说明书

拒付请求的处理方法、装置、设备、介质及程序产品

相关申请

本申请要求 2024 年 10 月 23 日申请的，申请号为 2024114871904，名称为“一种拒付请求的处理方法、装置、设备、介质及程序产品”的中国专利申请的优先权，在此将其全文引入作为参考。

技术领域

本申请属于计算机技术领域，具体而言，本申请涉及一种拒付请求的处理方法、装置、设备、介质及程序产品。

背景技术

在当今的数字化时代，电子支付系统已成为商业交易不可或缺的一部分，极大地促进了全球经济活动的便捷性和效率。支付行为，作为交易流程的核心环节，涉及资金从付款方账户向收款方账户转移的过程，通常通过银行卡、第三方支付平台等多种渠道实现。随着技术的进步，支付系统不仅要求高度的安全性与稳定性，还需具备快速响应市场变化及用户需求的灵活性。

然而，在实际应用中，支付过程并非总是顺利进行。当出现交易争议等情况时，例如，付款方认为某一笔支付或者交易可能属于盗刷，或者刷错的情况时，收款方可能会面临来自付款方的拒付请求。拒付请求是指付款方通过银行或支付机构向收款方提出，要求撤销已完成支付交易的行为。这一机制旨在保护消费者权益，但同时也给商家带来了潜在的财务风险和运营挑战，尤其是当拒付请求频繁且缺乏合理依据时。

处理拒付请求的过程中，证据的角色至关重要，以用于验证某笔交易是否属于付款方本人所发起的交易，以验证是否存在盗刷或者刷错的情况，因此，如何得到更为合理的证据，以准确地对付款方所发起的拒付请求的交易进行验证成为一个关键问题。

发明内容

本申请实施例的目的旨在提供一种能够获得更为合理的证据，以更为准确地对付款方所发起的拒付请求交易进行验证的一种拒付请求的处理方法、装置、设备、介质及程序产品。为了实现上述目的，本申请实施例提供的技术方案如下：

第一方面，提供了一种拒付请求的处理方法，由支付验证设备执行，所述方法包括：

接收拒付请求处理设备发送的针对已完成支付的支付证据提供请求，其中，所述支付证据提供请求中携带已完成支付的支付标识；所述支付证据提供请求是所述拒付请求处理设备接收到携带所述支付标识的拒付请求时发送的；所述已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，所述第一生物特征是在所述已完成支付的支付过程中采集的支付方的第一部位的生物特征；

基于所述支付标识，获取所述已完成支付所对应的第二生物特征；其中，所述第二生物特征是在所述已完成支付的支付过程中所采集的支付方的第二部位的生物特征；

向所述拒付请求处理设备发送包括所述第二生物特征的支付证据信息，以使所述拒付请求处理设备基于所述支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对所述拒付请求进行处理。

第二方面，提供了一种拒付处理的方法，由拒付请求处理设备执行，所述方法包括：

向支付验证设备发送支付证据提供请求；其中，所述支付证据提供请求中携带已完成支付所对应的支付标识；所述支付证据提供请求是所述拒付请求处理设备接收到携带所述支付标识的拒付请求时发送的；所述已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，所述第一生物特征是在所述已完成支付的支付过程中采集的支付方的第一部位的生物特征；

接收所述支付验证设备发送的包括第二生物特征的支付证据信息；所述第二生物特征

是由支付验证设备基于所述支付标识获取到的；其中，所述第二生物特征是在支付过程中所采集的第二部位的生物特征；

确定所述支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度，并基于所述匹配程度，对所述拒付请求进行处理。

第三方面，提供了一种拒付请求的处理装置，所述装置设置在支付验证设备中，所述装置包括：

支付证据提供请求接收模块，用于接收拒付请求处理设备发送的针对已完成支付的支付证据提供请求，其中，所述支付证据提供请求中携带已完成支付的支付标识；所述支付证据提供请求是所述拒付请求处理设备接收到携带所述支付标识的拒付请求时发送的；所述已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，所述第一生物特征是在所述已完成支付的支付过程中采集的支付方的第一部位的生物特征；

获取模块，用于基于所述支付标识，获取所述已完成支付所对应的第二生物特征；其中，所述第二生物特征是在所述已完成支付的支付过程中所采集的支付方的第二部位的生物特征；

支付证据信息发送模块，用于向所述拒付请求处理设备发送包括所述第二生物特征的支付证据信息，以使所述拒付请求处理设备基于所述支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对所述拒付请求进行处理。

第四方面，提供了一种拒付处理的装置，所述装置设置在拒付请求处理设备中，所述装置包括：

支付证据提供请求发送模块，用于向支付验证设备发送支付证据提供请求；其中，所述支付证据提供请求中携带已完成支付所对应的支付标识；所述支付证据提供请求是所述拒付请求处理设备接收到携带所述支付标识的拒付请求时发送的；所述已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，所述第一生物特征是在所述已完成支付的支付过程中采集的支付方的第一部位的生物特征；

支付证据信息接收模块，用于接收所述支付验证设备发送的包括第二生物特征的支付证据信息；所述第二生物特征是由支付验证设备基于所述支付标识获取到的；其中，所述第二生物特征是在支付过程中所采集的第二部位的生物特征；

匹配程度确定模块，用于确定所述支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度；

拒付请求处理模块，用于基于所述匹配程度，对所述拒付请求进行处理。

第五方面，本申请实施例还提供了一种支付验证设备，该支付验证设备包括存储器和处理器，存储器中存储有计算机程序，处理器执行该计算机程序以实现第一方面任一可能的实现方式所提供的拒付请求的处理方法。

第六方面，本申请实施例还提供了一种拒付请求处理设备，该拒付请求处理设备包括存储器和处理器，存储器中存储有计算机程序，处理器执行该计算机程序以实现第二方面任一可能的实现方式所提供的拒付请求的处理方法。

第七方面，本申请实施例还提供了一种计算机可读存储介质，该存储介质中存储有计算机程序，该计算机程序被处理器执行时实现第一方面或第二方面任一可能的实现方式所提供的拒付请求的处理方法。

第八方面，本申请实施例还提供了一种计算机程序产品，该计算机程序产品包括计算机程序，该计算机程序被处理器执行时实现第一方面或第二方面任一可能的实现方式所提供的拒付请求的处理方法。

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其它特征、目的和优点将从说明书、附图以及权利要求书变得明显。

附图说明

为了更清楚地说明本申请实施例中的技术方案，下面将对实施例中所需要使用的附图

作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的实施例，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，还可以根据公开的附图获得其他的附图。

图 1 为本申请实施例中一种拒付请求的处理系统示意图；

图 2 为本申请实施例中一种拒付请求的处理系统的示例图；

图 3a 为本申请实施例中一种拒付请求的处理方法的流程图；

图 3b 为本申请实施例中一种拒付请求的处理方法的示例图；

图 4 为本申请实施例中支付特征采集设备执行生物特征采集的流程图；

图 5 为本申请实施例中支付特征采集设备执行生物特征采集的更为具体的流程图；

图 6 为本申请实施例中另一种拒付请求的处理方法的流程图；

图 7 为本申请实施例中一种拒付请求的处理装置的结构示意图；

图 8 为本申请实施例中另一种拒付请求的处理装置的结构示意图；

图 9 为本申请实施例中一种电子设备的装置结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本申请实施例所使用的术语“包括”以及“包含”是指相应特征可以实现为所呈现的特征、信息、数据、步骤、操作、元件和/或组件，但不排除实现为本技术领域所支持其他特征、信息、数据、步骤、操作、元件、组件和/或它们的组合等。应该理解，当我们称一个元件被“连接”或“耦接”到另一元件时，该一个元件可以直接连接或耦接到另一元件，也可以指该一个元件和另一元件通过中间元件建立连接关系。此外，这里使用的“连接”或 “耦接”可以包括无线连接或无线耦接。这里使用的术语“和/或”指示该术语所限定的项目中的至少一个，例如“A 和/或 B”可以实现为“A”，或者实现为“B”，或者实现为“A 和 B”。在描述多个（两个或两个以上）项目时，如果没有明确限定多个项目之间的关系，这多个项目之间可以是指多个项目中的一个、多个或者全部，例如，对于“参数 A 包括 A1、A2、A3”的描述，可以实现为参数 A 包括 A1 或 A2 或 A3，还可以实现为参数 A 包括参数 A1、A2、A3 这三项中的至少两项。

在相关技术中，付款方在线下通过刷信用卡或者其它电子支付方式进行支付时，可以通过以下方式来验证付款方的身份，以完成支付，其中，

1、持卡人在线下商户刷信用卡后签名，通过核对签名与卡片背面或银行记录中的签名是否一致，来确认持卡人的身份，验证持卡人的身份，防止欺诈行为；

2、用户 3D Secure，用户输入办卡的手机短信验证码或在发卡行手机银行确认等身份验证和账户确认；

其中，针对 1 中所示的方式验证签名和申诉过程如下：

签名采集：当持卡人进行刷卡交易时，签名会记录在交易小票上。商家有责任核对持卡人的签名与信用卡背面的签名是否一致，以此初步验证持卡人的身份；

签名存档：商家将签名的收据妥善保管，通常会保存一定的时间（如几个月到几年不等），以备将来核查。

争议处理：如果交易出现争议（例如持卡人否认进行过某笔交易），持卡人可以向发卡行提出申诉。在这种情况下，发卡行会要求商家提供签名的收据作为证据。

签名核对：发卡行收到商家提供的签名收据后，会将其与持卡人在银行登记的签名进行核对，以确定交易的真实性。如果签名不一致，银行可能会判断这笔交易为欺诈行为，并采取相应措施。

但是，该方式可能存在以下缺点：

1、易伪造性：用户签名可能容易被伪造，尤其是在没有严格验证的情况下，也即同样的验证准确度偏低；

2、不一致性：用户在不同时间或情况下的签名可能会有所不同，导致验证困难，并且验证的准确度较低；

3、用户体验差：需要用户签名可能会增加支付时间，影响用户体验，尤其是在人流高峰期。所以部分商家不验证；

其中，针对 2 中所示的方式，交易有 3DS 验证，发卡行将对欺诈性拒付负责。如果发卡行和持卡人之间无法解决争议，卡组织网络可能会介入进行仲裁，基于双方提供的证据作出最终裁决，具体如下所示：

1、用户确认支付，商户下单发起交易；

2、发卡行要求用户验证短信或在发卡行银行网页/APP 授权验证；

3、验证成功后发起扣款，以完成支付；

4、争议处理方式（若出现付款方认为上述支付存在争议，也即提交拒付请求时，具体处理方式）：如果交易出现争议（例如持卡人否认进行过某笔交易），持卡人可以向发卡行提出申诉。在这种情况下，发卡行会要求商家提供签名的收据作为证据。

但是，该方式（3DS）可能存在以下缺点：

1、使用者体验：3DS 常常要求使用者输入额外的认证信息（如密码或一次性验证码），可能导致支付过程变得繁琐，影响使用者体验；

2、有可伪造性：恶意用户可将验证信息给到另外一个人进行填写和校验；

3、弃用率高：由于额外的认证步骤，一些用户可能会放弃交易，导致转化率下降。

对本申请实施例进行进一步详细说明之前，对本申请实施例中涉及的名词和术语进行说明，本申请实施例中涉及的名词和术语适用于如下的解释。

拒付：也称退单，指的是持卡人在支付后一定期限内（一般为 120 天，部分拒付原因可延长至 540 天），可以向银行申请拒付账单上的某笔交易。拒付实际上是信用卡公司给予持卡人的一种权利。

