于刷脸机具的屏幕上；检测到通过物理键盘输入的对应于刷脸支付的按键操作；检测到人脸的眼部注视刷脸机具的屏幕；检测到刷脸机具的屏幕上出现对应于刷脸支付的人体动作；检测到对应于刷脸支付的语音口令。

[23]在本说明书的一个实施例中，进一步包括：支付确认模块；所述支付确认模块被配置为执行如下中的任一项处理：根据所获取的人脸图像，进行注意力识别，如果确定注意力在所述刷脸机具的屏幕上，则触发所述身份核验模块执行所述根据获取的所述人脸图像进行用户的身份核验；判断当前是否获取了至少两个人脸图像，如果是，则计算每一个人脸图像对应的人脸相对于所述刷脸机具的屏幕的空间位置数据，利用计算出的空间位置数据计算每一个人脸对象对应的概率，将概率值最大的人脸图像确定为所述用户的人脸图像，并触发所述身份核验模块执行根据获取的所述用户的人脸图像进行用户的身份核验；检测刷脸机具的屏幕上是否出现人体躯干，如果是，则判断该人体躯干与获取的人脸图像是否属于同一个用户，如果属于，则触发所述身份核验模块执行所述根据获取的所述人脸图像进行用户的身份核验。

[24]在本说明书的一个实施例中，所述风险控制模块被配置为执行如下处理：获取 N 个维度的用户风险数据；其中，N 为正整数；以及对每一个维度的用户风险数据均进行归一化处理，得到该维度的用户风险向量；则，所述利用所述风险数据判断交易的支付风险是否可控，包括：利用如下计算式，计算用户风险值：

$$R^u(X^u)=\left(\prod_{n=1}^{N}x_n^u\right)^{\frac{1}{aN}}，\ 其中0\le x_n^u\le 1，\ 常量a>1$$

[25]其中，$R^u(X^u)$表征所述用户风险值，x_n^u表征第 n 个维度的用户风险向量，n 为 1 至 N 中的任意一个整数；判断所述用户风险值是否大于第一预定值，如果是，则确定所述交易的支付风险可控。

[26]在本说明书的一个实施例中，所述风险控制模块进一步被配置为执行如下处理：获取刷脸机具的风险数据；利用所述刷脸机具的风险数据判断交易的支付风险是否可控。

[27]在本说明书的一个实施例中，所述风险控制模块被配置为执行如下处理：获取 M 个维度的刷脸机具风险数据；其中，M 为正整数；以及对每一个维度的刷脸机具风险数据均进行归一化处理，得到该维度的刷脸机具风险向量；则，所述利用所述刷脸机具的风险数据判断交易的支付风险是否可控，包括：利用如下计算式，计算机具风险值：

$$R^d(X^d) = \prod_{m=1}^{M} x_m^d ,$$

[28]其中，$R^d(X^d)$表征所述机具风险值，x_m^d表征第 m 个维度的机具风险向量，x_m^d的值为 0 或 1，m 为 1 至 M 中的任意一个整数；判断所述机具风险值是否为 1，如果是，则确定所述交易的支付风险可控。

[29]在本说明书的一个实施例中，所述刷脸机具的风险数据包括如下中的任一项：所述刷脸机具的软件环境的风险数据、所述刷脸机具的硬件环境的风险数据以及通信网络风险数据。

[30]在本说明书的一个实施例中，所述风险控制模块进一步被配置为执行如下处理：获取商户的风险数据；利用所述商户的风险数据判断交易的支付风险是否可控，如果是，则继续执行所述通知所述用户可离开。

[31]在本说明书的一个实施例中，所述风险控制模块被配置为执行如下处理：所述获取商户的风险数据，包括：获取 I 个维度的商户风险数据；其中，I 为正整数；以及对每一个维度的商户风险数据均进行归一化处理，得到该维度的商户风险向量；则，所述利用所述商户的风险数据判断交易的支付风险是否可控，包括：利用如下计算式，计算商户风险值：

$$R^m(X^m) = \left(\prod_{i=1}^{I} x_i^m\right)^{\frac{b}{I}}, \quad 其中 0 \le x_i^m \le 1, \ 常量 b > 1$$

[32]其中，$R^m(X^m)$表征所述商户风险值，x_i^m表征第 i 个维度的商户风险向量，i 为 1 至 I 中的任意一个整数；判断所述商户风险值是否大于第二预定值，如果是，则确定所述交易的支付风险可控。

[33]在本说明书的一个实施例中，所述商户的风险数据包括如下中的任一项：商户的历

史行为数据、所述用户的信用状态数据、所述商户的服务等级数据。

[34]在本说明书的一个实施例中，所述用户的风险数据包括如下中的任一项：所述用户的历史行为数据、所述用户的消费能力统计数据、所述用户的信用状态数据以及所述用户的芝麻信用分数。

[35]在本说明书的一个实施例中，进一步包括：扣款处理模块；所述扣款处理模块被配置为执行如下处理中的至少一项：在所述风险控制模块判断出交易的支付风险可控之后，利用获取的所述用户的账户信息进行扣款处理，如果扣款不成功，则从预先设立的刷脸付资金池的账户中进行扣款；和/或，在所述风险控制模块判断出交易的支付风险不可控之后，利用获取的所述用户的账户信息进行扣款处理，如果扣款不成功，则通知用户扣款失败，如果扣款成功，则通知用户可离开。

[36]根据第三方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书任一实施例所述的方法。

[37]根据第四方面，提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书任一实施例所述的方法。

[38]根据本说明书实施例提供的刷脸支付的方法和装置，一旦在用户的身份核验通过，并且判断出交易的支付风险可控之后，用户就可以离开。这样，后续的收单支付阶段的处理中，用户就无需在现场等待，从而减少了用户的等待时间。

