

生物特征匹配方法、终端设备、服务器、系统及介质

相关申请的交叉引用

本申请要求享有于 2023 年 1 月 20 日提交的名称为“生物特征匹配方法、终端设备、服务器、系统及介质”的中国专利申请 202310095121.8 的优先权，该申请的全部内容通过引用并入本文中。

技术领域

本申请属于数据处理领域，尤其涉及一种生物特征匹配方法、终端设备、服务器、系统及介质。

背景技术

随着信息技术的发展，人脸识别等生物特征识别技术被广泛应用在身份认证、鉴权核验等场景中。利用生物特征识别技术进行匹配，需要预先采集用户的生物特征数据上传至服务器作为匹配样本，在用户进行生物特征匹配时，将当前采集的生物特征数据与作为匹配样本的生物特征数据进行比对，从而实现生物特征匹配。

但用户的生物特征是用户的隐私数据，服务器中存储的匹配样本或上传过程中的生物特征数据一旦泄露，将会对用户的数据安全带来巨大的风险。

发明内容

本申请实施例提供一种生物特征匹配方法、终端设备、服务器、系统及介质，能够降低用户隐私数据的安全风险。

第一方面，本申请实施例提供一种生物特征匹配方法，应用于终端设备，该方法包括：与服务器基于第一私钥、获取的待匹配生物特征向量、预设的生成元、第二私钥和第一加密数据，进行多次交互和处理，得到第

二加密数据，第一私钥为终端设备的私钥，第二私钥为服务器的私钥，第一加密数据由终端设备预先利用生成元和第一私钥对样本生物特征向量加密得到并发送至服务器，第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子，目标欧式距离包括待匹配生物特征向量与样本生物特征向量的欧式距离；向服务器发送第二加密数据，以使服务器利用第二加密数据、生成元、第二私钥和预设欧式距离匹配阈值，得到待匹配生物特征向量与样本生物特征向量的匹配结果。

第二方面，本申请实施例提供一种生物特征匹配方法，应用于服务器，该方法包括：与终端设备基于第二私钥、第一加密数据、第一私钥、预设的生成元和终端设备获取的待匹配生物特征向量，进行多次交互和处理，以使终端设备得到第二加密数据，第一私钥为终端设备的私钥，第二私钥为服务器的私钥，第一加密数据由终端设备预先利用生成元和第一私钥对样本生物特征向量加密得到并发送至服务器，第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子，目标欧式距离包括待匹配生物特征向量与样本生物特征向量的欧式距离；接收终端设备发送的第二加密数据；利用第二加密数据、第二私钥、生成元和预设欧式距离匹配阈值，得到待匹配生物特征向量与样本生物特征向量的匹配结果。

第三方面，本申请实施例提供一种终端设备，包括第一通信模块和第一加密模块；第一通信模块和第一加密模块用于与服务器基于第一私钥、获取的待匹配生物特征向量、预设的生成元、第二私钥和第一加密数据，进行多次交互和处理，得到第二加密数据，第一私钥为终端设备的私钥，第二私钥为服务器的私钥，第一加密数据由终端设备预先利用生成元和第一私钥对样本生物特征向量加密得到并发送至服务器，第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子，目标欧式距离包括待匹配生物特征向量与样本生物特征向量的欧式距离；第一通信模块还用于向服务器发送第二加密数据，以使服务器利用第二加密数据、生成元、第二私钥和预设欧式距离匹配阈值，得到待匹配生物特征向量与样本生物特征向量的匹配结果。

第四方面，本申请实施例提供一种服务器，包括第二通信模块、第二

加密模块和匹配模块；第二通信模块和第二加密模块用于与终端设备基于第二私钥、第一加密数据、第一私钥、预设的生成元和终端设备获取的待匹配生物特征向量，进行多次交互和处理，以使终端设备得到第二加密数据，第一私钥为终端设备的私钥，第二私钥为服务器的私钥，第一加密数据由终端设备预先利用生成元和第一私钥对样本生物特征向量加密得到并发送至服务器，第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子，目标欧式距离包括待匹配生物特征向量与样本生物特征向量的欧式距离；第二通信模块还用于接收终端设备发送的第二加密数据；匹配模块用于利用第二加密数据、第二私钥、生成元和预设欧式距离匹配阈值，得到待匹配生物特征向量与样本生物特征向量的匹配结果。

第五方面，本申请实施例提供一种终端设备，包括：处理器以及存储有计算机程序指令的存储器；所述处理器执行所述计算机程序指令时实现第一方面的生物特征匹配方法。

第六方面，本申请实施例提供一种服务器，包括：处理器以及存储有计算机程序指令的存储器；所述处理器执行所述计算机程序指令时实现第二方面的生物特征匹配方法。

第七方面，本申请实施例提供一种生物特征匹配系统，包括第五方面的终端设备和第六方面的服务器。

第八方面，本申请实施例提供一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现第一方面的生物特征匹配方法或第二方面的生物特征匹配方法。

本申请实施例提供一种生物特征匹配方法、终端设备、服务器、系统及介质，终端设备与服务器可基于第一私钥、待匹配生物特征向量、生成元、第二私钥、第一加密数据进行多次交互和处理，终端设备具有第一私钥、待匹配生物特征和生成元，服务器具有第二私钥和第一加密数据。通过终端设备利用第一私钥的加密处理、服务器利用第二私钥的加密处理、以及终端设备与服务器之间的数据交互，使终端设备能够得到包括第二私钥和能够表征待匹配生物特征向量与样本生物特征向量的欧式距离的目标欧氏距离的计算算子的第二加密数据，第二加密数据中包含第二私钥，终