3DS（3D Secure）：在交易中认证持卡人身份，或提供密码、短信验证码、发卡行手机银行确认等身份验证和账户确认。实施通常由发卡行负责。

为了解决上述技术问题，本申请实施例提供了一种拒付请求的处理方法，该拒付处理的方法，可以应用于拒付请求处理系统，如图 1 所示，该拒付请求处理系统可以包括：拒付请求方设备、支付特征采集设备、支付验证设备以及拒付请求处理设备，其中，拒付请求方设备与拒付请求处理设备进行信息交互，拒付请求处理设备与支付验证设备进行信息交互，支付验证设备和支付特征采集设备进行信息交互；

在一种可能的实现方式中，如图 2 所示，拒付请求处理设备可以为：发卡行设备（也即该支付所通过的发卡行的设备），该支付系统还可以包括：收单行设备、商户设备（接收支付方设备）等，此时，拒付请求方设备与发卡行设备进行信息交互，发卡行设备和收单行设备进行信息交互，收单行设备和商户设备进行信息交互，商户设备和支付验证设备进行信息交互，支付验证设备和支付特征采集设备进行信息交互。

支付验证设备是在拒付请求处理流程中，专门负责接收拒付请求处理设备发出的支付证据提供请求的设备。它会依据请求中携带的支付标识，从相应存储处获取已完成支付所对应的第二生物特征，该第二生物特征是支付过程中支付方第二部位的生物特征。之后，支付验证设备会将包含第二生物特征的支付证据信息发送给拒付请求处理设备，以此协助拒付请求处理设备对拒付请求进行准确处理，其功能的实现有助于提高支付交易验证的合理性和准确性。

拒付请求处理设备在整个支付拒付处理体系中扮演核心角色。当它接收到付款方发起的携带支付标识的拒付请求时，会迅速生成支付证据提供请求并发送给支付验证设备。在接收支付验证设备反馈的支付证据信息后，该设备会将支付证据信息中的生物特征与拒付

请求方的生物特征进行匹配计算，得出匹配程度。基于这个匹配程度，拒付请求处理设备会做出相应决策，如拒绝或同意拒付请求，从而完成对拒付请求的处理，保障支付交易的公平性和安全性。

支付特征采集设备是支付过程中生物特征数据的采集源头。在支付流程启动后，它会响应支付请求，利用自身的采集功能，获取包含支付方第一生物特征和第二生物特征的生物特征采集视频流。当接收到支付成功信息时，会将采集到的支付方的第一生物特征和第二生物特征存储到支付证据存储设备中，为后续可能出现的拒付请求提供关键的证据数据，确保支付交易的可追溯性。

支付证据存储设备是专门用于存储支付相关生物特征数据的设备。它会关联存储各支付的支付标识与支付方的第二部位的生物特征，同时也会存储支付方的第一生物特征。这些存储的数据以加密且关联的方式保存，通过特定的存储密钥进行管理，确保数据的安全性和完整性。在支付验证设备需要获取已完成支付的生物特征时，支付证据存储设备会依据相应的密钥和标识提供准确的数据，为拒付请求的处理提供有力的数据支持。

在上述支付系统的基础上，本申请实施例提供的一种拒付处理的方法，如图 3a 所示，该方法由支付验证设备执行，该支付验证设备可以为图 1 或者图 2 中的支付验证设备，该方法可以包括：

步骤 S301、接收拒付请求处理设备发送的针对已完成支付的支付证据提供请求，其中，支付证据提供请求中携带已完成支付的支付标识；支付证据提供请求是拒付请求处理设备接收到携带支付标识的拒付请求时发送的；已完成支付是基于第一生物特征进行支付且已支付成功的支付；第一生物特征是在已完成支付的支付过程中采集的支付方的第一部位的生物特征。

其中，支付证据提供请求中携带已完成支付的支付标识；支付证据提供请求是拒付请求处理设备接收到携带支付标识的拒付请求时发送的；在本申请实施例中，若某一对象发现其账户所对应的某一笔支付存在问题，或者，并非其自身的消费，此时可以发起拒付请求，该拒付请求中携带支付标识，该支付标识可以包括：该笔支付（已完成支付）所对应的流水号。进一步地，拒付请求中除了携带支付标识，还有可能携带该拒付请求方的身份标识。

已完成支付是指基于支付方第一部位的第一生物特征进行验证并成功完成资金转移的支付交易。在支付过程中，支付系统会采集支付方第一部位的生物特征（如掌纹特征）进行身份验证，验证通过后完成支付操作。同时，在支付过程中还会采集支付方第二部位的生物特征（如面部特征），这些生物特征将作为后续可能出现的拒付请求处理的重要证据。

拒付请求是付款方在认为某笔已完成的支付交易存在问题，如可能属于盗刷或刷错的情况下，通过银行或支付机构向收款方提出的撤销该笔支付交易的请求。该请求中必须携带能够唯一标识该笔已完成支付的支付标识，同时还可能包含拒付请求方的身份标识等相关信息，是启动拒付处理流程的关键触发因素。

进一步地，拒付请求方所发起拒付请求的已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，第一生物特征是在已完成支付的支付过程中采集的支付方的第一部位的生物特征。在本申请实施例中，第一部位可以为手掌，也就是说，第一生物特征是在支付过程中采集到的支付方的掌纹特征，也即，拒付请求方所发起拒付请求的已完成支付是通过掌纹特征验证通过，且已经支付成功的支付。

对于本申请实施例，拒付请求处理设备在接收到拒付请求方所发起的拒付请求时，生成针对已完成支付的支付证据提供请求，并向支付验证设备发送。

具体地，如图 2 所示的系统，拒付请求处理设备可以为该支付所通过的发卡行的设备，当发卡行的设备在接收到拒付请求所发起的拒付请求后，生成支付证据提供请求，通过收单行设备、已完成支付所对应的商户设备将支付证据提供请求发送给支付验证设备，进一步地，在该流程中，若商户设备在接收到支付证据提供请求后，商户可以根据支付证据提

供请求获知拒付请求方的拒付请求后，若接受该拒付请求，此时不需要将支付证据提供请求发送给支付验证设备，而是将同意拒付消息发送给收单行设备，收单行设备可以告知发卡行的设备，商户同意该拒付请求方的拒付请求，发卡行的设备将该已完成支付所扣除的金额返回，具体如图 3b 所示。

收单行设备是支付交易流程中的中间环节设备，它接收拒付请求处理设备（如发卡行设备）发送的支付证据提供请求，并将其转发给商户设备。同时，收单行设备会依据特定的匹配算法，对支付证据信息中生物特征之间的匹配度进行检查，然后将检查结果发送给拒付请求处理设备，在整个拒付请求处理流程中起到信息传递和初步验证的作用。

商户设备是与支付交易直接相关的设备，在支付过程中负责接收支付请求和处理支付业务。在拒付请求处理流程中，商户设备接收收单行设备转发的支付证据提供请求，商户可根据该请求获知拒付请求方的拒付请求。若商户接受该拒付请求，会将同意拒付消息发送给收单行设备；若不接受，则将支付证据提供请求继续转发给支付验证设备。

步骤 S302、基于支付标识，获取已完成支付所对应的第二生物特征；其中，第二生物特征是在已完成支付的支付过程中所采集的支付方的第二部位的生物特征。

其中，第二生物特征是在已完成支付的支付过程中所采集的支付方的第二部位的生物特征。在本申请实施例中，支付方的第二部位的生物特征可以为支付方的面部特征，也可以为虹膜特征等，在本申请实施例中不作限定。

在本申请实施例中，以支付方的第二部位的生物特征为支付方的面部特征为例进行介绍，也即支付验证设备在接收到携带支付标识（流水号）的支付证据提供请求后，获取该已完成支付由支付特征采集设备在支付过程中所采集到的面部特征。

步骤 S303、向拒付请求处理设备发送包括第二生物特征的支付证据信息，以使拒付请求处理设备基于支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对拒付请求进行处理。

进一步地，支付验证设备在获取到该已完成支付由支付特征采集设备在支付过程中所采集到的面部特征后，向拒付请求处理设备发送包括该面部特征的支付证据信息，拒付请求处理设备在接收到包括该面部特征的支付证据信息后，基于接收到的包括该面部特征的支付证据信息与拒付请求方的生物特征进行匹配，并基于匹配程度，对拒付请求进行处理。在本申请实施例中，至少根据支付证据信息中所携带的面部特征和拒付请求方所提供的第二生物特征（也即拒付请求方的面部特征）之间的匹配程度，对拒付请求进行处理。

匹配程度是衡量支付证据信息中的生物特征与拒付请求方的生物特征相似性的量化指标。它综合考虑了第二生物特征（支付过程中支付方第二部位的生物特征）与拒付请求方第二部位的第五生物特征的匹配情况，以及第三生物特征（支付方标识对应的对象所注册的第一部位的生物特征）与拒付请求方第一部位的第四生物特征的匹配情况。拒付请求处理设备会依据这个匹配程度来判断拒付请求的合理性，进而做出相应的处理决策。

具体地，在本申请实施例中，拒付请求方的第二生物特征（拒付请求方的面部特征）可以由拒付请求处理设备采集或者获取。拒付请求方的第二生物特征还可以从拒付请求中获取到，此种情况下，拒付请求中可以携带拒付请求方的第二生物特征。

具体地，在如图 2 所示的系统中，若商户并未接受该拒付请求，此时需要从支付验证设备中获取支付证据信息，通过商户设备将支付证据信息发送给收单行设备。收单行设备会依据特定的匹配算法，对支付证据信息中生物特征（如支付过程中采集的面部特征、掌纹特征等）之间的匹配度进行检查。例如，对于面部特征，采用 SIFT（尺度不变特征变换）算法提取特征点，计算特征点之间的欧氏距离来确定匹配度；对于掌纹特征，结合清晰度、完整性、距离、亮度等多指标评估的综合得分来衡量匹配情况。

收单行设备将检查结果发送给发卡行的设备，发卡行的设备会基于该结果做出拒付决策。拒付决策主要有两种情况：一是拒绝拒付请求，即判定该笔已完成支付不存在盗刷或刷错情况，维持支付状态；二是同意拒付请求，将已支付成功的支付金额返回给拒付请求

方的账户。

发卡行的设备将针对拒付请求的处理结果（即拒付决策）发送给拒付请求方设备，由拒付请求方决定同意或者拒绝该拒付决策。若拒付请求方同意该拒付决策，例如同意拒绝拒付请求，认可该笔支付是自己发起的；或者同意拒付请求，接受退款，则关闭该拒付流程。反之，若拒付请求方拒绝该拒付决策，比如认为发卡行判定拒绝拒付请求不合理，坚持该笔支付存在问题，可通过其他流程解决该拒付请求，其他流程可能包括进一步提供补充证据、申请仲裁等，具体方式不作限定，如图 3b 所示。

再者，在一些情况下，拒付请求处理设备可以是发卡行的设备，也可以是包含发卡行设备和收单行设备的组合。当包含收单行的设备时，收单行的设备作为透传设备，负责传输支付证据提供请求和支付证据，而生物特征匹配以及根据匹配结果对拒付请求进行处理的操作由发卡行的设备执行，具体情况不作限定。再者，基于支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对拒付请求进行处理，也可以由发卡行或者收单行进行人工核对处理。

本申请实施例提供了一种拒付请求的处理方法，在该方法中，拒付请求处理设备在接收到携带支付标识的拒付请求时，并且该支付标识所对应的已完成支付是基于第一生物特征进行支付且已经支付成功的支付，此时拒付请求设备向支付验证设备发送针对已完成支付的支付证据提供请求，支付验证设备基于支付标识获取该已完成支付在所述支付过程中所采集的支付方的第二部位的生物特征，并向拒付请求处理设备发送包含该支付方的第二部位的生物特征的支付证据信息，以使得拒付请求处理设备基于支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对拒付请求进行处理。也就是说，拒付请求处理设备所得到的针对已完成支付的支付证据信息中携带有该支付方的第二部位的生物特征，以使得拒付请求处理设备基于该支付方的第二部位的生物特征与拒付请求方的生物特征进行匹配，以确定已完成支付的支付方与拒付请求方是否一致，若一致，则已完成支付为拒付请求方本人的支付，如若不一致，则已完成支付可能不是拒付请求方本人的支付，也即所提供的证据为支付方在支付过程中的另一部位的生物特征，以使得所提供的证据对于验证付款方所发起的拒付请求的交易是否为本人更为合理，从而可以准确地对付款方所发起的拒付请求的交易进行验证。