附图说明

[39]为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[40]图 1 示出了本说明书一个实施例中刷脸支付的方法的流程图。

[41]图 2 示出了本说明书一个实施例中刷脸支付装置的一种结构示意图。

[42]图 3 示出了本说明书一个实施例中刷脸支付装置的另一种结构示意图。

[43]图 4 示出了本说明书一个实施例中刷脸支付装置的又一种结构示意图。

具体实施方式

[44]下面结合附图，对本说明书提供的方案进行描述。

[45]在现有的刷脸支付过程中，用户刷脸后，可以获取到人脸图像，则会对用户的身份进行核验，在核验通过后，需要进行收单支付阶段的处理，该收单支付阶段的处理包括：用户确认支付，获取用户对应的付款码，根据付款码对用户的交易进行扣款处理。在该收单支付阶段完成且扣款成功后，会通知用户可离开。

[46]可见，在现有的刷脸支付过程中，即使用户的身份核验通过，用户仍然不能离开，而是需要等到整个收单支付阶段完成且扣款成功后，用户方可离开。因此，增加了用户的等待时间。用户等待时间过长，会导致用户体验差，从而限制了业务的发展。

[47]对刷脸支付的过程进行分析可知，在对用户的身份进行核验时，因为涉及对用户的处理，因此，用户需要在现场等待，不能离开。但是，一旦在用户的身份核验通过后，由于用户已经完成刷脸，因此后续的收单支付阶段的处理与用户是否在现场没有必然联系。该收单支付阶段是与用户的支付能力相关。也就是说，在用户身份核验通过且用户的支付风险可控后，用户就无需在现场等待，随时可以离开，从而减少用户的等待时间。

[48]下面描述本说明书所提供构思的具体实现方式。

[49]图 1 示出根据一个实施例的刷脸支付方法的流程图。可以理解，该方法可以通过任何具有计算、处理能力的装置、设备、平台、设备集群来执行。参见图 1，该方法包括：步骤 101：检测到刷脸支付触发事件；步骤 103：获取人脸图像；步骤 105：根据获取的所述人脸图像进行用户的身份核验；步骤 107：在所述用户的身份核验通过后，获取所述用户的风险数据；步骤 109：利用所述用户的风险数据判断交易的支付风险是否可控，如果可控，通知所述用户可离开。

[50]可见，在上述图 1 所示过程中，一旦在用户的身份核验通过，并且判断出交易的支付风险可控之后，用户就可以离开。这样，后续的收单支付阶段的处理中，用户就无需在现场等待，从而减少了用户的等待时间。

[51]下面对图 1 所示的各个步骤进行说明。

[52]在本说明书的一个实施例中，步骤 101 中检测到的刷脸支付触发事件可以包括如下任一项的触发事件：触发事件 1：检测到刷脸机具的屏幕上出现人脸。

[53]在本触发事件 1 中，如果刷脸机具的屏幕上出现人脸，则可以说明用户站在了刷脸

机具前，表示用户有刷脸支付的意愿， 因此，可以将此事件作为刷脸支付触发事件来启动刷脸支付的流程。

[54]同时，该触发事件 1 不仅能说明当前需要启动刷脸支付流程，而且也能说明用户有支付意愿。应用该触发事件 1 后，本说明书的实施例则可以将用户支付意愿的确认提前到启动刷脸支付的阶段，而不是现有技术中在用户身份核验通过后，在收单支付阶段才需要用户确认支付意愿。应用该触发事件 1 后，本说明书的实施例可以简化刷脸支付的流程。

[55]触发事件 2：检测到对刷脸支付按钮的点击输入，该刷脸支付按钮位于刷脸机具的屏幕上。

[56]在本说明书的一个实施例中，可以在刷脸机具的屏幕上显示刷脸支付开启的按钮，如果用户或者商户点击了屏幕上的该按钮，则可以说明当前需要启动刷脸支付的流程。

[57]触发事件 3：检测到通过物理键盘输入的对应于刷脸支付的按键操作；在本说明书的一个实施例中，可以预先设置物理键盘上的一个按键操作对应于启动刷脸支付。那么，如果用户或者商户在物理键盘上进行该按键操作，则说明当前需要启动刷脸支付的流程。

[58]触发事件 4：检测到人脸的眼部注视刷脸机具的屏幕。

[59]在本说明书的一个实施例中，当检测到人脸的眼部注视刷脸机具的屏幕时，也可以说明用户当前将注意力放在了刷脸机具上，可以证明用户有意愿开启刷脸支付的流程。因此，通过该触发事件 3 不仅能说明当前应该启动刷脸支付的流程，而且也能将用户支付意愿的确认提前到启动刷脸支付的阶段，从而简化了刷脸支付的流程。

[60]触发事件 5：检测到刷脸机具的屏幕上出现对应于刷脸支付的人体动作。

[61]在本说明书的一个实施例中，可以预先约定一个对应于刷脸支付的人体动作，比如，用户摆出胜利的手势，或者，用户用手摸脸等。通过该预先约定的人体动作来启动刷脸支付的过程，此种处理方式能够增加用户的趣味体验，并且，由于是基于动态的活体人类动作，因此，增加了仿造的难度，提高了刷脸支付的安全性。

[62]触发事件 6：检测到对应于刷脸支付的语音口令。

[63]在本说明书的一个实施例中，可以预先约定一个对应于刷脸支付的语音口令，比如，用户说出“刷脸支付”。此种处理方式能够增加用户的趣味体验。

[64]接下来，在步骤 103 中，获取人脸图像。具体的获取人类图像的方法可以跟现有技

术中相同，比如，启动刷脸机具上的摄像头，从而拍摄出人脸图像。

[65]需要说明的是，如果在步骤 101 中，是通过上述触发事件 1 或者触发事件 3 来触发启动刷脸支付流程，那么，本步骤 103 中，也可以直接将步骤 101 中得到的人脸图像作为获取的人脸图像。