端设备无法得知第二私钥，难以破解得到待匹配生物特征向量和样本生物特征向量的明文，同理，服务器无法得知第一私钥，也难以破解第一加密私钥。且服务器是根据第二加密数据、生成元、第二私钥和预设欧式距离匹配阈值，来确定待匹配生物特征向量与样本生物特征向量的匹配结果的，可在不涉及待匹配生物特征向量的明文和样本生物特征向量的明文的条件下完成匹配，从而降低用户隐私数据的安全风险，提高生物特征匹配的安全性。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单的介绍，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。

图 1 为本申请实施例提供的生物特征匹配系统的架构示意图；

图 2 为本申请第一方面一实施例提供的生物特征匹配方法的流程图；

图 3 为本申请第一方面另一实施例提供的生物特征匹配方法的流程图；

图 4 为本申请第二方面一实施例提供的生物特征匹配方法的流程图；

图 5 为本申请第二方面另一实施例提供的生物特征匹配方法的流程图；

图 6 为本申请第三方面一实施例提供的终端设备的结构示意图；

图 7 为本申请第四方面一实施例提供的服务器的结构示意图；

图 8 为本申请第五方面一实施例提供的终端设备的结构示意图；

图 9 为本申请第六方面一实施例提供的服务器的结构示意图。

具体实施方式

下面将详细描述本申请的各个方面的特征和示例性实施例，为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及具体实施例，对本申请进行进一步详细描述。应理解，此处所描述的具体实施例仅意在解释本申请，而不是限定本申请。对于本领域技术人员来说，本申请可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本申请的示例来提供对本申请更好的理解。

随着信息技术的发展，人脸识别等生物特征识别技术被广泛应用在身份认证、鉴权核验等场景中。利用生物特征识别技术进行匹配，需要预先采集用户的生物特征数据上传至服务器作为匹配样本，在用户进行生物特征匹配时，将当前采集的生物特征数据与作为匹配样本的生物特征数据进行比对，从而实现生物特征匹配。但用户的生物特征是用户的隐私数据，服务器中存储的匹配样本或上传过程中的生物特征数据一旦泄露，将会对用户的数据安全带来巨大的风险。

本申请提供一种生物特征匹配方法、终端设备、服务器、系统及介质，能够由终端设备利用自身的私钥对生物特征向量进行加密，与服务器交互，由服务器利用自身的私钥对接收到的数据进行加密处理。通过终端设备利用自身的私钥的加密处理、服务器利用自身的私钥的加密处理，构建出包括能够表征待匹配生物特征向量和样本生物特征向量的相似度的欧式距离的计算算子的加密数据，利用该加密数据得到匹配结果，从而在终端设备和服务器均不存储生物特征的明文数据的情况下，实现生物特征的匹配，降低用户隐私数据的安全风险，提高生物特征匹配的安全性。

需要说明的是，本申请中对信息、数据的获取、存储、使用、处理等均得到用户或相关机构的授权，符合国家法律法规的相关规定。

本申请实施例提供的生物特征匹配方法、终端设备、服务器、系统及介质可应用于支付、打卡、通行等需要进行身份识别的场景中，在此并不限定。下面对本申请提供的生物特征匹配方法、终端设备、服务器、系统及介质分别进行说明。

为了便于理解，这里先对本申请实施例提供的生物特征匹配方法所应用的系统架构进行简单说明。图 1 为本申请实施例提供的生物特征匹配系统的架构示意图，如图 1 所示，该生物特征匹配系统可包括终端设备 11 和服务器 12。

终端设备 11 可为用户所使用的设备，终端设备 11 中可安装有需要进行生物特征识别功能的应用程序，或者，终端设备 11 的操作系统本身具有生物特征识别功能的需求，在此并不限定。终端设备 11 可采集用户的生物特征数据，并对生物特征数据进行处理。例如，终端设备 11 可包括手机、

平板电脑、智能穿戴设备、打卡设备、自动售货机等设备，在此并不限定终端设备 11 的类型和数量。终端设备 11 可与服务器 12 进行通信交互。在本申请实施例中，终端设备 11 具有自身的私钥即第一私钥，可对数据进行加密处理。

服务器 12 可与终端设备 11 通信交互，接收终端设备 11 传输来的数据。服务器 12 存储有密文形式的样本生物特征数据，样本生物特征数据包括作为匹配样本或识别样本的生物特征数据。在本申请实施例中，服务器 12 具有自身的私钥即第二私钥，可对数据进行加密处理。服务器 12 可得到匹配结果，将匹配结果反馈给终端设备 11。在此并不限定服务器 12 的种类和数量。

本申请第一方面提供一种生物特征匹配方法，该生物特征匹配方法可应用于终端设备，即，该生物特征匹配方法可由终端设备执行。图 2 为本申请第一方面一实施例提供的生物特征匹配方法的流程图，如图 2 所示，该生物特征匹配方法可包括步骤 S201 和步骤 S202。