进一步地，支付验证设备在通过支付证据提供请求中得到已完成支付的支付标识后，基于支付标识，获取已完成支付所对应的第二生物特征。具体地，在本申请实施例中，步骤 S302 中基于支付标识，获取已完成支付所对应的第二生物特征，具体可以包括：向支付证据存储设备发送生物特征获取请求；接收支付证据存储设备发送的已完成支付所对应的第二生物特征。

其中，生物特征获取请求中包括支付标识；支付证据存储设备中存储有各支付的支付标识所对应的支付方的第二部位的生物特征。

由上述实施例可知，第二部位的生物特征可以为面部特征，也即，支付证据存储设备中存储有各支付的支付标识所对应的支付方的面部特征。其中，每笔支付的支付标识所对应的支付方的面部特征是在该支付的支付过程中，由支付特征采集设备所采集到的关于支付方的面部特征，也就是说，在一个支付的支付过程中，支付特征采集设备除了采集支付方的掌纹特征，还采集支付的面部特征，由上述可知，采集支付方的掌纹特征是为了找到支付方标识，以从对应的账号中划取对应的金额；采集支付方在支付过程中的面部特征，是为了为拒付请求提供证据，以验证拒付请求方和支付方是否一致，以获知拒付请求所对应的已完成支付是否属于盗刷或者刷错的情况。

进一步地，针对一次支付过程，其所对应的支付证据信息是由支付特征采集设备所采集的，当然针对上述已完成支付，其所对应的支付证据信息也是由支付特征采集设备所采集的，在本申请实施例中，已完成支付所对应的支付证据信息是由支付特征采集设备通过以下方式（步骤 Sa 和步骤 Sb）采集，并存储至支付证据存储设备的，在本申请实施例中，

支付证据存储设备可以云端存储设备，也可以为其他存储设备，还可以为支付验证设备中的存储设备。具体如图 4 所示，其中，

步骤 Sa、接收针对已完成支付的支付请求。

对于本申请实施例，收银设备（例如，收银 pos）发起支付，并将携带该已完成支付的支付标识（流水号）传给支付特征采集设备，此时支付特征采集设备接收到针对已完成支付的支付请求。

步骤 Sb、响应于支付请求，获取生物特征采集视频流，并在接收到支付成功信息时，将支付方的第一生物特征和第二生物特征存储至支付证据存储设备中。

其中，生物特征采集视频流至少包括支付方的第一生物特征和第二生物特征。

具体地，步骤 Sb 中，获取生物特征采集视频流，并在接收到支付成功消息时，将第二生物特征存储至支付证据存储设备中，具体可以包括：步骤 Sb1、步骤 Sb2、步骤 Sb3、步骤 Sb4 以及步骤 Sb5，其中，步骤 Sb1-步骤 Sb5 在图中并未示出，具体地，

步骤 Sb1、采集第一视频帧。

其中，第一视频帧中包含有支付方所对应的第二生物特征。

对于本申请实施例，支付特征采集设备在接收到收银设备的支付请求后，开启拍摄，采集包含有支付方所对应的第二生物特征的第一视频帧，也即在刷取掌纹特征之前，采集支付方的面部特征。

步骤 Sb2、输出第一提示信息。

其中，第一提示信息用于提示支付方提供第一生物特征。在本申请实施例中，在支付特征采集设备采集到第一视频帧后，输出用于提示支付方提供第一生物特征的提示信息。也即，当采集到包含支付方的面部特征的第一视频帧中，提醒支付方伸出手掌，采集对应的掌纹特征。

步骤 Sb3、采集包含第一生物特征的第二视频帧。也即，生物特征采集设备采集包含支付方掌纹特征的第二视频帧。

具体地，生物特征采集设备在采集包含掌纹特征的第二视频帧时，为了提升掌纹验证的准确度以及降低存储支付方掌纹特征的存储空间，可以从包含的支付方掌纹特征的视频流中截取优选帧作为第二视频帧，其中，优选帧为掌纹清晰且完整的掌纹所属的视频帧，当然还可以包含手掌距离生物特征采集设备的距离适中，以及所采集到的视频帧的亮度合适等。

采用多指标评估的方法从包含支付方掌纹特征的视频流中截取优选帧。具体可采用如下步骤：

清晰度评估：对视频流中的每一帧图像进行拉普拉斯方差计算，拉普拉斯方差越大表示图像越清晰。公式为 $V_{laplace} = Var(\nabla^2 I)$，其中 $V_{laplace}$ 表示拉普拉斯方差，$\nabla^2 I$ 表示对图像 I 进行拉普拉斯变换，Var 表示计算方差。

完整性评估：使用边缘检测算法（如 Canny 算法）检测掌纹的边缘，计算边缘的周长和面积。若周长和面积在预设的合理范围内，则认为掌纹完整。

距离评估：通过深度传感器测量手掌与生物特征采集设备的距离，若距离在预设的适中范围内，则给予较高的得分。

亮度评估：计算图像的平均亮度，若平均亮度在预设的合适范围内，则认为亮度合适。将上述各项评估指标的得分进行加权求和，得到每一帧图像的综合得分。各项评估指标的权重通过以下方法确定：首先，收集一定数量的包含掌纹特征的样本视频帧，并人工标注出其中的优选帧。然后，使用这些样本数据对一个线性回归模型进行训练，以综合得分作为目标变量，各项评估指标的得分作为自变量。训练完成后，模型的系数即为各项评估指标的权重。公式为 $S_{total} = w_1 \times S_{clarity} + w_2 \times S_{integrity} + w_3 \times S_{distance} + w_4 \times S_{brightness}$，

其中 S_{total} 表示综合得分，w_1、w_2、w_3、w_4 分别表示清晰度、完整性、距离、亮度各项评估指标的权重，且 $w_1+w_2+w_3+w_4=1$，$S_{clarity}$ 表示清晰度得分，$S_{integrity}$ 表示完整性得分，$S_{distance}$ 表示距离得分，$S_{brightness}$ 表示亮度得分。选取综合得分最高的帧作为优选帧作为第二视频帧。

步骤 Sb4、若接收到支付成功消息，且，在检测到支付方的第一部位离开拍摄范围时，采集包括支付方的第二生物特征的第三视频帧。

对于本申请实施例，支付特征采集设备可以在得到优选帧后，即发送给支付验证设备进行匹配验证，也即，支付验证设备从各支付方所对应的第一生物特征中确定出匹配的支付方，以完成支付，此时由支付验证设备向支付特征采集设备发送支付成功消息，当支付特征采集设备接收到支付成功消息时即可以输出第二提示信息；其中，第二提示信息用于提示支付方基于第一生物特征支付验证成功，此时支付方的手掌可以离开拍摄范围，在检测到支付方的手掌离开拍摄范围时，采集包括支付方的第二生物特征（面部特征）的第三视频帧。

在本申请实施例中，需要进行说明的是，第一视频帧、第二视频帧以及第三视频帧都可以是帧序列，也即多帧图像，当然，也可以为一帧图像，在本申请实施例中不作限定。再者，在本申请实施例中，采集支付方在支付过程中的第一部位的生物特征和第二部位的生物特征均是由支付方授权同意的。

步骤 Sb5、向支付证据存储设备发送第一视频帧、第三视频帧以及所对应的支付标识，以使得支付证据存储设备中关联存储第一视频帧中所包含的第二生物特征、第三视频帧中所包含的第二生物特征以及支付标识。

进一步地，需要进行说明的是，支付证据存储设备中还可以关联存储有第一视频帧中所包含的第二生物特征、第二视频帧中所包含的第一生物特征、第三视频帧中所包含的第二生物特征以及支付标识。

具体地，支付采集设备在采集到第一视频帧、第二视频帧和第三视频帧后，可以由支付采集设备从各视频帧中提取对应的生物特征，也即从第一视频帧中获取第二生物特征、从第二视频帧中获取第一生物特征以及从第三视频帧中获取第二生物特征，并将这些生物特征以及支付标识存储在支付证据存储设备中；在另一种可能的实现方式中，还可以由支付证据存储设备或者其他设备从各视频帧中提取对应的生物特征，并将这些生物特征以及支付标识存储在支付证据存储设备中。

再者，需要进行说明的是，支付证据存储设备中还可以直接存储视频帧，也即支付证据存储设备中还可以直接关联存储第一视频帧、第三视频帧和支付标识。具体地，还可以关联存储有第二视频帧，也就是说，支付证据存储设备中还可以关联存储有第一视频帧、第二视频帧、第三视频帧以及支付标识。在本申请实施例中，若支付证据存储设备中至少关联存储有第一视频帧、第三视频帧以及支付标识，则支付验证设备在接收到支付证据提供请求时，基于支付证据提供请求中所携带的支付标识，从支付证据存储设备中获取第一视频帧和第三视频帧（当然也可以包括第二视频帧），并向拒付请求处理设备发送第一视频帧和第三视频帧（当然也可以包括第二视频帧）。

拒付请求处理设备从第一视频帧和第三视频帧中解析出各自对应的第二生物特征的具体方法如下：对于第一视频帧和第三视频帧，首先进行图像预处理，包括灰度化处理，将彩色图像转换为灰度图像，以减少数据量和计算复杂度；然后进行直方图均衡化，增强图像的对比度，使图像中的特征更加明显。接着，使用人脸检测算法（如 Haar 级联分类器或深度学习-based 的人脸检测算法）在预处理后的图像中检测人脸区域。检测到人脸区域后，使用特征提取算法（如主成分分析 PCA、线性判别分析 LDA 或深度学习-based 的特征提取网络）从人脸区域中提取第二生物特征（如面部特征向量）。最终得到第一视频帧和

第三视频帧各自对应的第二生物特征。

其中，针对步骤 Sb1-步骤 Sb5 的一个具体示例，如图 5 所示，其中，

1. 收银 Pos 发起支付，传给刷掌终端（支付特征采集设备）传入流水号；

2. 刷掌终端拍照，再提示伸手掌，此步骤中的拍照作为凭证首帧，也即上文所示的第一视频帧；

3. 刷掌终端一直拍摄掌纹，并检测；若刷掌终端在此步骤中并未检测到掌纹，此时返回至步骤 2；

4、从 3 中拍摄的视频流中筛选出优选的图，将优选的图作为凭证中间帧，发送给后台服务器（支付验证设备）进行识别；若刷掌终端未得到优选帧，此时返回步骤 3 中重复拍摄掌纹特征；

5、如果后台服务器识别成功，则刷掌终端提示成功；

6、此时刷掌终端需要再次检索，当手掌离开时进行拍摄，并手掌离开时所拍摄的那帧作为尾帧；

7、刷掌终端将凭证首帧、优选帧以及尾帧以及流水号发送至云端设备进行关联存储。其中，刷掌终端和云端存储设备之间通过传输层安全性协议（Transport Layer Security，TLS）加密。