[66]在实际的业务实现中，很可能会存在刷脸机具的屏幕上出现非交易的用户的人脸的干扰情况，比如旁人经过刷脸机具时其人脸无意中出现在该屏幕上；再如，进行交易的用户与他人同行时，他人站在该交易的用户的旁边导致屏幕上出现多个人脸。针对此种情况，在本说明书的一个实施例中，在步骤 103 获取了人脸图像之后，并执行上述步骤 105 进行用户的身份核验之前，还可以进一步执行如下的去干扰处理中的任一项：去干扰处理 1：根据步骤 103 所获取的人脸图像，进行注意力识别，如果确定对应的人脸的注意力在刷脸机具的屏幕上，比如，眼睛直视屏幕和/或人脸正对屏幕等，都可以说明当前获取的人脸图像正确，即该人脸图像对应的用户正是当前需要交易的用户，则可以继续执行步骤 105 中根据获取的人脸图像进行用户的身份核验的处理。

[67]去干扰处理 2：根据步骤 103 所获取的人脸图像判断当前是否获取了至少两个人脸图像，如果是，则计算每一个人脸图像对应的人脸相对于所述刷脸机具的屏幕的空间位置数据，比如该人脸相对于刷脸机具屏幕的位置或距离，再如该人脸在屏幕上的大小等，然后，利用计算出的空间位置数据计算每一个人脸图像对应的概率，将概率值最大的人脸图像确定为当前需要交易的用户的人脸图像，并根据该当前需要交易的用户的人脸图像进行步骤 105 中用户的身份核验；去干扰处理 3：在步骤 103 获取人脸图像之后，检测刷脸机具的屏幕上是否同时出现人体躯干，如果是，则判断该人体躯干与获取的人脸图像是否属于同一个用户，如果属于，则说明用户确实站在刷脸机具前，屏幕上出现的是当前需要交易的用户，而不是一个探出的干扰的人脸，则可以继续执行步骤 105 中根据获取的人脸图像进行用户的身份核验的处理。

[68]接下来，在步骤 105 中，根据获取的人脸图像进行用户的身份核验，具体可以包括：首先，根据所获取的人脸图像进行活体检测；其次，如果活体检测通过，则说明当前的人脸图像不是仿冒的一个预先准备的静态图像，而是真实从现场采集的人脸图像，之后，根据所获取的人脸图像进行人脸识别，判断能否识别出对应于人脸图像的用户身份，如果能，则说明确定了用户身份，比如识别出人脸图像对应的是身份证号为 A 的用户张三，这样，则用户的身份核验通过。

[69]接下来，在步骤 107 和步骤 109 中，在用户的身份核验通过后，会获取用户的风险

数据，并根据该风险数据判断交易的支付风险是否可控，如果可控，则说明用户无需在现场等待支付扣款成功，则可以通知用户离开。

[70]在本说明书的一个实施例中，为了更加全面地评价用户的支付能力，更为准确地判断出交易的支付风险是否可控，可以从多个维度来获取用户的风险数据，并进行判断。具体地，在步骤 107 中，获取 N 个维度的用户风险数据；其中，N 为正整数，较佳地，N 可以为大于 1 的自然数；并且，对每一个维度的用户风险数据均进行归一化处理，得到该维度的用户风险向量，该用户风险向量为 0 至 1 范围内的一个数值；相应地，在步骤 109 中，利用风险数据判断交易的支付风险是否可控的具体实现过程包括：利用如下计算式 1，计算用户风险值：

$$R^u(X^u)=\left(\prod_{n=1}^{N}x_n^u\right)^{\frac{1}{aN}}，其中\ 0\le x_n^u\le 1，常量a>1$$

[71]其中，$R^u(X^u)$表征所述用户风险值，x_n^u表征第 n 个维度的用户风险向量，x_n^u的值为 0 至 1 范围内的一个数值；n 为 1 至 N 中的任意一个整数；判断计算出的用户风险值是否大于第一预定值，如果是，则确定交易的支付风险可控。

[72]第一预定值可以根据业务需要，设定为大于等于 0 且小于 1 的一个数值。

[73]在上述计算式 1 中，当 N 为大于 1 的正整数时，利用的是多个维度的用户风险向量，因此，基于多个维度考虑时，相当于风险会被分摊到该多个维度，那么，计算出的用户风险值应该小于每一个维度对应的用户风险向量的值，所以将 N 个维度的用户风险向量进行相乘，这样则相当于进行了风险分摊处理，即风险缩小处理。在进行相乘处理（即风险缩小处理）之后，得到的数值会比较小，可以对该相乘后的数值再进行$\frac{1}{aN}$次方计算，则相当于对相乘处理（即风险缩小处理）的数值进行放大处理，从而能够通过该放大处理后的数值来更为明显、更为差异化地体现出交易的支付风险。

[74]在上述计算式 1 中，常量 a＞1，可以使得计算式 1 最终得到的结果被放大的倍数更多，从而更进一步地体现交易的支付风险。

[75]在本说明书的一个实施例中，用户的风险数据包括如下中的任一项：用户的历史行为数据、用户的消费能力统计数据、用户的信用状态数据以及用户的芝麻信用分数。

[76]在实际的业务实现中，刷脸支付的交易风险可以来源于用户、刷脸机具以及商户中的任意一方。比如，用户的历史支付情况较差、刷脸机具被攻击带病毒、商户存在欺诈

交易行为等，都会导致刷脸支付的交易风险不可控。因此，可以从用户、刷脸机具以及商户的角度，分别来判断交易风险是否可控。

[77]在上述本说明书的实施例中，已经从用户的角度描述了确定交易的支付风险是否可控的实现过程。下面分别从刷脸机具的角度以及商户的角度，来分别说明确定交易的支付风险是否可控的实现过程。