在步骤 S201 中，与服务器基于第一私钥、获取的待匹配生物特征向量、预设的生成元、第二私钥和第一加密数据，进行多次交互和处理，得到第二加密数据。

终端设备具有第一私钥、待匹配生物特征向量和生成元。第一私钥为终端设备的私钥，服务器并不能得知第一私钥。待匹配生物特征向量为待匹配生物数据转化得到的向量。终端设备可采集待匹配生物数据，待匹配生物数据即为待匹配的原始生物数据，终端设备可利用向量转化模型，将待匹配生物数据转化为待匹配生物特征向量。待匹配生物数据可包括人脸数据、指纹数据、掌静脉数据、虹膜数据等中的一种或两种以上，在此并不限定。向量转化模型可选用与原始生物数据的类型匹配的转化模型，在此并不限定向量转化模型的类型，例如，待匹配生物数据包括人脸数据，人脸数据具体可为人脸图像数据，可选用 OpenFace、Eigenface 等模型对人脸数据进行特征提取，并形成人脸特征向量。

服务器具有第二私钥和第一加密数据。第二私钥为服务器的私钥，终端设备并不能得知第二私钥。第一加密数据可由终端设备预先利用生成元

和第一私钥对样本生物特征向量加密得到并发送至服务器。终端设备可将获取到的样本生物数据转化为样本生物特征向量。样本生物数据可包括人脸数据、指纹数据、掌静脉数据、虹膜数据等中的一种或两种以上，在此并不限定。将样本生物数据转化为样本生物特征向量的向量转化模型，可与将待匹配生物数据转化为待匹配生物特征向量的向量转化模型一致。生成元可由终端设备与服务器两端预先约定，生成元可作为参与终端设备和服务器各自的加密处理的基础数据之一。

终端设备可利用生成元和第一私钥对待匹配生物特征向量进行加密处理，也可对从服务器传输来的数据进行加密处理。终端设备加密处理后的数据可向服务器发送，以使服务器对从终端设备传输来的数据进行加密处理，服务器可利用第二私钥进行加密处理。通过终端设备与服务器之间的加密处理和数据的交互，可在终端设备这一侧构成第二加密数据。第二加密数据实质上是基于终端设备对数据的加密处理、服务器对数据的加密处理以及终端设备与服务器的交互得到的。第二加密数据中形成包括第二私钥和目标欧式距离的计算算子。目标欧式距离包括待匹配生物特征向量与样本生物特征向量的欧式距离，目标欧式距离可表征待匹配生物特征向量与样本生物特征向量的相似度，目标欧式距离越小，表示待匹配生物特征向量与样本生物特征向量的相似度越高，待匹配生物特征向量对应的用户与样本生物特征向量对应的用户是同一用户的可能性越高。

计算算子可视为计算处理得到的数据的组成成分，这里的计算处理为广义的计算处理，计算处理可包括多种计算处理方式，如加密处理、转化处理、映射处理、判断处理等均可视为计算处理。例如，参数 A、参数 B 和参数 C 参与计算处理，得到了一数据，该数据为 $AC \times (A+B)$ ，则 AC 和 $(A+B)$ 均可为该数据中形成的计算算子，其中，计算算子 AC 可为包括 A 的计算算子，也可为包括 C 的计算算子。又例如，参数 A、参数 B 和参数 C 参与计算处理，得到一数据，该数据为 A^{BC} ，则 BC 可为该数据中形成的计算算子，其中，计算算子 BC 可为包括 B 的计算算子，也可为包括 C 的计算算子。在一些示例中，计算算子可包括模指数算子或点乘算子。模指数算子为指数形式的计算算子，例如，在数据 A^{BC} 中形成了包括 B 的

模指数算子 BC，也可以说，形成了包括 C 的模指数算子 BC。点乘算子为乘数形式的算子，例如，在数据 $AC \times (A+B)$ 中，AC 和 $(A+B)$ 可为点乘算子，计算算子 AC 可视为包括 A 的点乘算子，计算算子 AC 也可视为包括 C 的点乘算子。第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子，设第二私钥为 b ，待匹配生物特征向量为 n 维向量 $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$ ，样本生物特征向量为 n 维向量 $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ ，对应地，待匹配生物特征向量与样本生物特征向量的欧式距离为 $\sqrt{\sum_1^n (x_i - y_i)^2}$ ，则第二加密数据中可形成包括 $b\sqrt{\sum_1^n (x_i - y_i)^2}$ 的计算算子。为了便于后续的匹配比对，在一些示例中，第二加密数据中可包括计算算子 $b\sum_1^n (x_i - y_i)^2$ ，该计算算子 $b\sum_1^n (x_i - y_i)^2$ 包括 $b\sqrt{\sum_1^n (x_i - y_i)^2}$ 。

在一些示例中，第一私钥可为终端设备生成的一随机数，第二私钥可为服务器生成的一随机数。为了进一步提高数据安全性，第一私钥可为占用比特位至少为 128 比特的大整数，如，第一私钥可为占用比特位为 256 比特的大整数；同理，第二私钥可为占用比特位至少为 128 比特的大整数，如，第二私钥可为占用比特位为 256 比特的大整数。通过设置比特位数量大于等于 128 比特的第一私钥和第二私钥，能够满足密码学安全强度的要求，进一步提高用户的个人隐私数据的安全性，也能进一步提高生物特征匹配的安全性。

在步骤 S202 中，向服务器发送第二加密数据，以使服务器利用第二加密数据、第二私钥、生成元和预设欧式距离匹配阈值，得到待匹配生物特征向量与样本生物特征向量的匹配结果。