进一步地，由于在每次支付过程中，支付特征采集设备所采集到的生物特征会存储在支付证据存储设备，也就是说，支付证据存储设备中加密且关联存储有各支付方的第二部位的生物特征与存储密钥，其中，各支付方的第二部位的生物特征是加密算法进行加密存储的，例如可以通过 SM4 加密算法，再者为了进一步地提高存储的安全性，存储密钥也是通过支付标识（例如流水号）、支付方标识（支付方身份 ID）、设备号（支付特征采集设备的设备标识）以及初始密钥通过特定算法（例如 sha64 算法）所计算得到的，其中，初始密钥存储在支付特征采集设备的安全元件（Secure Element，SE）中。进一步地，支付特征采集设备中具体可以加密且关联存储有各支付方的视频帧（第一视频帧、第二视频帧和第三视频帧）的生物特征与存储密钥。

进一步地，由于各支付方所对应的第二生物特征是通过上述加密方式存储在支付证据存储设备中的，因此，步骤 S302 中基于支付标识，获取已完成支付所对应的第二生物特征，具体可以包括：基于支付标识，确定已完成支付所对应的支付方标识；从已完成支付对应的支付特征采集设备中获取设备标识以及初始密钥；对支付标识、支付方标识、设备标识和初始密钥进行加密，得到生物特征存储加密密钥；基于生物特征存储加密密钥，从支付证据存储设备中获取已完成支付所对应的第二生物特征。

其中，可使用 sha64 算法对支付标识、支付方标识、设备标识和初始密钥进行加密，得到生物特征存储加密密钥。具体步骤如下：首先将支付标识、支付方标识、设备标识和初始密钥进行字符串拼接，形成一个新的字符串。然后将该字符串输入到 sha64 算法中进行哈希计算，得到一个 64 位的哈希值，此哈希值即为生物特征存储加密密钥。公式为 $K = sha64\big(concat(PID, UID, DID, IK)\big)$，其中 K 表示生物特征存储加密密钥，PID 表示支付标识，UID 表示支付方标识，DID 表示设备标识，IK 表示初始密钥，$concat$ 表示字符串拼接操作。

在本申请实施例中，基于生物特征存储加密密钥从支付证据存储设备中获取到的加密存储后的第二生物特征（已完成支付所对应的第二生物特征）。当然，支付证据存储设备中可以不直接存储各支付方所对应的第二生物特征，而是存储各支付方分别对应的视频帧（第一视频帧、第二视频帧和第三视频帧）。基于上述实施例，具体地，步骤 S303 中支付验证设备向拒付请求处理设备发送包括第二生物特征的支付证据信息，具体可以包括：支付验证设备向拒付请求处理设备发送包含第一视频帧和第三视频帧的支付证据信息。

其中，支付验证设备向拒付请求处理设备发送包含第一视频帧和第三视频帧的支付证

据信息，其中，支付证据信息中所包含的第一视频帧和第三视频帧是加密的，此时，拒付请求处理设备也还需要对此进行解密，遇得到解密后的第一视频帧和第三视频帧，又或者，支付验证信息在得到支付证据信息中的加密后的第一视频帧和第三视频帧后，先解密后，再向拒付请求处理设备发送。需要进行说明的是，支付验证设备还可向拒付请求处理设备所发送的支付证据信息中还可以包括与之关联的第二视频帧，当然也可以不包含与之关联的第二视频帧，在本申请实施例中不作限定。进一步地，由上述实施例可知，针对一次支付（已完成支付），拒付请求处理设备至少可以得到：第一视频帧所对应的第二生物特征、第三视频帧所对应的第二生物特征，在第一视频帧中所包含第二生物特征与第三视频帧中所包含的第二生物特征相匹配的条件下（也即在第一视频帧和第三视频帧中所包含的面部特征中存在相同的面部特征时，也就是说存在同一张人脸），由拒付请求处理设备通过以下方式（步骤 S1 和步骤 S2）对拒付请求进行处理。具体地，步骤 S1 和步骤 S2 在图中并未示出，其中，上文所示的拒付请求方的特征包括：拒付请求方的第二部位的第五生物特征，例如，拒付请求方的第二部位的第五生物特征也即拒付请求方的面部特征，其中，

步骤 S1、若拒付请求方的第二部位的第五生物特征与指定第二生物特征匹配，则拒绝拒付请求，并向拒付请求方发送第一通知消息。

其中，指定第二生物特征为第一视频帧或者第三视频帧中所包含的第二生物特征；在本申请实施例中，若拒付请求方的第二部位的第五生物特征与指定第二生物特征匹配，则表明已完成支付在实际支付的过程中所采集到的面部特征和拒付请求方的面部特征一致，也即此时表征该已完成支付属于盗刷或者错刷的概率较低，此时，拒付请求处理设备拒绝上述拒付请求，并向拒付请求方发送第一通知消息，第一通知消息中携带有第二生物特征的匹配结果，并用于通知拒付请求方，拒付请求处理设备已拒绝拒付请求。

步骤 S2、若拒付请求方的第二部位的第五生物特征与指定第二生物特征不匹配，则同意拒付请求，并将已支付成功的支付金额返回给拒付请求方的账户。

对于本申请实施例，若拒付请求方的第二部位的第五生物特征与指定第二生物特征不匹配，则表明已完成支付在实际支付的过程中所采集到的面部特征和拒付请求方的面部特征不一致，也即此时表征该已完成支付属于盗刷或者错刷的概率较高，此时，拒付请求处理设备同意拒付请求，并将已支付成功的支付金额返回给拒付请求方的账户，当然为了提高安全性和准确性，此时也可以采用其它错误再次进行核对后，再作为对应的拒付决策（基于拒付请求所作出的决策）。

进一步地，在第一视频帧中所包含第二生物特征与第三视频帧中所包含的第二生物特征相匹配的条件下，若拒付请求方的第二部位的第五生物特征与指定第二生物特征不匹配，表明已完成支付在实际支付的过程中所采集到的面部特征和拒付请求方的面部特征不一致，也即此时表征该已完成支付属于盗刷或者错刷的概率较高，则由拒付请求处理设备执行步骤 S3、步骤 S4、步骤 S5（图中未示出），其中，步骤 S3-步骤 S5 与步骤 S1-步骤 S2，不存在严格的先后执行顺序，具体地，

步骤 S3、将指定第二生物特征与拒付请求方存在关联关系的对象所对应的第二生物特征进行匹配。

对于本申请实施例，拒付请求方的账户（该已完成支付的账户）除了绑定有拒付请求方的第一部位的第一生物特征（也即掌纹特征）外，还可能绑定有与之存在关联关系的其他对象的掌纹特征，例如，亲属的掌纹特征，也即，此时该已完成支付也可能是与之关联的对象刷掌纹所进行支付的。则此时拒付请求方的面部特征与支付过程中所采集到的面部特征（第一视频帧和第三视频帧中的面部特征）不一致，此时获取与拒付请求方存在关联关系的对象的面部特征（此获取功能是由拒付请求方同意的，或者拒付请求方提供的），进而将第一视频帧和第三视频帧中的面部特征与拒付请求方存在关联关系的对象的面部特征进行匹配。

例如，与拒付请求方存在关联关系的对象可以包括：对象 1 和对象 2，即将对象 1 的

面部特征和对象 2 的面部特征与第一视频帧和第三视频帧中的面部特征进行匹配。

步骤 S4、若存在关联关系的对象中存在第二生物特征相匹配的关联匹配对象，则向拒付请求方发送携带关联匹配对象的第二生物特征的第二通知消息。

例如，若对象 1 的面部特征与第一视频帧和第三视频帧中的面部特征匹配，则将携带对象 1 的面部特征的第二通知消息发送给拒付请求方。

其中，第二通知消息用于通知拒付请求方已完成支付是由关联匹配对象完成的。

步骤 S5、接收拒付请求方针对第二通知消息的回复信息，并基于回复信息对拒付请求进行处理。

对于本申请实施例，拒付请求方在接收到第二通知消息后，若拒付请求方认可，则向拒付请求处理设备发送针对第二通知消息的回复消息，并且该回复消息中表明拒付请求方认可该已完成支付（或者，认可撤回拒付请求），此时可以结束；若该回复消息中表明不认可该拒付请求，此时拒付请求处理设备还可以驳回该拒付请求，也可以将该拒付请求发送给其它机构的设备进行处理，或者采用其它方式进行处理，不作限定。

进一步地，在第一视频帧中所包含第二生物特征与第三视频帧中所包含的第二生物特征不匹配的条件下，也即，支付特征采集设备采集支付方在支付前后的视频帧中的面部特征不匹配，也就是说，第一视频帧所采集的面部特征和第三视频帧所采集到的面部特征并非是同一人的面部特征；为了合理对所提交的生物特征进行处理，以对拒付请求进行准确的处理；由拒付请求处理设备通过步骤 S6 以及步骤 S7 对拒付请求进行处理（图中并未示出），其中，步骤 S6-步骤 S7 和上文的步骤 S1-步骤 S5 不存在严格的先后执行顺序，具体地，

步骤 S6、若第一视频帧所包含的第二生物特征与拒付请求方的第二生物特征相匹配，则按照已完成支付所对应的支付时间，获取第一已完成支付方所对应的第七生物特征，并将第七生物特征与第三视频帧所包含的第二生物特征进行匹配，基于匹配结果对拒付请求进行处理。

对于本申请实施例，第一视频帧所包含的第二生物特征与拒付请求方的第二生物特征相匹配，也即，支付特征采集设备在支付方在支付前（第二视频帧）之前可能采集到了支付方的面部特征，但是在支付方的支付后并未采集到支付方的面部特征，此时拒付请求处理设备从支付验证设备获取到第一已完成支付方所对应的面部特征，以与第三视频帧中所包含的面部特征进行匹配。

其中，第一已完成支付方为在已完成支付之后完成支付的支付方；其中，第七生物特征为第一已完成支付方所对应的第二部位的生物特征。

进一步地，若拒付请求处理设备从支付验证设备获取到第一已完成支付方所对应的面部特征，以与第三视频帧中所包含的面部特征进行匹配，且匹配成功，则表征并未存在刷错的情况，则拒绝拒付请求方的拒付请求，或者采取其它措施以对拒付请求进行处理，在本申请实施例中不作限定。

步骤 S7、若第三视频帧所包含的第二生物特征与拒付请求方的第二生物特征相匹配，则按照已完成支付所对应的支付时间，获取第二已完成支付方所对应的第八生物特征，并将第八生物特征与第一视频帧所包含的第二生物特征进行匹配，基于匹配结果对拒付请求进行处理。

对于本申请实施例，第三视频帧所包含的第二生物特征与拒付请求方的第二生物特征相匹配，也即，支付特征采集设备在支付方在支付后（第二视频帧）之后可能采集到了支付方的面部特征，但是在支付方的支付前并未采集到支付方的面部特征，此时拒付请求处理设备从支付验证设备获取到第二已完成支付方所对应的面部特征，以与第一视频帧中所包含的面部特征进行匹配。

其中，第二已完成支付方为在已完成支付之前完成支付的支付方；其中，第八生物特征为第二已完成支付方所对应的第二部位的生物特征。

进一步地，若拒付请求处理设备从支付验证设备获取到第二已完成支付方所对应的面部特征，以与第一视频帧中所包含的面部特征进行匹配，且匹配成功，则表征并未存在刷错的情况，则拒绝拒付请求方的拒付请求，或者采取其它措施以对拒付请求进行处理，在本申请实施例中不作限定。