[78]刷脸机具角度：在上述步骤 109 通知用户可离开之前，进一步执行：步骤 A1、获取刷脸机具的风险数据；步骤 B1、利用刷脸机具的风险数据判断交易的支付风险是否可控，如果是，则继续执行步骤 109 中通知用户可离开的处理。

[79]在本说明书一个实施例中，步骤 A1 中获取刷脸机具的风险数据可以包括：获取 M 个维度的刷脸机具风险数据；其中，M 为正整数；以及对每一个维度的刷脸机具风险数据均进行归一化处理，得到该维度的刷脸机具风险向量；每一个维度的刷脸机具风险向量的值为 0 或 1，即要么是表示风险不可控的数值 0，要么是表示风险可控的数值 1，而没有介于 0 与 1 之间的中间值；则步骤 B1 中利用刷脸机具的风险数据判断交易的支付风险是否可控，包括：利用如下计算式 2，计算机具风险值：

$$R^d(X^d) = \prod_{m=1}^{M} x_m^d ,$$

[80]其中，$R^d(X^d)$表征机具风险值，x_m^d表征第 m 个维度的机具风险向量，x_m^d的值为 0 或 1，m 为 1 至 M 中的任意一个整数；

[81]判断计算出的机具风险值是否为 1，如果是 1，则确定所述交易的支付风险可控，则可以执行步骤 109 中通知用户可离开的处理；如果不为 1，为 0，则确定交易的支付风险不可控，则不会通知用户可离开。

[82]在上述计算式 2 中，机具风险向量x_m^d的值只有两个，0 或 1，而没有中间值。这是因为，无论刷脸机具在哪个维度上产生风险，交易都必然是不可进行的，比如，一个维度的机具风险向量的值为 0，可能表示刷脸机具软件环境被黑客攻击，此种情况下，不能进行交易。

[83]刷脸机具的风险数据可以包括如下中的任一项：所述刷脸机具的软件环境的风险数据、所述刷脸机具的硬件环境的风险数据以及通信网络风险数据。

[84]至此，则完成了从刷脸机具角度来判断交易的支付风险是否可控。

[85]商户角度：在上述步骤 109 通知用户可离开之前，进一步执行：步骤 A2、获取商户的风险数据；步骤 B2、利用商户的风险数据判断交易的支付风险是否可控，如果是，则继续执行步骤 109 中通知用户可离开的处理。

[86]在本说明书一个实施例中，步骤 A2 中获取商户的风险数据可以包括：获取 I 个维度的商户风险数据；其中，I 为正整数；以及对每一个维度的商户风险数据均进行归一化处理，得到该维度的商户风险向量，每一个维度的商户风险向量为 0 至 1 范围内的一个数值；则步骤 B2 中，利用商户的风险数据判断交易的支付风险是否可控，包括：利用如下计算式 3，计算商户风险值：

$$R^m(X^m)=\left(\prod_{i=1}^{I}x_i^m\right)^{\frac{b}{I}}，其中\ 0\le x_i^m\le 1，常量 b>1$$

[87]其中，$R^m(X^m)$表征商户风险值，x_i^m表征第 i 个维度的商户风险向量，x_i^m为 0 至 1 范围内的一个数值，i 为 1 至 I 范围内的任意一个整数；判断商户风险值是否大于第二预定值，如果是，则确定交易的支付风险可控。

[88]第二预定值可以根据业务需要，设定为大于等于 0 且小于 1 的一个数值。

[89]在上述计算式 3 中，当 I 为大于 1 的正整数时，利用的是多个维度的商户风险向量，因此，基于多个维度考虑时，相当于风险会被分摊到该多个维度，那么，计算出的商户风险值应该小于每一个维度对应的风险值，所以将 I 个维度的商户风险向量进行相乘，这样则相当于进行了风险分摊处理，即风险缩小处理。在进行相乘处理（即风险缩小处理）之后，得到的数值会比较小，可以对该相乘后的数值再进行$\frac{b}{I}$次方计算，则相当于对相乘处理（即风险缩小处理）的数值进行适当的放大处理，从而能够通过该放大处理后的数值来更为明显、更为差异化地体现出交易的支付风险。

[90]在上述计算式 3 中，常量 b＞1，可以使得计算式 3 最终得到的结果被放大的倍数更多，从而更进一步地从商户的角度来体现交易的支付风险。

[91]在本说明书的一个实施例中，商户的风险数据包括如下中的任一项：商户的历史行为数据、所述用户的信用状态数据、所述商户的服务等级数据。

[92]在上述计算式 1 中，为了进行放大处理，进行的是$\frac{1}{aN}$次方计算，在上述计算式 3 中，为了进行放大处理，进行的是$\frac{b}{I}$次方计算。在维度数相等即 N=I 的情况下，计算式 1 中的放大效果将远大于计算式 3 中的放大效果。这是因为，在实际的业务实现中，用户支

付风险的判断结果一般比商户支付风险的判断结果更为重要，通过增大放大倍数，能够更为突出用户支付风险的重要性。

[93]当然，上述 3 个计算式中的维度数的值可以不相等，具体看实际业务需求。

[94]另外，在本说明书的一个实施例中，可以综合用户角度、刷脸机具角度以及商户角度来一起判断交易的支付风险是否可控，具体的，则是将上述 3 个计算式的计算结果相乘，如果得到的数值大于第三预定值（该第三预定值可以根据业务需要，设定为大于等于 0 且小于 1 的一个数值），则可以认为交易的支付风险可控，则可以通知用户可离开，否则，认为交易的支付风险不可控，则不会通知用户可离开。