服务器可利用第二私钥、生成元和预设欧式距离匹配阈值构建与第二加密数据格式一致的数据，通过对比第二加密数据与利用第二私钥、生成元和预设欧式距离匹配阈值构建的数据，得到待匹配生物特征向量与样本生物特征向量的匹配结果。预设欧式距离匹配阈值为用于判断两向量是否为同一向量的欧式距离的判断阈值，可根据场景、需求、经验等设定，在此并不限定。若目标欧氏距离小于等于预设欧式距离匹配阈值，则表示待匹配生物特征向量和样本生物特征向量匹配成功，即匹配结果为匹配成功；

若目标欧氏距离大于预设欧式距离匹配阈值，则表示待匹配生物特征向量和样本生物特征向量匹配失败，即匹配结果为匹配失败。第二加密数据含有包括第二私钥和目标欧式距离的计算算子，服务器利用第二私钥、生成元和预设欧式距离匹配阈值构建的数据含有包括第二私钥和预设欧式距离匹配阈值的计算算子，因此，第二加密数据与服务器利用第二私钥、生成元和预设欧式距离匹配阈值构建的数据的比对结果，与目标欧式距离与预设欧式距离匹配阈值的比对结果是相互对应的，可通过第二加密数据与服务器利用第二私钥、生成元和预设欧式距离匹配阈值构建的数据的比对结果，确定目标欧式距离与预设欧式距离匹配阈值的比对结果，该比对结果即可表征匹配结果。

在本申请实施例中，终端设备与服务器可基于第一私钥、待匹配生物特征向量、生成元、第二私钥、第一加密数据进行多次交互和处理，终端设备具有第一私钥、待匹配生物特征和生成元，服务器具有第二私钥和第一加密数据。通过终端设备利用第一私钥的加密处理、服务器利用第二私钥的加密处理、以及终端设备与服务器之间的数据交互，使终端设备能够得到包括第二私钥和能够表征待匹配生物特征向量与样本生物特征向量的欧式距离的目标欧氏距离的计算算子的第二加密数据，第二加密数据中包含第二私钥，终端设备无法得知第二私钥，难以破解得到待匹配生物特征向量和样本生物特征向量的明文，同理，服务器无法得知第一私钥，也难以破解第一加密私钥。且服务器是根据第二加密数据、生成元、第二私钥和预设欧式距离匹配阈值，来确定待匹配生物特征向量与样本生物特征向量的匹配结果的，可在不涉及待匹配生物特征向量的明文和样本生物特征向量的明文的条件下完成匹配，从而降低用户隐私数据的安全风险，提高生物特征匹配的安全性。由于终端设备和服务器也不会存储待匹配生物特征向量的明文和样本生物特征向量的明文，能够保证用户对个人隐私数据的控制权，从而限制个人隐私数据的使用场景，满足个人隐私数据的最小化使用原则，防止个人隐私数据被滥用。

而且，本申请实施例中是对待匹配生物特征向量、样本生物特征向量进行加密处理，以及通过加密处理后的数据的比对来确定匹配结果，待匹

配生物数据和样本生物数据的种类不同，可采用的向量转化模型也可不同，但本申请实施例中是通过特征向量的相似度来描述生物数据的相似度。本申请实施例的生物特征的匹配过程中对个人隐私数据的保护流程与待匹配生物数据转化为待匹配生物特征向量、样本生物数据转换为样本生物特征向量的转化流程可相互独立，从而实现了向量转化模型与生物特征匹配模型的可组装、可插拔的技术方案，即实现了向量转化模型与生物特征匹配模型的解耦。

在一些实施例中，在终端设备与服务器的交互和处理过程中，可生成多个中间加密数据，可通过对多个中间加密数据的进一步处理得到第二加密数据。图 3 为本申请第一方面另一实施例提供的生物特征匹配方法的流程图，图 3 与图 2 的不同之处在于，图 2 中的步骤 S201 可具体细化为图 3 中的步骤 S2011 至步骤 S2013。

在步骤 S2011 中，接收服务器发送的第一中间加密数据。

第一中间加密数据由服务器利用第二私钥对第一加密数据加密得到。第一加密数据中可形成包括第一私钥和样本生物特征向量中元素的计算算子。进一步地，第一加密数据中可形成包括第一私钥和样本生物特征向量中元素的乘积的计算算子。例如，第一私钥为 a ，样本生物特征向量为 n 维向量 $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ ，第一加密数据中可包括计算算子 ay_i ，第一加密数据中可包括计算算子 ay_i^2 ， $i=1,2,\dots,n$ ；需要说明的是，计算算子 ay_i^2 中也包括计算算子 ay_i 。

服务器可利用第二私钥对第一加密数据加密，得到第一中间加密数据。第一中间加密数据中可形成包括第一私钥、第二私钥与样本生物特征向量中元素的乘积的计算算子。第一加密数据中包括第一私钥和样本生物特征向量中元素的乘积的计算算子，可利用第二私钥参与加密计算，使包括第一私钥和样本生物特征向量中元素的乘积的计算算子再与第二私钥相乘，从而得到形成有包括第一私钥、第二私钥和样本生物特征向量中元素的乘积的计算算子的第一中间加密数据。例如，第一私钥为 a ，第二私钥为 b ，样本生物特征向量为 n 维向量 $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ ，第一中间加密数据中可包括计算算子 aby_i 。

在步骤 S2012 中, 根据第一中间加密数据、待匹配生物特征向量、生成元、第一私钥, 得到第二中间加密数据。

第二中间加密数据中的至少部分数据可在第一中间加密数据的基础上得到, 第二中间加密数据中形成包括第一私钥和待匹配生物特征向量中元素的乘积的计算算子。例如, 第一私钥为 a , 待匹配生物特征向量为 n 维向量 $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, 第二中间加密数据中可形成包括 ax_i 的计算算子。为了能够在后续的步骤中构建得到第二加密数据, 第二中间加密数据可为在 ax_i 的基础上进一步构建得到。第二中间加密数据用于在后续步骤中参与构建目标欧式距离。