进一步地，在某些情况下，拒付请求方在针对某一账户去绑定第一部位的生物特征（掌纹）时存在绑错的情况，例如，绑定了其它人的第一部位的生物特征，为了提升对拒付请求处理的准确性，在得到已完成支付的支付标识，此时该方法还可以包括：基于支付标识，确定已完成支付所对应的支付方标识；确定支付方标识所绑定的第三生物特征。其中，基于支付标识，支付验证设备通过查询本地数据库中预先构建的支付标识与支付方标识的关联表来确定已完成支付所对应的支付方标识。该关联表的构建过程如下：在每笔支付完成时，支付验证设备接收支付特征采集设备发送的支付标识（如流水号）和支付方标识（如支付对象标识），并将这两者的对应关系存储在本地数据库的关联表中。关联表以支付标识为索引，方便快速查询。若本地数据库中未查询到相关信息，则向云端存储设备发送查询请求，云端存储设备根据支付标识在其存储的海量交易数据中进行检索。检索时，云端存储设备会对存储的数据进行分区管理，按照支付时间、支付金额等维度进行划分，以提高检索效率。找到对应的支付方标识后，将其反馈给支付验证设备。

在本申请实施例中，在通过支付证据提供请求中得到已完成支付的支付标识后，基于支付标识确定出已完成支付所对应的支付方标识，也即，支付验证设备中可以存储有支付标识与支付方标识之间的映射关系，也可以从其它设备（例如云端存储设备中）获取支付标识与支付方标识之间的映射关系。

进一步地，在另一种可能的实现方式中，支付验证设备所接收到的支付证据提供请求中携带有支付方标识。在本申请实施例中，支付证据提供请求中所携带的支付方标识可以由拒付请求方所触发的拒付请求中携带，还可以是拒付请求处理设备在接收到拒付请求后，基于拒付请求中所携带的支付标识所确定出，并携带在支付证据提供请求中。

例如，支付标识为已完成支付的流水号，支付方标识为已完成支付的实际支付方的身份 ID。

进一步地，支付验证设备在得到已完成支付所对应的支付方标识（已完成支付的实际支付方的身份 ID）后，确定支付方标识所绑定的第三生物特征。其中，第三生物特征是支付方标识对应的对象所注册的第一部位的生物特征。由上述实施例可知，第一部位的生物特征可以为掌纹特征，也即第三生物特征是支付方标识对应的对象所注册的掌纹特征（也可以称为支付关联掌纹特征），也就是说，每一次支付，若支付采集设备所采集的掌纹特征和支付关联掌纹特征匹配，则表征验证通过，可以使得从该支付方标识所对应的账户中划取该支付所对应的金额。例如，支付方 1 购买了 10 元的苹果，支付方 1 通过刷掌的方式，与支付关联掌纹特征匹配，则从该支付关联掌纹特征所绑定的账户中划取 10 元至商户的账户。支付关联掌纹特征是支付方标识对应的对象所注册的掌纹特征，每一次支付时，支付采集设备会将采集到的掌纹特征与该支付关联掌纹特征进行匹配。若匹配成功，则表征验证通过，可从该支付方标识所对应的账户中划取该支付所对应的金额，是支付验证的重要依据之一。

为了提高所提供的证据的合理性，以进一步地更为准确地对付款方所发起的拒付请求的交易进行验证，进一步地，支付验证设备向拒付请求处理设备所提供的支付证据中还可以包括：第三生物特征，也即包括支付方标识所对应的对象所注册的第一部位的生物特征，由上述实施例可知，第一部位的生物特征可以为掌纹特征，第三生物特征为已完成支付的实际支付方为某一电子账户（电子账户 1）所绑定的掌纹特征（支付关联掌纹特征），也就是说，在支付的过程中，若支付验证设备匹配到与之相应的掌纹特征，表征验证通过，此时可以从电子账户 1 中划取对应的金额；

进一步地，拒付请求方的生物特征包括拒付请求方的第一部位的第四生物特征和第二

部位的第五生物特征，匹配程度包括第二生物特征和第五生物特征的匹配程度、以及第三生物特征和第四生物特征的匹配程度。也就是说，在上述实施例中根据支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对拒付请求进行处理时，除了根据拒付请求方的第五生物特征（面部特征）和第二生物特征（支付过程中所采集的面部特征）进行匹配，还需要根据拒付请求方的第一部位的第四生物特征（掌纹）和其账户所绑定的第五生物特征（其账户所绑定的掌纹特征）进行匹配，若上述两种匹配结果均高于预设匹配程度，则表征拒付请求中拒付请求方和实际支付过程中所采集到的支付方为同一人，也即不存在盗刷，或者刷错（其后边的支付的支付方刷错，或者其前面的支付的支付方刷错）的情况，则拒绝该拒付请求；其它的情况详见上述实施例，在此不在赘述。

本申请实施例还提供了另一种拒付请求的处理方法，由拒付请求处理设备执行，如图6所示，该方法可以包括：

步骤S601、向支付验证设备发送支付证据提供请求；其中，支付证据提供请求中携带已完成支付所对应的支付标识；支付证据提供请求是拒付请求处理设备接收到携带支付标识的拒付请求时发送的；已完成支付是基于第一生物特征进行支付且已支付成功的支付；第一生物特征是在已完成支付的支付过程中采集的支付方的第一部位的生物特征。

其中，支付证据提供请求中携带已完成支付所对应的支付标识；支付证据提供请求是拒付请求处理设备接收到携带支付标识的拒付请求时发送的；已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，第一生物特征是在已完成支付的支付过程中采集的支付方的第一部位的生物特征。

步骤S602、接收支付验证设备发送的包括第二生物特征的支付证据信息；第二生物特征是由支付验证设备基于支付标识获取到的；其中，第二生物特征是在支付过程中所采集的第二部位的生物特征。

其中，第二生物特征是由支付验证设备基于支付标识获取到的；其中，第二生物特征是在支付过程中所采集的第二部位的生物特征。

步骤S603、确定支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度，并基于匹配程度，对拒付请求进行处理。

具体地，第二生物特征包括：两个视频帧分别对应的第二生物特征信息，一个视频帧是由支付特征采集设备在采集支付方的第一生物特征之前所采集到的视频帧，另一视频帧是由支付特征采集设备在检测到支付方的第一生物特征离开拍摄范围时所采集到的视频帧；

其中，步骤S603中确定支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度，并基于匹配程度，对拒付请求进行处理，具体可以包括：获取拒付请求方的第二部位的第五生物特征；基于两个视频帧分别对应的第二生物特征信息以及第五生物特征确定支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度；基于匹配程度，对拒付请求进行处理。

其中，可采用特征点匹配算法来确定匹配程度。首先，对两个视频帧分别对应的第二生物特征信息和第五生物特征进行特征提取，得到各自的特征点集合。然后，使用SIFT（尺度不变特征变换）算法在这些特征点集合中寻找匹配的特征点对。匹配的特征点对是在使用特征点匹配算法（如SIFT算法）对两个生物特征信息进行匹配时，从各自的特征点集合中找到的相互对应的特征点组合。通过计算这些匹配的特征点对的特征向量之间的欧氏距离，并对所有匹配特征点对的欧氏距离进行求和取平均值，得到平均欧氏距离，进而以平均欧氏距离的倒数作为匹配程度，用于判断生物特征之间的相似性。

对于每一个匹配的特征点对，计算其特征向量之间的欧氏距离。将所有匹配特征点对的欧氏距离进行求和并取平均值，得到平均欧氏距离。最后，将平均欧氏距离的倒数作为匹配程度。公式为 $M=\frac{1}{\frac{1}{n}\sum_{i=1}^{n}d_i}$，其中 M 表示匹配程度，n 表示匹配的特征点对的数量，

d_i 表示第 i 个匹配特征点对的欧氏距离。

需要进行说明的是，在本申请实施例中由拒付请求处理设备所执行的流程详见上述实施例，在此不再赘述。

为了更好的理解和说明书本申请实施例提供的方案的实用价值，下面结合具体的场景实施例对本申请的可选实施方式进行说明。

一、支付流程：

1、收银 POS 给刷掌终端发送支付请求，其中，支付请求中携带当前所支付账单的流水号，此支付在后文中称为支付 1；

2、刷掌终端启动拍照，得到在刷掌之前的几帧图像，以用于拍摄到待进行刷掌的支付对象的面部特征，作为初始帧；

3、提示支付对象伸掌，以刷取掌纹；

4、刷掌终端检测到支付手掌后，拍摄掌纹；其中，当刷掌终端检测到支付掌纹后，可以拍摄预设时间段的掌纹，然后提醒支付对象移开手掌，又或者，当检测到拍摄到清晰且完整的掌纹后，可以提醒支付对象移开手掌），其中，将清晰且完整的掌纹作为优选帧；

5、刷掌终端将所选取的帧（优选帧）发送给后台服务器进行识别，以确定支付对象的身份，并发送给发卡行，以由发卡行从对应的账户进行扣款支付；

6、当后台服务器识别到相匹配的掌纹，则向刷掌终端发送匹配成功的指示信息；

7、刷掌终端输出提示信息，以提示支付对象移开手掌；

8、当刷掌终端检测到支付对象移开手掌后，再次进行拍摄，以拍摄到刚才进行刷掌的支付对象的面部特征，作为尾帧；

9、刷掌终端将全部帧（初始帧、优选帧以及尾帧）通过存储密钥并采用 SM4 的方式进行加密；其中，存储密钥是由流水号、识别成功用户 ID（支付对象标识）、设备号和初始密钥，并采用 sha64 进行加密后得到的；其中，初始密钥存储在刷掌终端的安全元件（Secure Element，SE）中。

二、当检测到拒付请求时，提供证据，以对拒付请求进行决策的流程：

1、发卡行的设备在检测到拒付请求方所发送的针对支付 1 的拒付请求时，生成支付证据提供请求，发送给收单行设备，其中，支付证据提供请求用于请求支付 1 所对应的支付证据，以对拒付请求进行决策；

2、收单行设备将支付证据提供请求发送给对应的商户设备；若商户设备接受拒付，此时可以由收单行设备将商户接受拒付的消息给发卡行的设备，以使得发卡行设备将所支付 1 所支付的金额返回给拒付请求方的账户；

3、若商户不接受拒付，则商户设备向后台服务器（支付验证设备）发送携带流水号的支付证据提供请求；进一步地，该支付证据提供请求中还携带有拒付请求方的身份标识、刷掌终端的设备标识以及初始密钥（从刷掌终端的 SE 中获取）；

4、后台服务器基于拒付请求方的身份标识、刷掌终端的设备标识以及初始密钥以及流水号，得到存储密钥，基于存储密钥从云端存储中获取支付 1 所对应的支付证据，该支付证据中至少可以包括：初始帧和尾帧；

5、后台服务器可以通过收单行设备将支付证据透传给发卡行设备；

6、发卡行设备可以获取拒付请求方的面部特征，若拒付请求方的面部特征与初始帧中所包含的面部特征相匹配，以及和尾帧中所包含的面部特征相匹配，则拒绝该拒付请求；若拒付请求方的面部特征与初始帧和尾帧中所包含的面部特征均不匹配，则发卡行设备将所支付 1 所支付的金额返回给拒付请求方的账户，并通知对应的商户设备；或者，若拒付请求方的面部特征与初始帧和尾帧中所包含的面部特征均不匹配，则将证据和验证结果发送至对应的机构进行处理；

若拒付请求方的面部特征与初始帧中所包含的面部特征匹配，但与尾帧中所包含的面部特征不匹配，又或者，拒付请求方的面部特征与尾帧中所包含的面部特征相匹配，但与

初始帧中所包含的面部特征不匹配，则可以采取其它措施，或者发送给相关机构继续进行处理。

进一步地，除此之外的 IOT 终端措施，以提升支付的安全性：

风控措施：增加基于机器学习的风控模型，该模型采用随机森林算法对交易数据进行实时分析。具体步骤如下：首先，收集交易数据，包括交易金额、交易时间、交易地点、交易频率等特征，并将其划分为训练集和测试集。然后，使用训练集对随机森林模型进行训练。在训练过程中，通过调整模型的参数来优化模型的性能。对于树的数量，从较小的值（如 10 棵树）开始尝试，逐步增加树的数量，观察模型在测试集上的准确率、召回率等指标的变化，当这些指标不再有明显提升时，确定合适的树的数量。对于最大深度，同样采用逐步尝试的方法，从较小的深度（如 3 层）开始，逐渐增加深度，避免过拟合现象的发生。同时，还可以调整其他参数，如最小样本分割数、最小样本叶子数等。在实时分析阶段，将新的交易数据输入到训练好的模型中，模型会根据特征计算出该交易的风险概率。例如，若短时间内同一账户在不同地区发起多笔大额交易，模型计算出的风险概率超过预设的阈值（如 0.8），则判定为可能存在风险。当模型识别到可能的风险时，增加加验手段，如要求用户输入额外的短信验证码、进行人脸识别或者指纹识别等，以此减少欺诈可能性。