[95]至此，本说明书实施例则实现了确定交易的支付风险是否可控的处理。

[96]在上述步骤 109 之后，即在利用风险数据判断出交易的支付风险可控之后，可以进一步进行本说明书实施例提供的收单支付阶段的处理，包括：利用获取的用户的账户信息进行扣款处理；如果扣款不成功，则从预先设立的刷脸付资金池的账户中进行扣款。此种处理，因为执行支付风险判断的平台已经判断出交易的支付风险可控，如果后续扣款不成功，则可以由平台来承担该损失，即从预先设立的刷脸付资金池的账户中进行扣款，使得商户收单成功，防止漏单，从而将扣款不成功的钱款损失风险从商家转移到平台，商家无需承担扣款不成功的风险。并且，商家无需与平台进行任何签约处理，即可以享受钱款损失风险转移的好处。

[97]在上述步骤 109 之后，即在利用风险数据判断出交易的支付风险不可控之后，可以进一步进行现有的收单支付阶段的处理，包括：利用获取的用户的账户信息进行扣款处理，如果扣款不成功，则通知用户不可离开，扣款失败，如果扣款成功，则通知用户可离开。

[98]综上，根据本说明书提供的一个或多个刷脸支付的方法实施例，可以至少得到如下的有益效果：1、在用户的身份核验通过，并且判断出交易的支付风险可控之后，在未进行收单支付阶段的处理时，就通知用户可离开。这样，后续的收单支付阶段的处理中，用户就无需在现场等待，从而减少了用户的等待时间。

[99]2、本说明书的实施例，可以将用户支付意愿的确认提前到启动刷脸支付的阶段，整个刷脸支付过程中，用户只需要刷脸一次，而不是现有技术中在启动阶段刷脸一次，在收单支付阶段再刷脸一次确认支付意愿，共刷脸两次。从而简化了刷脸支付的流程。

[100]3、能够对获取的人脸图像进行去干扰处理，从而大大降低了刷脸机具的屏幕上出

现非交易用户的人脸时对交易所造成的干扰。

[101] 4、能够从用户、刷脸机具、商户三个角度来判断交易的支付风险是否可控，从而使得判断结果更为准确、全面。

[102] 5、在从用户或商户角度计算风险值时，可以先进行风险的分摊处理，即风险值缩小处理，然后再进行为了提示风险而进行的风险值放大处理，这样，则可以使得计算的风险值更为合理并且更易于表征风险程度。

[103] 6、在平台已经判断出交易的支付风险可控之后，如果后续扣款不成功，则可以由平台来承担该损失，即从预先设立的刷脸付资金池的账户中进行扣款，使得商户收单成功，防止漏单，从而将扣款不成功的钱款损失风险从商家转移到平台，商家无需承担扣款不成功的风险。并且，商家无需与平台进行任何签约处理，即可以享受钱款损失风险转移的好处。

[104] 在本说明书的一个实施例中，提出了一种刷脸支付的装置，参见图 2，包括：刷脸支付启动模块 201，配置为在检测到刷脸支付触发事件后，获取人脸图像；身份核验模块 202，配置为根据获取的所述人脸图像进行用户的身份核验；风险控制模块 203，配置为在所述用户的身份核验通过后，获取所述用户的风险数据；利用所述用户的风险数据判断交易的支付风险是否可控；通知模块 204，配置为在所述风险控制模块 203 判断出交易的支付风险可控之后，通知用户可离开。

[105] 在本说明书提出的装置的一个实施例中，刷脸支付启动模块 201 被配置为在检测到如下中的任一项时，确定检测到刷脸支付触发事件：检测到刷脸机具的屏幕上出现人脸；检测到对刷脸支付按钮的点击输入，该刷脸支付按钮位于刷脸机具的屏幕上；检测到通过物理键盘输入的对应于刷脸支付的按键操作；检测到人脸的眼部注视刷脸机具的屏幕；检测到刷脸机具的屏幕上出现对应于刷脸支付的人体动作；检测到对应于刷脸支付的语音口令。

[106] 在本说明书提出的装置的一个实施例中，参见图 3，可以进一步包括支付确认模块 301；支付确认模块 301 被配置为执行如下中的任一项处理：根据所获取的人脸图像，进行注意力识别，如果确定注意力在所述刷脸机具的屏幕上，则触发所述身份核验模块 202 执行所述根据获取的所述人脸图像进行用户的身份核验；判断当前是否获取了至少两个人脸图像，如果是，则计算每一个人脸图像对应的人脸相对于所述刷脸机具的屏幕的空间位置数据，利用计算出的空间位置数据计算每一个人脸对象对应的概率，将概率

值最大的人脸图像确定为所述用户的人脸图像，并触发所述身份核验模块 202 执行根据获取的所述用户的人脸图像进行用户的身份核验；检测刷脸机具的屏幕上是否出现人体躯干，如果是，则判断该人体躯干与获取的人脸图像是否属于同一个用户，如果属于，则触发所述身份核验模块 202 执行所述根据获取的所述人脸图像进行用户的身份核验。

[107] 在本说明书提出的装置的一个实施例中，身份核验模块 202 被配置为执行如下处理：根据所获取的所述人脸图像进行活体检测；如果所述活体检测通过，则根据所获取的所述人脸图像进行人脸识别，判断能否识别出对应于所述人脸图像的用户身份，如果能，则所述用户的身份核验通过。