在一些示例中, 第二中间加密数据包括第一中间加密子数据和第二中间加密子数据。步骤 S2012 可具体细化为: 根据第一中间加密数据和待匹配生物特征向量, 得到第一中间加密子数据; 根据第一私钥、生成元和待匹配生物特征向量, 得到第二中间加密子数据。

第一中间加密子数据中形成包括第一私钥、第二私钥、样本生物特征向量中元素与待匹配生物特征向量中元素的乘积的计算算子, 例如, 第一私钥为 a , 第二私钥为 b , 样本生物特征向量为 n 维向量 $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$, 待匹配生物特征向量为 n 维向量 $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, 第一中间加密子数据可形成有包括 abx_iy_i 的计算算子, 为了在后续过程中可构建得到目标欧式距离, 第一中间加密子数据可包括计算算子 $-2abx_iy_i$ 。

第二中间加密子数据中形成包括第一私钥、第二私钥与待匹配生物特征向量中元素的乘积的计算算子, 例如, 第一私钥为 a , 待匹配生物特征向量为 n 维向量 $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, 第二中间加密数据可形成包括 ax_i 的计算算子, 为了在后续过程中可构建得到目标欧式距离, 第二中间加密数据可包括计算算子 ax_i^2 。

在步骤 S2013 中, 与服务器基于第二中间加密数据、第一加密数据、第一私钥和第二私钥进行交互和处理, 消除处理后的数据中的第一私钥, 得到第二加密数据。

在得到第二中间加密数据后, 可向服务器发送第二中间加密数据, 以

使服务器基于第二中间加密数据进行加密处理，再将加密处理后的数据反馈给终端设备，再由终端设备对接收到的数据进行处理，以得到第二加密数据。在本申请实施例中，可通过终端设备进行的处理、服务器进行的处理以及终端设备与服务器的数据交互，在第二中间加密数据的基础上，得到第二加密数据。

在一些示例中，可向服务器发送第二中间加密数据，以使服务器基于第二中间加密数据、第一加密数据和第二私钥，得到第三中间加密数据；接收服务器发送的第三中间加密数据；利用第一私钥，消除第三中间加密数据中的第一私钥，得到第二加密数据。

服务器可对第二中间加密数据和第一加密数据进行计算得到第三中间加密数据。第二中间加密数据包括第一中间加密子数据和第二中间加密子数据，第一中间加密子数据和第二中间加密子数据的具体内容可参见上述实施例中的相关说明，在此不再赘述。服务器可对第一中间加密子数据、第二中间加密子数据和第一加密数据进行计算处理，从而得到第三中间加密数据。第三中间加密数据中形成包括第一私钥、第二私钥与目标欧式距离的乘积的计算算子。例如，第一私钥为 a ，第二私钥为 b ，待匹配生物特征向量为 n 维向量 $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$ ，样本生物特征向量为 n 维向量 $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ ，第三中间加密数据可形成包括 $ab\sqrt{\sum_1^n (x_i - y_i)^2}$ 的计算算子，如，第三中间加密数据可包括计算算子 $ab\sum_1^n (x_i - y_i)^2$ ，计算算子 $ab\sum_1^n (x_i - y_i)^2$ 包括 $ab\sqrt{\sum_1^n (x_i - y_i)^2}$ 。服务器无法识别第一私钥，因此将第三中间加密数据传输至终端设备，由具有第一私钥的终端设备将涉及第一私钥的第三中间加密数据中的第一私钥消除，得到第二加密数据。第二加密数据的具体内容可参见上述实施例中的相关说明，在此不再赘述。

通过终端设备与服务器之间的交互，使得终端设备和服务器各自可在接收到的数据的基础上进一步进行处理，通过中间加密数据的交互和再处理，构建得到第二加密数据，整个处理过程不涉及待匹配生物特征向量的明文与样本生物特征向量的明文，安全可靠。

在一些实施例中，服务器可通过判断第二加密数据是否属于匹配数据

集合，来确定匹配待匹配生物特征向量的与样本生物特征向量的匹配是否成功。匹配数据集合可由服务器生成，匹配数据集合中元素的最大值基于所述第二私钥和预设欧式距离匹配阈值得到，在一些示例中，匹配数据集合中元素的最大值中形成包括第二私钥与预设欧式距离匹配阈值的乘积的计算算子，这里的预设欧式距离匹配阈值可为预设欧式距离匹配阈值本身或整数化处理后的预设欧式距离匹配阈值，在此并不限定。

在第二加密数据属于匹配数据集合的情况下，匹配结果包括匹配成功；在第二加密数据不属于匹配数据集合的情况下，匹配结果包括匹配失败。第二加密数据属于匹配数据集合，表示目标欧式距离小于等于预设欧式距离匹配阈值。第二加密数据不属于匹配数据集合，表示目标欧式距离大于预设欧式距离匹配阈值。