限额措施：超出限额增加 3DS 验证，确保高风险交易有责任转移。具体根据用户的历史交易数据和信用评级设定不同的交易限额的方法如下：首先，对用户的历史交易数据进行分析，包括交易金额的分布、交易频率、交易稳定性等特征。同时，获取用户的信用评级信息，信用评级可以从专业的信用评级机构获取，或者根据用户在银行的信用记录自行评估。然后，使用线性回归模型来计算单笔交易限额和日累计交易限额。公式为 $L_{single} = \alpha_1 \times A_{avg} + \alpha_2 \times C + \beta_1$ 和 $L_{daily} = \gamma_1 \times A_{total} + \gamma_2 \times C + \beta_2$，其中 L_{single} 表示单笔交易限额，L_{daily} 表示日累计交易限额，A_{avg} 表示用户历史交易的平均金额，A_{total} 表示用户历史交易的日累计平均金额，C 表示用户的信用评级得分，α_1、α_2、γ_1、γ_2 是模型的系数，β_1、β_2 是常数项。这些系数和常数项可以通过对大量用户数据进行训练得到。当交易金额超出设定的限额时，增加 3DS（3D Secure）验证。具体流程为：当交易触发限额时，发卡行将向用户的注册手机发送验证码，用户需要在支付页面输入该验证码进行验证。同时，用户还可能需要在发卡行的手机银行 APP 或者网页上进行授权确认，验证成功后才能完成交易，以此确保高风险交易有责任转移。

设备和数据安全：设备布设在商家端，需要确保设备有极高安全性，不会被攻破以及篡改。

算法可靠：极低的误识别率、权威认证等，在业内建立起可靠的预期。

进一步地，在上述实施例所介绍的方案的基础，本申请实施例可以增强安全性：掌纹识别是生物识别技术，具有唯一性和难以伪造的特点，可以提高支付的安全性；进一步地可以提高使用体验：相比传统的 3DS 认证（如输入密码或一次性验证码），掌纹识别可能提供更顺畅的支付体验，减少使用者放弃交易的可能性；即时验证：生物识别技术可以快速验证用户身份，降低由于输入错误导致的拒付风险。

基于与本申请实施例提供的拒付请求的处理方法相同的原理，本申请实施例还提供了一种拒付请求的处理装置，如图 7 所示，该装置 70 可以设置在支付验证设备中，其中该装置 70 可以包括：

支付证据提供请求接收模块 71，用于接收拒付请求处理设备发送的针对已完成支付的支付证据提供请求，其中，支付证据提供请求中携带已完成支付的支付标识；支付证据提供请求是拒付请求处理设备接收到携带支付标识的拒付请求时发送的；已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，第一生物特征是在已完成支付的支付

过程中采集的支付方的第一部位的生物特征；

获取模块 72，用于基于支付标识，获取已完成支付所对应的第二生物特征；其中，第二生物特征是在已完成支付的支付过程中所采集的支付方的第二部位的生物特征；

支付证据信息发送模块 73，用于向拒付请求处理设备发送包括第二生物特征的支付证据信息，以使拒付请求处理设备基于支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对拒付请求进行处理。

本申请实施例的一种可能的实现方式，装置 70 还包括：第一确定模块以及第二确定模块，其中，

第一确定模块，用于基于支付标识，确定已完成支付所对应的支付方标识；

第二确定模块，用于确定支付方标识所绑定的第三生物特征；其中，第三生物特征是支付方标识对应的对象所注册的第一部位的生物特征；

其中，支付证据信息还包括第三生物特征，拒付请求方的生物特征包括拒付请求方的第一部位的第四生物特征和第二部位的第五生物特征，匹配程度包括第二生物特征和第五生物特征的匹配程度、以及第三生物特征和第四生物特征的匹配程度。

本申请实施例的一种可能的实现方式，获取模块 72 在基于支付标识，获取已完成支付所对应的第二生物特征时，具体用于：

向支付证据存储设备发送生物特征获取请求；其中，生物特征获取请求中包括支付标识；支付证据存储设备中存储有各支付的支付标识所对应的支付方的第二部位的生物特征；

接收支付证据存储设备发送的已完成支付所对应的第二生物特征。

本申请实施例的另一种可能的实现方式，支付证据信息是由支付特征采集设备通过以下方式采集，并存储至支付证据存储设备的：

接收针对已完成支付的支付请求；

响应于支付请求，获取生物特征采集视频流，并在接收到支付成功信息时，将支付方的第一生物特征和第二生物特征存储至支付证据存储设备中；其中，生物特征采集视频流至少包括支付方的第一生物特征和第二生物特征。

本申请实施例的另一种可能的实现方式，获取生物特征采集视频流，并在接收到支付成功消息时，将第二生物特征存储至支付证据存储设备中，包括：

采集第一视频帧；其中，第一视频帧中包含有支付方所对应的第二生物特征；

输出第一提示信息，第一提示信息用于提示支付方提供第一生物特征；

采集包含第一生物特征的第二视频帧；

若接收到支付成功消息，且，在检测到支付方的第一部位离开拍摄范围时，采集包括支付方的第二生物特征的第三视频帧；

向支付证据存储设备发送第一视频帧、第三视频帧以及所对应的支付标识，以使得支付证据存储设备中关联存储第一视频帧中所包含的第二生物特征、第三视频帧中所包含的第二生物特征以及支付标识。

本申请实施例的另一种可能的实现方式，第一视频帧中所包含第二生物特征与第三视频帧中所包含的第二生物特征相匹配；

其中，支付证据信息发送模块 73 在向拒付请求处理设备发送包括第二生物特征的支付证据信息时，具体用于：

向拒付请求处理设备发送包含第一视频帧和第三视频帧的支付证据信息，以由拒付请求设备通过以下方式对拒付请求进行处理：

若拒付请求方的第二部位的第五生物特征与指定第二生物特征匹配，则拒绝拒付请求，并向拒付请求方发送第一通知消息；其中，指定第二生物特征为第一视频帧或者第三视频帧中所包含的第二生物特征；第一通知消息中携带有第二生物特征的匹配结果，并用于通知拒付请求方，拒付请求处理设备已拒绝拒付请求。

本申请实施例的另一种可能的实现方式，以由拒付请求设备通过以下方式对拒付请求

进行处理：

若拒付请求方的第二部位的第五生物特征与指定第二生物特征不匹配，将指定第二生物特征与拒付请求方存在关联关系的对象所对应的第二生物特征进行匹配；

若存在关联关系的对象中存在第二生物特征相匹配的关联匹配对象，则向拒付请求方发送携带关联匹配对象的第二生物特征的第二通知消息；其中，第二通知消息用于通知拒付请求方已完成支付是由关联匹配对象完成的；

接收拒付请求方针对第二通知消息的回复信息，并基于回复信息对拒付请求进行处理。

本申请实施例的另一种可能的实现方式，由所述拒付请求设备通过以下任一方式对所述拒付请求进行处理：

若所述拒付请求方的第二部位的第五生物特征与指定第二生物特征不匹配，则同意所述拒付请求，并将已支付成功的支付金额返回给拒付请求方的账户。

本申请实施例的另一种可能的实现方式，第一视频帧中所包含第二生物特征与第三视频帧中所包含的第二生物特征不匹配；

其中，支付证据信息发送模块 73 在向拒付请求处理设备发送包括第二生物特征的支付证据信息时，具体用于：

向拒付请求处理设备发送包含第一视频帧和第三视频帧的支付证据信息，以由拒付请求设备通过以下方式对拒付请求进行处理：

若第一视频帧所包含的第二生物特征与拒付请求方的第二生物特征相匹配，则按照已完成支付所对应的支付时间，获取第一已完成支付方所对应的第七生物特征，并将第七生物特征与第三视频帧所包含的第二生物特征进行匹配，基于匹配结果对拒付请求进行处理；其中，第一已完成支付方为在已完成支付之后完成支付的支付方；其中，第七生物特征为第一已完成支付方所对应的第二部位的生物特征；

若第三视频帧所包含的第二生物特征与拒付请求方的第二生物特征相匹配，则按照已完成支付所对应的支付时间，获取第二已完成支付方所对应的第八生物特征，并将第八生物特征与第一视频帧所包含的第二生物特征进行匹配，基于匹配结果对拒付请求进行处理；其中，第二已完成支付方为在已完成支付之前完成支付的支付方；其中，第八生物特征为第二已完成支付方所对应的第二部位的生物特征。

本申请实施例的另一种可能的实现方式，支付证据存储设备中关联存储各支付方的第二部位的生物特征与存储密钥，一个支付方的存储密钥是基于该支付方的支付标识、支付方标识、初始密钥和对应的支付特征采集设备的设备标识进行加密后得到的；初始密钥存储在支付特征采集设备中；

其中，获取模块 72 在基于支付标识，获取已完成支付所对应的第二生物特征时，具体用于：

基于支付标识，确定已完成支付所对应的支付方标识；

从已完成支付对应的支付特征采集设备中获取设备标识以及初始密钥；

对支付标识、支付方标识、设备标识和初始密钥进行加密，得到生物特征存储加密密钥；

基于生物特征存储加密密钥，从支付证据存储设备中获取已完成支付所对应的第二生物特征。

本申请实施例还提供了另一种拒付请求处理的装置，如图 8 所示，该装置 80 设置在拒付请求处理设备中，该装置 80 可以包括：

支付证据提供请求发送模块 81，用于向支付验证设备发送支付证据提供请求；其中，支付证据提供请求中携带已完成支付所对应的支付标识；支付证据提供请求是拒付请求处理设备接收到携带支付标识的拒付请求时发送的；已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，第一生物特征是在已完成支付的支付过程中采集的支付方的第一部位的生物特征；

支付证据信息接收模块 82，用于接收支付验证设备发送的包括第二生物特征的支付证据信息；第二生物特征是由支付验证设备基于支付标识获取到的；其中，第二生物特征是在支付过程中所采集的第二部位的生物特征；

匹配程度确定模块 83，用于确定支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度；

拒付请求处理模块 84，用于基于匹配程度，对拒付请求进行处理。

本申请实施例的一种可能的实现方式，第二生物特征包括：两个视频帧分别对应的第二生物特征信息，一个视频帧是由支付特征采集设备在采集支付方的第一生物特征之前所采集到的视频帧，另一视频帧是由支付特征采集设备在检测到支付方的第一生物特征离开拍摄范围时所采集到的视频帧；

其中，匹配程度确定模块 83 在确定支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度时，具体用于：

获取拒付请求方的第二部位的第五生物特征；

基于两个视频帧分别对应的第二生物特征信息以及第五生物特征确定支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度。