[108] 在本说明书提出的装置的一个实施例中，风险控制模块 203 被配置为执行如下处理：获取 N 个维度的用户风险数据；其中，N 为正整数；以及对每一个维度的用户风险数据均进行归一化处理，得到该维度的用户风险向量；每一个维度的用户风险向量为 0 至 1 范围内的任意一个数值；则，所述利用所述风险数据判断交易的支付风险是否可控，包括：利用如下计算式，计算用户风险值：

$$R^u(X^u) = \left(\prod_{n=1}^{N} x_n^u\right)^{\frac{1}{aN}}，\text{其中 } 0 \le x_n^u \le 1，\text{常量} a > 1$$

[109] 其中，$R^u(X^u)$表征所述用户风险值，x_n^u表征第 n 个维度的用户风险向量，x_n^u为 0 至 1 范围内的一个数值；n 为 1 至 N 中的任意一个整数；判断所述用户风险值是否大于第一预定值，如果是，则确定所述交易的支付风险可控。

[110] 在本说明书提出的装置的一个实施例中，风险控制模块 203 进一步被配置为执行如下处理：获取刷脸机具的风险数据；

[111] 利用所述刷脸机具的风险数据判断交易的支付风险是否可控。

[112] 在本说明书提出的装置的一个实施例中，风险控制模块 203 被配置为执行如下处理：获取 M 个维度的刷脸机具风险数据；其中，M 为正整数；以及对每一个维度的刷脸机具风险数据均进行归一化处理，得到该维度的刷脸机具风险向量；每一个维度的刷脸机具风险向量的值为 0 或者 1；则，所述利用所述刷脸机具的风险数据判断交易的支付风险是否可控，包括：利用如下计算式，计算机具风险值：

$$R^d(X^d) = \prod_{m=1}^{M} x_m^d，$$

[113] 其中，$R^d(X^d)$表征所述机具风险值，x_m^d表征第 m 个维度的机具风险向量，x_m^d的值为 0 或 1，m 为 1 至 M 中的任意一个整数；判断所述机具风险值是否为 1，如果是，则确定所述交易的支付风险可控。

[114] 在本说明书提出的装置的一个实施例中，刷脸机具的风险数据包括如下中的任一项：所述刷脸机具的软件环境的风险数据、所述刷脸机具的硬件环境的风险数据以及通信网络风险数据。

[115] 在本说明书提出的装置的一个实施例中，风险控制模块 203 进一步被配置为执行如下处理：获取商户的风险数据；利用所述商户的风险数据判断交易的支付风险是否可控，如果是，则继续执行所述通知所述用户可离开。

[116] 在本说明书提出的装置的一个实施例中，风险控制模块 203 被配置为执行如下处理：所述获取商户的风险数据，包括：获取 I 个维度的商户风险数据；其中，I 为正整数；以及对每一个维度的商户风险数据均进行归一化处理，得到该维度的商户风险向量；每一个维度的商户风险向量的值为 0 至 1 中任意一个数值；则，所述利用所述商户的风险数据判断交易的支付风险是否可控，包括：利用如下计算式，计算商户风险值：

$$R^m(X^m)=\left(\prod_{i=1}^{I}x_i^m\right)^{\frac{b}{I}}，其中\ 0\le x_i^m\le 1，常量 b>1$$

[117] 其中，$R^m(X^m)$表征所述商户风险值，x_i^m表征第 i 个维度的机具风险向量，x_i^m的值为 0 至 1 中任意一个数值；i 为 1 至 I 中的任意一个整数；判断所述商户风险值是否大于第二预定值，如果是，则确定所述交易的支付风险可控。

[118] 在本说明书提出的装置的一个实施例中，商户的风险数据包括如下中的任一项：商户的历史行为数据、所述用户的信用状态数据、所述商户的服务等级数据。

[119] 在本说明书提出的装置的一个实施例中，用户的风险数据包括如下中的任一项：所述用户的历史行为数据、所述用户的消费能力统计数据、所述用户的信用状态数据以及所述用户的芝麻信用分数。

[120] 在本说明书提出的装置的一个实施例中，参见图 4，进一步包括：扣款处理模块 401；扣款处理模块 401 被配置为执行如下处理中的至少一项：在所述风险控制模块 203 判断出交易的支付风险可控之后，利用获取的所述用户的账户信息进行扣款处理，如果扣款不成功，则从预先设立的刷脸付资金池的账户中进行扣款；在风险控制模块 203 判断出交易的支付风险不可控之后，利用获取的所述用户的账户信息进行扣款处理，如果

扣款不成功，则通知用户扣款失败，如果扣款成功，则通知用户可离开。

[121] 在本说明书的一个实施例中，上述刷脸支付的装置可以被集成在刷脸机具中，或者也可以被集成在一个与刷脸机具相连的独立的设备中。

[122] 根据另一方面的实施例，还提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书任一实施例中所描述的方法。

[123] 根据再一方面的实施例，还提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书任一实施例中所描述的方法。

[124] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[125] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[126] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权利要求书

1、一种刷脸支付的方法，包括：

检测到刷脸支付触发事件；

获取人脸图像；

根据获取的所述人脸图像进行用户的身份核验；

在所述用户的身份核验通过后，获取所述用户的风险数据；

利用所述用户的风险数据判断交易的支付风险是否可控；

如果可控，通知用户可离开。

2、根据权利要求 1 所述的方法，其中，所述检测到刷脸支付触发事件包括如下中的任一项：

检测到刷脸机具的屏幕上出现人脸；

检测到对刷脸支付按钮的点击输入，该刷脸支付按钮位于刷脸机具的屏幕上；

检测到通过物理键盘输入的对应于刷脸支付的按键操作；

检测到人脸的眼部注视刷脸机具的屏幕；

检测到刷脸机具的屏幕上出现对应于刷脸支付的人体动作；

检测到对应于刷脸支付的语音口令。

3、根据权利要求 1 所述的方法，其中，在所述获取人脸图像之后，并在所述根据获取的人脸图像进行用户的身份核验之前，进一步执行如下中的任一项：

根据所获取的人脸图像，进行注意力识别，如果确定注意力在所述刷脸机具的屏幕上，则继续执行所述根据获取的所述人脸图像进行用户的身份核验；

如果当前获取了至少两个人脸图像，则计算每一个人脸图像对应的人脸相对于所述刷脸机具的屏幕的空间位置数据，利用计算出的空间位置数据计算每一个人脸图像对应的概率，将概率值最大的人脸图像确定为所述用户的人脸图像，并根据该用户的人脸图像进行所述用户的身份核验；