在一些实施例中，待匹配生物特征向量中的元素、样本生物特征向量中的元素以及预设欧式距离匹配阈值等倍数整数化，也就是说，等倍数整数化后的待匹配生物特征向量中的元素、样本生物特征向量中的元素以及预设欧式距离匹配阈值均为整数，且相较于原始的待匹配生物特征向量中的元素、样本生物特征向量中的元素以及预设欧式距离匹配阈值的倍数相同。对应地，由于等倍数整数化后的预设欧式距离匹配阈值为整数，匹配数据集合中的元素的数量有限，匹配数据集合中形成包括第二私钥分别与 0 至整数化后的预设欧式距离匹配阈值的平方的乘积的计算算子。例如，第二私钥为 b ，预设欧式距离匹配阈值为 θ ，则匹配数据集合可涉及的计算算子可包括 $b \times 0$ 、 $b \times 1$ 、 $b \times 2$ 、.....、 $b \times \theta^2$ 。

在一些实施例中，为了提高生物特征匹配的效率，可采用布隆过滤器来实现第二加密数据与匹配数据集合的属于关系判定。可在 K 个目标哈希值在预先建立的布隆过滤器查找表中对应位置的数值均为 1 的情况下，确定第二加密数据属于匹配数据集合；在 K 个目标哈希值在布隆过滤器查找表中对应位置的数值至少一处为 0 的情况下，确定第二加密数据不属于匹配数据集合。

其中， K 个目标哈希值基于第二加密数据根据 K 个哈希函数计算得到。每个第二加密数据根据一个哈希函数可计算得到一个目标哈希值。每个第

二加密数据均对应应有 K 个目标哈希值。 K 为正整数，具体可根据场景、需求、经验等设定，在此并不限定。布隆过滤器查找表中的数值是基于匹配数据集合中的元素根据 K 个哈希函数计算得到。布隆过滤器查找表可由服务器生成。具体地，服务器可利用 K 个哈希函数，对匹配数据集合中的每个元素进行计算，得到每个元素对应的 K 个哈希值；将每个元素对应的 K 个哈希值映射至值均为 0 的二进制数组中的 K 个位置，并将每个元素对应的 K 个位置的数值更新为 1，将更新后的二进制数组确定为布隆过滤器查找表。生成布隆过滤器查找表所采用的 K 个哈希函数和计算 K 个目标哈希值采用的 K 个哈希函数是相同的。在一些示例中，二进制数组在更新前是每个位置的数值均为 0 的二进制数组，二进制数组中各位置可通过二进制数组中元素的下标表示，将元素对应的哈希值映射至二进制数组中的位置，可具体将元素对应的哈希值映射至二进制数据中元素的下标。

通过布隆过滤器来实现第二加密数据是否属于匹配数据集合的判断，可提高判断第二加密数据是否属于匹配数据集合的速度，尤其是在待匹配生物特征向量、样本生物特征向量的数量非常巨大时，能够对生物特征匹配的效率产生大幅度的提升。

在一些实施例中，在进行待匹配生物特征向量与样本生物特征向量的匹配之前，终端设备可生成第一加密数据，并将第一加密数据传输至服务器，以使服务器存储第一加密数据。具体地，终端设备可获取样本生物特征向量；利用生成元和第一私钥对样本生物特征向量加密，得到第一加密数据；向服务器发送第一加密数据。第一加密数据中形成包括第一私钥与样本生物特征向量中元素的乘积的计算算子，具体可参见上述实施例中的相关说明，在此不再赘述。

第一加密数据汇中存在第一私钥，服务器无法得知第一私钥，因此第一加密数据在服务器侧难以被破解，可保证个人隐私数据在服务器中存储的安全性。

本申请第二方面提供一种生物特征匹配方法，可应用于服务器，即，该生物特征匹配方法可由服务器执行。图 4 为本申请第二方面一实施例提供的生物特征匹配方法的流程图，如图 4 所示，该生物特征匹配方法可包

括步骤 S301 至步骤 S303。

在步骤 S301 中，与终端设备基于第二私钥、第一加密数据、第一私钥、预设的生成元和终端设备获取的待匹配生物特征向量，进行多次交互和处理，以使终端设备得到第二加密数据。

第一私钥为终端设备的私钥。第二私钥为服务器的私钥。第一加密数据由终端设备预先利用生成元和第一私钥对样本生物特征向量加密得到并发送至服务器。第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子。目标欧式距离包括待匹配生物特征向量与样本生物特征向量的欧式距离。

在一些示例中，计算算子可包括模指数算子或点乘算子。

在步骤 S302 中，接收终端设备发送的第二加密数据。

在步骤 S303 中，利用第二加密数据、第二私钥、生成元和预设欧式距离匹配阈值，得到待匹配生物特征向量与样本生物特征向量的匹配结果。

上述步骤 S301 至步骤 S303 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在本申请实施例中，服务器与终端设备可基于第一私钥、待匹配生物特征向量、生成元、第二私钥、第一加密数据进行多次交互和处理，终端设备具有第一私钥、待匹配生物特征和生成元，服务器具有第二私钥和第一加密数据。通过终端设备利用第一私钥的加密处理、服务器利用第二私钥的加密处理、以及终端设备与服务器之间的数据交互，使终端设备能够得到包括第二私钥和能够表征待匹配生物特征向量与样本生物特征向量的欧式距离的目标欧氏距离的计算算子的第二加密数据，第二加密数据中包含第二私钥，终端设备无法得知第二私钥，难以破解得到待匹配生物特征向量和样本生物特征向量的明文，同理，服务器无法得知第一私钥，也难以破解第一加密私钥。且服务器是根据第二加密数据、生成元、第二私钥和预设欧式距离匹配阈值，来确定待匹配生物特征向量与样本生物特征向量的匹配结果的，可在不涉及待匹配生物特征向量的明文和样本生物特征向量的明文的条件下完成匹配，从而降低用户隐私数据的安全风险，提高生物特征匹配的安全性。由于终端设备和服务器也不会存储待匹配生物特