本申请实施例提供了一种拒付请求的处理装置，在本申请实施例中，拒付请求处理设备在接收到携带支付标识的拒付请求时，并且该支付标识所对应的已完成支付是基于第一生物特征进行支付且已经支付成功的支付，此时拒付请求设备向支付验证设备发送针对已完成支付的支付证据提供请求，支付验证设备基于支付标识获取该已完成支付在支付过程中所采集的支付方的第二部位的生物特征，并向拒付请求处理设备发送包含该支付方的第二部位的生物特征的支付证据信息，以使得拒付请求处理设备基于支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对拒付请求进行处理。也就是说，拒付请求处理设备所得到的针对已完成支付的支付证据信息中携带有该支付方的第二部位的生物特征，以使得拒付请求处理设备基于该支付方的第二部位的生物特征与拒付请求方的生物特征进行匹配，以确定已完成支付的支付方与拒付请求方是否一致，若一致，则已完成支付为拒付请求方本人的支付，如若不一致，则已完成支付可能不是拒付请求方本人的支付，也即所提供的证据为支付方在支付过程中的另一部位的生物特征，以使得所提供的证据对于验证付款方所发起的拒付请求的交易是否为本人更为合理，从而可以准确地对付款方所发起的拒付请求的交易进行验证。

图 9 示出了本发明实施例所适用的一种电子设备的结构示意图，如图 9 所示，该电子设备可以为上文所示的支付验证设备、拒付请求处理设备、支付特征采集设备等，如该电子设备为上文所示的支付验证设备可以用于实施由支付验证设备所执行的任一实施例中提供的方法；如该电子设备为上文所示的拒付请求处理设备，可以用于实施由上文中由拒付请求处理设备所执行的任一实施例中提供的方法；如该电子设备为上文所示的支付特征采集设备，可以用于实施由上文中由支付特征采集设备所执行的任一实施例中提供的方法。

如图 9 中所示，该电子设备 2000 主要可以包括至少一个处理器 2001（图 9 中示出了一个）、存储器 2002、通信模块 2003 和输入/输出接口 2004 等组件，可选的，各组件之间可以通过总线 2005 实现连接通信。需要说明的是，图 9 中示出的该电子设备 2000 的结构只是示意性的，并不构成对本申请实施例提供的方法所适用的电子设备的限定。

其中，存储器 2002 可以用于存储操作系统和应用程序等，应用程序可以包括在被处理器 2001 调用时实现本发明实施例所示方法的计算机程序，还可以包括用于实现其他功能或服务的程序。存储器 2002 可以是 ROM（Read Only Memory，只读存储器）或可存储静态信息和指令的其他类型的静态存储设备，RAM（Random Access Memory，随机存取存储器）或者可存储信息和计算机程序的其他类型的动态存储设备，也可以是 EEPROM（Electrically Erasable Programmable Read Only Memory，电可擦可编程只读存储器）、CD-ROM（Compact Disc Read Only Memory，只读光盘）或其他光盘存储、光碟存储（包括压

缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。

处理器 2001 通过总线 2005 与存储器 2002 连接，通过调用存储器 2002 中所存储的应用程序实现相应的功能。其中，处理器 2001 可以是 CPU（Central Processing Unit，中央处理器），通用处理器，DSP（Digital Signal Processor，数据信号处理器），ASIC（Application Specific Integrated Circuit，专用集成电路），FPGA（Field Programmable Gate Array，现场可编程门阵列）或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合，其可以实现或执行结合本发明公开内容所描述的各种示例性的逻辑方框，模块和电路。处理器 2001 也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP 和微处理器的组合等。

电子设备 2000 可以通过通信模块 2003（可以包括但不限于网络接口等组件）连接到网络，以通过网络与其它设备（如用户终端或服务器等）的通信，实现数据的交互，如向其他设备发送数据或从其他设备接收数据。其中，通信模块 2003 可以包括有线网络接口和/或无线网络接口等，即通信模块可以包括有线通信模块或无线通信模块中的至少一项。

电子设备 2000 可以通过输入/输出接口 2004 可以连接所需要的输入/输出设备，如键盘、显示设备等，电子设备 200 自身可以具有显示设备，还可以通过接口 2004 外接其他显示设备。可选的，通过该接口 2004 还可以连接存储装置，如硬盘等，以可以将电子设备 2000 中的数据存储到存储装置中，或者读取存储装置中的数据，还可以将存储装置中的数据存储到存储器 2002 中。可以理解的，输入/输出接口 2004 可以是有线接口，也可以是无线接口。根据实际应用场景的不同，与输入/输出接口 2004 连接的设备，可以是电子设备 2000 的组成部分，也可以是在需要时与电子设备 2000 连接的外接设备。

用于连接各组件的总线 2005 可以包括一通路，在上述组件之间传送信息。总线 2005 可以是 PCI（Peripheral Component Interconnect，外设部件互连标准）总线或 EISA（Extended Industry Standard Architecture，扩展工业标准结构）总线等。根据功能的不同，总线 2005 可以分为地址总线、数据总线、控制总线等。

可选的，对于本发明实施例所提供的方案而言，存储器 2002 可以用于存储执行本发明方案的计算机程序，并由处理器 2001 来运行，处理器 2001 运行该计算机程序时实现本发明实施例提供的方法或装置的动作。

基于与本申请实施例提供的方法相同的原理，本申请实施例提供了一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，计算机程序被处理器执行时可实现前述方法实施例的相应内容。

本申请实施例还提供了一种计算机程序产品，该产品包括计算机程序，该计算机程序被处理器执行时可实现前述方法实施例的相应内容。

综上所述，本申请提供一种拒付请求的处理方法、装置、设备、计算机可读存储介质和计算机程序产品，支付验证设备接收拒付请求处理设备发送的携带已完成支付的支付标识的支付证据提供请求，该请求是在拒付请求处理设备接收到携带相同支付标识的拒付请求时发出的，且已完成支付是基于支付过程中采集的支付方第一部位的第一生物特征支付成功的。接着，支付验证设备基于支付标识获取已完成支付对应的支付方第二部位的第二生物特征，并向拒付请求处理设备发送包含该第二生物特征的支付证据信息，使拒付请求处理设备基于支付证据信息中的生物特征和拒付请求方生物特征的匹配程度处理拒付请求。通过引入第二部位的生物特征作为支付证据，增加了生物特征验证的维度，相较于单一生物特征验证，能更全面地反映支付方的身份特征，从而提高了对付款方拒付请求交易验证的准确性。不同部位的生物特征具有不同的特征信息，结合使用可降低因单一生物特征易被伪造或出现误差而导致的误判概率，增强了支付验证的可靠性，保障了支付交易的安全性。

进一步地，支付验证设备在接收到支付证据提供请求后，还基于支付标识确定已完成支付对应的支付方标识，并确定该支付方标识所绑定的第三生物特征，即支付方标识对应的对象所注册的第一部位的生物特征。支付证据信息中除了第二生物特征，还包括第三生物特征，拒付请求方的生物特征包括其第一部位的第四生物特征和第二部位的第五生物特征，匹配程度综合考虑第二生物特征和第五生物特征、第三生物特征和第四生物特征的匹配情况。这种多维度的生物特征匹配方式，从不同角度对支付方和拒付请求方的身份进行验证，减少了因生物特征个体差异或环境因素导致的验证误差。多个生物特征的综合验证，提高了身份识别的准确性和可靠性，使得对拒付请求的处理更加科学合理，降低了误判和漏判的可能性。

进一步地，支付验证设备基于支付标识获取已完成支付对应的第二生物特征时，会向支付证据存储设备发送包含支付标识的生物特征获取请求，支付证据存储设备存储有各支付的支付标识对应的支付方第二部位的生物特征，支付验证设备接收该存储设备发送的已完成支付对应的第二生物特征。通过专门的支付证据存储设备集中存储生物特征，实现了生物特征数据的统一管理。这种集中存储方式便于对数据进行分类、索引和检索，提高了数据查询的效率。同时，集中存储也有利于对数据进行安全防护，采用统一的安全策略和技术手段，保障生物特征数据的完整性和保密性，防止数据泄露和篡改，为后续准确处理拒付请求提供了可靠的数据基础。

进一步地，支付证据信息由支付特征采集设备采集并存储至支付证据存储设备。支付特征采集设备接收针对已完成支付的支付请求，响应请求获取至少包含支付方第一生物特征和第二生物特征的生物特征采集视频流，并在接收到支付成功信息时，将支付方的第一生物特征和第二生物特征存储至支付证据存储设备。在支付过程中同步采集生物特征，确保了数据的及时性和准确性。采集的生物特征是在支付行为发生时实时获取的，反映了支付方当时的真实身份信息，避免了事后采集可能出现的信息偏差或伪造情况。同时，将生物特征及时存储至支付证据存储设备，便于后续在处理拒付请求时快速获取相关数据，提高了处理流程的效率。

进一步地，支付特征采集设备获取生物特征采集视频流并存储第二生物特征的过程包括：采集包含支付方第二生物特征的第一视频帧，输出提示支付方提供第一生物特征的第一提示信息，采集包含第一生物特征的第二视频帧，若接收到支付成功消息且检测到支付方第一部位离开拍摄范围时，采集包含支付方第二生物特征的第三视频帧，然后向支付证据存储设备发送第一视频帧、第三视频帧及对应的支付标识，使存储设备关联存储这些信息。分阶段采集不同视频帧，全面记录了支付方在支付过程中的生物特征变化情况。第一视频帧在支付前采集，反映了支付方初始状态的生物特征；第二视频帧采集第一生物特征，用于支付身份验证；第三视频帧在支付后采集，验证支付方身份的连续性。关联存储这些视频帧和支付标识，便于在处理拒付请求时根据支付标识快速准确地获取相关生物特征信息，提高了证据采集和管理的效率，增强了对拒付请求处理的准确性和可靠性。

进一步地，当第一视频帧中所包含的第二生物特征与第三视频帧中所包含的第二生物特征相匹配时，支付验证设备向拒付请求处理设备发送包含第一视频帧和第三视频帧的支付证据信息。若拒付请求方的第二部位的第五生物特征与第一视频帧或第三视频帧中包含的指定第二生物特征匹配，拒付请求处理设备拒绝拒付请求，并向拒付请求方发送携带有第二生物特征匹配结果的第一通知消息。基于多视频帧生物特征匹配的判断方式，增加了验证的维度和可靠性。多个视频帧中的生物特征相互印证，提高了对支付方身份验证的准确性。当匹配成功时，能更有把握地判断支付为本人操作，减少误判拒付请求的情况。及时向拒付请求方发送匹配结果通知，提高了处理流程的透明度，使拒付请求方能够及时了解处理结果，增强了用户对支付系统的信任度。

进一步地，若拒付请求方的第二部位的第五生物特征与指定第二生物特征不匹配，拒付请求处理设备有两种处理方式。一是将指定第二生物特征与拒付请求方存在关联关系的

对象所对应的第二生物特征进行匹配，若存在匹配的关联匹配对象，则向拒付请求方发送携带关联匹配对象第二生物特征的第二通知消息，通知拒付请求方已完成支付是由关联匹配对象完成的，并接收拒付请求方针对该通知消息的回复信息，基于回复信息处理拒付请求；二是直接同意拒付请求，并将已支付成功的支付金额返回给拒付请求方的账户。这两种处理方式考虑了多种可能情况，增加了处理拒付请求的灵活性和准确性。当拒付请求方与支付生物特征不匹配时，通过关联对象匹配进一步排查，避免因支付方可能委托他人支付等情况导致的误判。若无法找到合理关联，则及时处理拒付请求，保障了拒付请求方的权益，提高了支付系统的公正性和用户体验。

进一步地，支付证据存储设备关联存储各支付方的第二部位的生物特征与存储密钥，一个支付方的存储密钥基于该支付方的支付标识、支付方标识、初始密钥和对应的支付特征采集设备的设备标识加密得到，初始密钥存储在支付特征采集设备中。支付验证设备基于支付标识获取已完成支付对应的第二生物特征时，先确定支付方标识，从支付特征采集设备获取设备标识和初始密钥，对这些信息加密得到生物特征存储加密密钥，再基于该密钥从支付证据存储设备中获取第二生物特征。采用加密存储和获取生物特征的方式，提高了生物特征数据的安全性。加密算法对生物特征数据进行加密处理，将数据转换为密文形式，只有使用正确的存储密钥才能解密获取原始数据。即使数据在传输或存储过程中被截取，攻击者也无法获取有效信息，保障了支付方的隐私和支付交易的安全。同时，使用基于多因素生成的存储密钥，增加了密钥的复杂性和随机性，进一步提高了加密的可靠性。