如果检测到刷脸机具的屏幕上出现人体躯干，则判断该人体躯干与获取的人脸图像是否属于同一个用户，如果属于，则继续执行所述根据获取的所述人脸图像进行用户的身份核验。

4、根据权利要求 1 所述的方法，其中，所述根据获取的所述人脸图像进行所述用户的身份核验，包括：

根据所获取的所述人脸图像进行活体检测；

如果所述活体检测通过，则根据所获取的所述人脸图像进行人脸识别，判断能否识别出对应于所述人脸图像的用户身份，如果能，则所述用户的身份核验通过。

5、根据权利要求 1 所述的方法，其中，

所述获取所述用户的风险数据包括：

获取 N 个维度的用户风险数据；其中，N 为正整数；以及

对每一个维度的用户风险数据均进行归一化处理，得到该维度的用户风险向量；

所述利用所述风险数据判断交易的支付风险是否可控，包括：

利用如下计算式，计算用户风险值：

$$R^u(X^u)=\left(\prod_{n=1}^{N}x_n^u\right)^{\frac{1}{aN}}，其中0\le x_n^u\le 1，常量a>1$$

其中，$R^u(X^u)$表征所述用户风险值，x_n^u表征第 n 个维度的用户风险向量，n 为 1 至 N 中的任意一个整数；

如果所述用户风险值大于第一预定值，则确定所述交易的支付风险可控。

6、根据权利要求 1 所述的方法，其中，在所述通知所述用户可离开之前，进一步包括：

获取刷脸机具的风险数据；

利用所述刷脸机具的风险数据判断交易的支付风险是否可控。

7、根据权利要求 6 所述的方法，其中，

所述获取刷脸机具的风险数据，包括：

获取 M 个维度的刷脸机具风险数据；其中，M 为正整数；以及

对每一个维度的刷脸机具风险数据均进行归一化处理，得到该维度的刷脸机具风险向量；

所述利用所述刷脸机具的风险数据判断交易的支付风险是否可控，包括：

利用如下计算式，计算机具风险值：

$$R^d(X^d)=\prod_{m=1}^{M}x_m^d，$$

其中，$R^d(X^d)$表征所述机具风险值，x_m^d表征第 m 个维度的机具风险向量，x_m^d的值为 0 或 1，m 为 1 至 M 中的任意一个整数；

如果所述机具风险值为 1，则确定所述交易的支付风险可控。

8、根据权利要求 6 所述的方法，其中，所述刷脸机具的风险数据包括如下中的任一项：所述刷脸机具的软件环境的风险数据、所述刷脸机具的硬件环境的风险数据以及通信网络风险数据。

9、根据权利要求 1 所述的方法，其中，在所述通知所述用户可离开之前，进一步包括：

获取商户的风险数据；

利用所述商户的风险数据判断交易的支付风险是否可控。

10、根据权利要求 9 所述的方法，其中，

所述获取商户的风险数据，包括：

获取 I 个维度的商户风险数据；其中，I 为正整数；以及

对每一个维度的商户风险数据均进行归一化处理，得到该维度的商户风险向量；

所述利用所述商户的风险数据判断交易的支付风险是否可控，包括：

利用如下计算式，计算商户风险值：

$$R^m(X^m)=\left(\prod_{i=1}^{I}x_i^m\right)^{\frac{b}{I}}，其中0\le x_i^m\le 1，常量b>1$$

其中，$R^m(X^m)$表征所述商户风险值，x_i^m表征第 i 个维度的商户风险向量，i 为 1 至 I 中的任意一个整数；

如果所述商户风险值大于第二预定值，则确定所述交易的支付风险可控。

11、根据权利要求 9 所述的方法，其中，所述商户的风险数据包括如下中的任一项：商户的历史行为数据、所述用户的信用状态数据、所述商户的服务等级数据。

12、根据权利要求 1 至 11 中任一所述的方法，其中，所述用户的风险数据包括如下中的任一项：所述用户的历史行为数据、所述用户的消费能力统计数据、所述用户的信用状态数据以及所述用户的芝麻信用分数。

13、根据权利要求 1 至 11 中任一所述的方法，

在利用所述风险数据判断出交易的支付风险可控之后，进一步包括：利用所述用户的账户信息进行扣款处理；如果扣款不成功，则从预先设立的刷脸付资金池的账户中进行扣款；和/或，

在利用所述风险数据判断出交易的支付风险不可控之后，进一步包括：利用所述用户的账户信息进行扣款处理，如果扣款不成功，则通知用户扣款失败，如果扣款成功，则通知用户可离开。