征向量的明文和样本生物特征向量的明文，能够保证用户对个人隐私数据的控制权，从而限制个人隐私数据的使用场景，满足个人隐私数据的最小化使用原则，防止个人隐私数据被滥用。

而且，本申请实施例中是对待匹配生物特征向量、样本生物特征向量进行加密处理，以及通过加密处理后的数据的比对来确定匹配结果，待匹配生物数据和样本生物数据的种类不同，可采用的向量转化模型也可不同，但本申请实施例中是通过特征向量的相似度来描述生物数据的相似度。本申请实施例的生物特征的匹配过程中对个人隐私数据的保护流程与待匹配生物数据转化为待匹配生物特征向量、样本生物数据转换为样本生物特征向量的转化流程可相互独立，从而实现了向量转化模型与生物特征匹配模型的可组装、可插拔的技术方案，即实现了向量转化模型与生物特征匹配模型的解耦。

在一些实施例中，在服务器与终端设备的交互和处理过程中，可生成多个中间加密数据，可通过对多个中间加密数据的进一步处理得到第二加密数据。图 5 为本申请第二方面另一实施例提供的生物特征匹配方法的流程图，图 5 与图 4 的不同之处在于，图 4 中的步骤 S301 可具体细化为图 5 中的步骤 S3011 至步骤 S3013，图 4 中的步骤 S303 可具体细化为图 5 中的步骤 S3031 至步骤 S3033。

在步骤 S3011 中，利用第二私钥对第一加密数据加密，得到第一中间加密数据。

第一中间加密数据中形成包括第一私钥、第二私钥与样本生物特征向量中元素的乘积的计算算子。

在步骤 S3012 中，向终端设备发送第一中间加密数据，以使终端设备根据第一中间加密数据、待匹配生物特征向量、生成元和第一私钥得到第二中间加密数据。

第二中间加密数据中形成包括第一私钥和待匹配生物特征向量中元素的乘积的计算算子。

在一些示例中，第二中间加密数据包括第一中间加密子数据和第二中间加密子数据。第一中间加密子数据由终端设备根据第一中间加密数据和

待匹配生物特征向量得到。第一中间加密子数据中形成包括第一私钥、第二私钥、样本生物特征向量中元素与待匹配生物特征向量中元素的乘积的计算算子。第二中间加密子数据由终端设备根据第一私钥、生成元和待匹配生物特征向量得到。第二中间加密子数据中形成包括第一私钥与待匹配生物特征向量中元素的乘积的计算算子。

在步骤 S3013 中，与终端设备基于第二中间加密数据、第一加密数据、第一私钥和第二私钥进行交互和处理，以使终端设备消除处理后的数据中的第一私钥，得到第二加密数据。

在一些示例中，步骤 S3013 可具体细化为：接收终端设备发送的第二中间加密数据；基于第二中间加密数据、第一加密数据和第二私钥，得到第三中间加密数据，第三中间加密数据中形成包括第一私钥、第二私钥与目标欧式距离的乘积的计算算子；向终端设备发送第三中间加密数据，以使终端设备利用第一私钥消除第三中间加密数据中的第一私钥，得到第二加密数据。

在步骤 S3031 中，基于第二私钥、生成元和预设欧式距离匹配阈值，得到匹配数据集合。

匹配数据集合中元素的最大值基于第二私钥和预设欧式距离匹配阈值得到。

在一些示例中，待匹配生物特征向量中的元素、样本生物特征向量中的元素以及预设欧式距离匹配阈值等倍数整数化。步骤 S3031 可具体细化为：分别计算第二私钥与 0 至整数化后的预设欧式距离匹配阈值的平方的乘积；根据第二私钥与 0 至整数化后的预设欧式距离匹配阈值的平方的乘积和生成元，得到匹配数据集合。

在步骤 S3032 中，在第二加密数据属于匹配数据集合的情况下，确定匹配结果包括匹配成功。

在步骤 S3033 中，在第二加密数据不属于匹配数据集合的情况下，确定匹配结果包括匹配失败。

在一些实施例中，服务器可采用布隆过滤器的方式来进行第二加密数据是否属于匹配数据集合的判断。具体地，服务器可基于第二加密数据，

根据 K 和哈希函数，计算得到 K 个目标哈希值；在 K 个目标哈希值在预先建立的布隆过滤器查找表中对应位置的数值均为 1 的情况下，确定第二加密数据属于匹配数据集合；在 K 个目标哈希值在布隆过滤器查找表中对应位置的数值至少一处为 0 的情况下，确定第二加密数据不属于匹配数据集合。其中， K 个目标哈希值基于第二加密数据根据 K 个哈希函数计算得到，布隆过滤器查找表中的数值基于匹配数据集合中的元素根据 K 个哈希函数计算得到。

在一些实施例中，服务器可预先生成布隆过滤器查找表，以便于实现上述采用布隆过滤器的方式来进行第二加密数据是否属于匹配数据集合的判断。具体地，服务器可利用 K 个哈希函数，对匹配数据集合中的每个元素进行计算，得到每个元素对应的 K 个哈希值；将每个元素对应的 K 个哈希值映射至值均为 0 的二进制数组中的 K 个位置，并将每个元素对应的 K 个位置的数值更新为 1，将更新后的二进制数组确定为布隆过滤器查找表。