进一步地，拒付请求处理设备接收到携带支付标识的拒付请求时，向支付验证设备发送携带相同支付标识的支付证据提供请求，接收支付验证设备发送的包含第二生物特征的支付证据信息，并确定支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度，基于匹配程度处理拒付请求。拒付请求处理设备在整个流程中起到核心协调和决策作用，通过与支付验证设备的信息交互，实现了生物特征数据的有效利用。准确确定生物特征的匹配程度，能够科学合理地判断拒付请求的合理性，保障支付交易的正常秩序。同时，基于匹配程度进行决策处理，减少了人为因素的干扰，提高了处理结果的客观性和准确性，增强了支付系统的稳定性和可靠性。

需要说明的是，本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”、“1”、“2”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例能够以除图示或文字描述以外的顺序实施。

本申请实施例中，术语“模块”或“单元”是指有预定功能的计算机程序或计算机程序的一部分，并与其他相关部分一起工作以实现预定目标，并且可以通过使用软件、硬件（如处理电路或存储器）或其组合来全部或部分实现。同样的，一个处理器（或多个处理器或存储器）可以用来实现一个或多个模块或单元。此外，每个模块或单元都可以是包含该模块或单元功能的整体模块或单元的一部分。

应该理解的是，虽然本申请实施例的流程图中通过箭头指示各个操作步骤，但是这些步骤的实施顺序并不受限于箭头所指示的顺序。除非本文中有明确的说明，否则在本申请实施例的一些实施场景中，各流程图中的实施步骤可以按照需求以其他的顺序执行。此外，各流程图中的部分或全部步骤基于实际的实施场景，可以包括多个子步骤或者多个阶段。这些子步骤或者阶段中的部分或全部可以在同一时刻被执行，这些子步骤或者阶段中的每个子步骤或者阶段也可以分别在不同的时刻被执行。在执行时刻不同的场景下，这些子步骤或者阶段的执行顺序可以根据需求灵活配置，本申请实施例对此不限制。

以上实施例的各技术特征可以进行任意的组合，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

权利要求

1、一种拒付请求的处理方法，由支付验证设备执行，所述方法包括：

接收拒付请求处理设备发送的针对已完成支付的支付证据提供请求，其中，所述支付证据提供请求中携带已完成支付的支付标识；所述支付证据提供请求是所述拒付请求处理设备接收到携带所述支付标识的拒付请求时发送的；所述已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，所述第一生物特征是在所述已完成支付的支付过程中采集的支付方的第一部位的生物特征；

基于所述支付标识，获取所述已完成支付所对应的第二生物特征；其中，所述第二生物特征是在所述已完成支付的支付过程中所采集的支付方的第二部位的生物特征；及

向所述拒付请求处理设备发送包括所述第二生物特征的支付证据信息，以使所述拒付请求处理设备基于所述支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对所述拒付请求进行处理。

2、根据权利要求 1 所述的方法，所述方法还包括：

基于所述支付标识，确定所述已完成支付所对应的支付方标识；

确定所述支付方标识所绑定的第三生物特征；其中，所述第三生物特征是所述支付方标识对应的对象所注册的第一部位的生物特征；

其中，所述支付证据信息还包括所述第三生物特征，所述拒付请求方的生物特征包括所述拒付请求方的第一部位的第四生物特征和第二部位的第五生物特征，所述匹配程度包括所述第二生物特征和所述第五生物特征的匹配程度、以及所述第三生物特征和所述第四生物特征的匹配程度。

3、根据权利要求 1 或 2 所述的方法，所述基于所述支付标识，获取所述已完成支付所对应的第二生物特征，包括：

向支付证据存储设备发送生物特征获取请求；其中，所述生物特征获取请求中包括所述支付标识；所述支付证据存储设备中存储有各支付的支付标识所对应的支付方的第二部位的生物特征；

接收所述支付证据存储设备发送的所述已完成支付所对应的第二生物特征。

4、根据权利要求 3 所述的方法，所述支付证据信息是由支付特征采集设备通过以下方式采集，并存储至所述支付证据存储设备的：

接收针对所述已完成支付的支付请求；

响应于所述支付请求，获取生物特征采集视频流，并在接收到支付成功信息时，将所述支付方的第一生物特征和第二生物特征存储至所述支付证据存储设备中；其中，所述生物特征采集视频流至少包括所述支付方的第一生物特征和第二生物特征。

5、根据权利要求 4 所述的方法，获取生物特征采集视频流，并在接收到支付成功消息时，将所述第二生物特征存储至所述支付证据存储设备中，包括：

采集第一视频帧；其中，所述第一视频帧中包含有所述支付方所对应的第二生物特征；

输出第一提示信息，所述第一提示信息用于提示所述支付方提供第一生物特征；

采集包含所述第一生物特征的第二视频帧；

若接收到支付成功消息，且，在检测到支付方的第一部位离开拍摄范围时，采集包括支付方的第二生物特征的第三视频帧；

向所述支付证据存储设备发送所述第一视频帧、第三视频帧以及所对应的支付标识，以使得所述支付证据存储设备中关联存储所述第一视频帧中所包含的第二生物特征、所述第三视频帧中所包含的第二生物特征以及所述支付标识。

6、根据权利要求 5 所述的方法，所述第一视频帧中所包含第二生物特征与所述第三视频帧中所包含的第二生物特征相匹配；

其中，所述向所述拒付请求处理设备发送包括所述第二生物特征的支付证据信息，包括：

向所述拒付请求处理设备发送包含所述第一视频帧和所述第三视频帧的支付证据信息，以由所述拒付请求设备通过以下方式对所述拒付请求进行处理：

若所述拒付请求方的第二部位的第五生物特征与指定第二生物特征匹配，则拒绝所述拒付请求，并向所述拒付请求方发送第一通知消息；其中，所述指定第二生物特征为所述第一视频帧或者所述第三视频帧中所包含的第二生物特征；所述第一通知消息中携带有第二生物特征的匹配结果，并用于通知所述拒付请求方，所述拒付请求处理设备已拒绝所述拒付请求。

7、根据权利要求 6 所述的方法，由所述拒付请求设备通过以下任一方式对所述拒付请求进行处理：

若所述拒付请求方的第二部位的第五生物特征与指定第二生物特征不匹配，将指定第二生物特征与所述拒付请求方存在关联关系的对象所对应的第二生物特征进行匹配；若所述存在关联关系的对象中存在第二生物特征相匹配的关联匹配对象，则向所述拒付请求方发送携带关联匹配对象的第二生物特征的第二通知消息；接收所述拒付请求方针对第二通知消息的回复信息，并基于所述回复信息对所述拒付请求进行处理；其中，所述第二通知消息用于通知所述拒付请求方所述已完成支付是由所述关联匹配对象完成的；

若所述拒付请求方的第二部位的第五生物特征与指定第二生物特征不匹配，则同意所述拒付请求，并将已支付成功的支付金额返回给拒付请求方的账户。

8、根据权利要求 3-7 任一项所述的方法，所述支付证据存储设备中关联存储各支付方的第二部位的生物特征与存储密钥，一个支付方的存储密钥是基于该支付方的支付标识、支付方标识、初始密钥和对应的支付特征采集设备的设备标识进行加密后得到的；所述初始密钥存储在所述支付特征采集设备中；

其中，所述基于所述支付标识，获取所述已完成支付所对应的第二生物特征，包括：

基于所述支付标识，确定所述已完成支付所对应的支付方标识；

从所述已完成支付对应的支付特征采集设备中获取设备标识以及初始密钥；

对所述支付标识、支付方标识、所述设备标识和所述初始密钥进行加密，得到生物特征存储加密密钥；

基于所述生物特征存储加密密钥，从所述支付证据存储设备中获取所述已完成支付所对应的第二生物特征。

9、一种拒付请求的处理方法，由拒付请求处理设备执行，所述方法包括：

向支付验证设备发送支付证据提供请求；其中，所述支付证据提供请求中携带已完成支付所对应的支付标识；所述支付证据提供请求是所述拒付请求处理设备接收到携带所述支付标识的拒付请求时发送的；所述已完成支付是基于第一生物特征进行支付且已支付成功的支付；所述第一生物特征是在所述已完成支付的支付过程中采集的支付方的第一部位的生物特征；

接收所述支付验证设备发送的包括第二生物特征的支付证据信息；所述第二生物特征是由支付验证设备基于所述支付标识获取到的；其中，所述第二生物特征是在支付过程中所采集的第二部位的生物特征；及

确定所述支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度，并基于所述匹配程度，对所述拒付请求进行处理。

10、一种拒付请求的处理装置，所述装置设置在支付验证设备中，所述装置包括：

支付证据提供请求接收模块，用于接收拒付请求处理设备发送的针对已完成支付的支付证据提供请求，其中，所述支付证据提供请求中携带已完成支付的支付标识；所述支付证据提供请求是所述拒付请求处理设备接收到携带所述支付标识的拒付请求时发送的；所述已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，所述第一生物特征是在所述已完成支付的支付过程中采集的支付方的第一部位的生物特征；

获取模块，用于基于所述支付标识，获取所述已完成支付所对应的第二生物特征；其

中，所述第二生物特征是在所述已完成支付的支付过程中所采集的支付方的第二部位的生物特征；

支付证据信息发送模块，用于向所述拒付请求处理设备发送包括所述第二生物特征的支付证据信息，以使所述拒付请求处理设备基于所述支付证据信息中的生物特征和拒付请求方的生物特征的匹配程度，对所述拒付请求进行处理。

11、一种拒付请求的处理装置，所述装置设置在拒付请求处理设备中，所述装置包括：

支付证据提供请求发送模块，用于向支付验证设备发送支付证据提供请求；其中，所述支付证据提供请求中携带已完成支付所对应的支付标识；所述支付证据提供请求是所述拒付请求处理设备接收到携带所述支付标识的拒付请求时发送的；所述已完成支付是基于第一生物特征进行支付且已支付成功的支付；其中，所述第一生物特征是在所述已完成支付的支付过程中采集的支付方的第一部位的生物特征；

支付证据信息接收模块，用于接收所述支付验证设备发送的包括第二生物特征的支付证据信息；所述第二生物特征是由支付验证设备基于所述支付标识获取到的；其中，所述第二生物特征是在支付过程中所采集的第二部位的生物特征；

匹配程度确定模块，用于确定所述支付证据信息中的生物特征与拒付请求方的生物特征的匹配程度；

拒付请求处理模块，用于基于所述匹配程度，对所述拒付请求进行处理。

12、一种支付验证设备，所述支付验证设备包括存储器和处理器，所述存储器中存储有计算机程序，所述处理器在运行所述计算机程序时执行权利要求 1 至 8 任一项所述的拒付请求的处理方法。

13、一种拒付请求处理设备，所述拒付请求处理设备包括存储器和处理器，所述存储器中存储有计算机程序，所述处理器在运行所述计算机程序时执行权利要求 9 所述的拒付请求的处理方法。

14、一种计算机可读存储介质，所述存储介质中存储有计算机程序，所述计算机程序被处理器执行时实现权利要求 1 至 9 任一项所述的拒付请求的处理方法。

15、一种计算机程序产品，包括计算机程序，所述计算机程序被处理器执行时实现权利要求 1 至 9 任一项所述的拒付请求的处理方法。