14、一种刷脸支付的装置，包括：

刷脸支付启动模块，配置为在检测到刷脸支付触发事件后，获取人脸图像；

身份核验模块，配置为根据获取的所述人脸图像进行用户的身份核验；

风险控制模块，配置为在所述用户的身份核验通过后，获取所述用户的风险数据；利用所述用户的风险数据判断交易的支付风险是否可控；

通知模块，配置为在所述风险控制模块判断出交易的支付风险可控之后，通知所述用户可离开。

15、根据权利要求 14 所述的装置，其中，所述刷脸支付启动模块被配置为在检测到如下中的任一项时，确定检测到刷脸支付触发事件：

检测到刷脸机具的屏幕上出现人脸；

检测到对刷脸支付按钮的点击输入，该刷脸支付按钮位于刷脸机具的屏幕上；

检测到通过物理键盘输入的对应于刷脸支付的按键操作；

检测到人脸的眼部注视刷脸机具的屏幕；

检测到刷脸机具的屏幕上出现对应于刷脸支付的人体动作；

检测到对应于刷脸支付的语音口令。

16、根据权利要求 14 所述的装置，进一步包括：支付确认模块，被配置为执行如下中的任一项处理：

根据所获取的人脸图像，进行注意力识别，如果确定注意力在所述刷脸机具的屏幕上，则触发所述身份核验模块执行所述根据获取的所述人脸图像进行用户的身份核验；

如果当前获取了至少两个人脸图像，则计算每一个人脸图像对应的人脸相对于所述刷脸机具的屏幕的空间位置数据，利用计算出的空间位置数据计算每一个人脸对象对应的概率，将概率值最大的人脸图像确定为所述用户的人脸图像，并触发所述身份核验模块执行根据获取的所述用户的人脸图像进行用户的身份核验；

如果检测到刷脸机具的屏幕上出现人体躯干，则判断该人体躯干与获取的人脸图像是否属于同一个用户，如果属于，则触发所述身份核验模块执行所述根据获取的所述人脸图像进行用户的身份核验。

17、根据权利要求 14 所述的装置，其中，

所述风险控制模块被配置为执行如下处理：

获取 N 个维度的用户风险数据；其中，N 为正整数；以及

对每一个维度的用户风险数据均进行归一化处理，得到该维度的用户风险向量；

则，所述利用所述风险数据判断交易的支付风险是否可控，包括：

利用如下计算式，计算用户风险值：

$$R^u(X^u)=\left(\prod_{n=1}^{N}x_n^u\right)^{\frac{1}{aN}}，\ 其中0\le x_n^u\le 1，\ 常量a>1$$

其中，$R^u(X^u)$表征所述用户风险值，x_n^u表征第 n 个维度的用户风险向量，n 为 1 至 N 中的任意一个整数；

如果所述用户风险值大于第一预定值，则确定所述交易的支付风险可控。

18、根据权利要求 14 所述的装置，其中，所述风险控制模块进一步被配置为执行如下处理：

获取刷脸机具的风险数据；

利用所述刷脸机具的风险数据判断交易的支付风险是否可控。

19、根据权利要求 18 所述的装置，其中，

所述风险控制模块被配置为执行如下处理：

获取 M 个维度的刷脸机具风险数据；其中，M 为正整数；以及

对每一个维度的刷脸机具风险数据均进行归一化处理，得到该维度的刷脸机具风险向量；

则，所述利用所述刷脸机具的风险数据判断交易的支付风险是否可控，包括：

利用如下计算式，计算机具风险值：

$$R^d(X^d)=\prod_{m=1}^{M}x_m^d，$$

其中，$R^d(X^d)$表征所述机具风险值，x_m^d表征第 m 个维度的机具风险向量，x_m^d的值为 0 或 1，m 为 1 至 M 中的任意一个整数；

如果所述机具风险值为 1，则确定所述交易的支付风险可控。

20、根据权利要求 18 所述的装置，其中，所述刷脸机具的风险数据包括如下中的任一项：所述刷脸机具的软件环境的风险数据、所述刷脸机具的硬件环境的风险数据以

及通信网络风险数据。

21、根据权利要求 14 所述的装置，其中，所述风险控制模块进一步被配置为执行如下处理：

获取商户的风险数据；

利用所述商户的风险数据判断交易的支付风险是否可控。

22、根据权利要求 21 所述的装置，其中，

所述风险控制模块被配置为执行如下处理：

获取 I 个维度的商户风险数据；其中，I 为正整数；以及

对每一个维度的商户风险数据均进行归一化处理，得到该维度的商户风险向量；

则，所述利用所述商户的风险数据判断交易的支付风险是否可控，包括：

利用如下计算式，计算商户风险值：

$$R^m(X^m)=\left(\prod_{i=1}^{I}x_i^m\right)^{\frac{b}{I}}，\ 其中0\le x_i^m\le 1，\ 常量b>1$$

其中，$R^m(X^m)$表征所述商户风险值，x_i^m表征第 i 个维度的商户风险向量，i 为 1 至 I 中的任意一个整数；

如果所述商户风险值大于第二预定值，则确定所述交易的支付风险可控。

23、根据权利要求 21 所述的装置，其中，所述商户的风险数据包括如下中的任一项：商户的历史行为数据、所述用户的信用状态数据、所述商户的服务等级数据。

24、根据权利要求 14 至 23 中任一所述的装置，其中，所述用户的风险数据包括如下中的任一项：所述用户的历史行为数据、所述用户的消费能力统计数据、所述用户的信用状态数据以及所述用户的芝麻信用分数。

25、根据权利要求 14 至 23 中任一所述的装置，进一步包括：扣款处理模块，被配置为执行如下处理中的至少一项：

在所述风险控制模块判断出交易的支付风险可控之后，利用获取的所述用户的账户信息进行扣款处理，如果扣款不成功，则从预先设立的刷脸付资金池的账户中进行扣款；和/或，

在所述风险控制模块判断出交易的支付风险不可控之后，利用获取的所述用户的账户信息进行扣款处理，如果扣款不成功，则通知用户扣款失败，如果扣款成功，则通知用户可离开。

26、一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行权利要求 1-13 中任一项所述的方法。

27、一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-13 中任一项所述的方法。