上述步骤 S3011 至步骤 S3013，以及步骤 S3031 至步骤 S3033 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在上述实施例中，计算算子可包括模指数算子或点乘算子。为了便于理解，下面分别以计算算子包括模指数算子，计算算子包括点乘算子为例对生物特征的注册及匹配流程进行说明。生物特征的注册流程是指终端设备对数据处理得到第一加密数据，并将第一加密数据传输至服务器，并由服务器存储的流程，生物特征的匹配流程是指终端设备与服务器进行多次交互，得到待匹配生物特征向量与样本生物特征向量的匹配结果的流程。

在第一个示例中，计算算子包括模指数算子，生物特征的注册及匹配流程可包括以下步骤 c1 至步骤 c12。

在步骤 c1 中，终端设备采集样本生物数据，通过向量转化模型将样本生物数据转化为样本生物特征向量 $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ 。

在步骤 c2 中，终端设备生成随机数 a ，将随机数 a 作为第一私钥。

在步骤 c3 中，终端设备利用生成元 g 和第一私钥 a ，对样本生物特征向量 $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ 进行加密，得到第一加密数据。

第一加密数据可包括下式 (1) 中的数据 g^{ay_i} 和 SY1，或者，可包括下

式 (1) 中的数据 g^{ay_i} 和 $g^{ay_i^2}$, $i=1, 2, \dots, n$ 。

$$\begin{cases} y'_1 = g^{ay_1} \\ y'_2 = g^{ay_2} \\ \dots \dots \\ y'_n = g^{ay_n} \\ SY1 = g^{a(y_1^2+y_2^2+\dots+y_n^2)} \end{cases} \quad (1)$$

在步骤 c4 中, 将第一加密数据发送至服务器, 由服务器存储第一加密数据。

模指数算子的格式为 g^p , 可利用密码学领域中的离散对数困难问题, 来保证第一加密数据的安全性。即在生成元为 g 的有限域中, 给定整数 p , 计算 $g^p = q$ 是容易的, 但根据 g 和 q 计算 p 则是困难的。服务器无法得知第一私钥 a , 且由于离散对数困难问题, 服务器得到 g^{ay_i} , 也无法破解得到 y_i , 第一加密数据在服务器是以密态形式来保存的。

上述步骤 c1 至步骤 c4 属于生物特征的注册流程。

在步骤 c5 中, 终端设备采集待匹配生物数据, 通过向量转化模型将待匹配生物数据转化为待匹配生物特征向量 $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$ 。

在步骤 c6 中, 服务器生成随机数 b , 将随机数 b 作为第二私钥。

在步骤 c7 中, 服务器利用第二私钥对第一加密数据加密, 得到第一中间加密数据, 并向终端设备发送第一中间加密数据。

第一中间加密数据可包括下式 (2) 中的 g^{aby_i} 。

$$\begin{cases} y''_1 = g^{aby_1} \\ y''_2 = g^{aby_2} \\ \dots \dots \\ y''_n = g^{aby_n} \end{cases} \quad (2)$$

在步骤 c8 中, 终端设备根据待匹配生物特征向量 $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$ 、第一中间加密数据和第一私钥, 得到第二中间加密数据, 并向服务器发送第二中间加密数据。

第二中间加密数据可包括下式 (3) 中的 $g^{-2abx_i y_i}$ 和 $g^{ax_i^2}$ 。

$$\begin{cases} (g^{aby_1})^{-2x_1} = g^{-2abx_1 y_1} \\ (g^{aby_2})^{-2x_2} = g^{-2abx_2 y_2} \\ \dots \dots \\ (g^{aby_n})^{-2x_n} = g^{-2abx_n y_n} \\ g^{a(x_1^2+x_2^2+\dots+x_n^2)} \end{cases} \quad (3)$$

在步骤 c9 中, 服务器利用第二中间加密数据、第一加密数据和第二私

钥 b ，得到第三中间加密数据，并向终端设备发送第三中间加密数据。

第三中间加密数据包括下式（4）中的 $g^{ab \sum_1^n (x_i - y_i)^2}$ 。

$$\begin{aligned} & g^{-2abx_1y_1} \times g^{-2abx_2y_2} \times \dots \times g^{-2abx_ny_n} \times g^{ab(x_1^2+x_2^2+\dots+x_n^2)} \times g^{ab(y_1^2+y_2^2+\dots+y_n^2)} \\ & = g^{ab \sum_1^n (x_i - y_i)^2} \end{aligned} \quad (4)$$

需要说明的是，由于在生物特征匹配场景中，终端设备被认为是不可信方，因此，加密状态中的目标欧氏距离必须由服务器构建得到。

在步骤 c10 中，终端设备利用第一私钥，消除第三中间加密数据中的第一私钥，得到第二加密数据，并向服务器发送第二加密数据。

第二加密数据包括下式（5）中的 $g^{b \sum_1^n (x_i - y_i)^2}$ 。

$$(g^{ab \sum_1^n (x_i - y_i)^2})^{-a} = g^{b \sum_1^n (x_i - y_i)^2} \quad (5)$$

由于终端设备无法得知第二私钥，因此终端设备无法构造出包括小于预设欧式距离匹配阈值的欧氏距离的计算算子，进一步提高了数据的安全性。

在步骤 c11 中，服务器根据第二私钥 b 和预设欧式距离匹配阈值 θ ，得到匹配数据集 $\{g^{b \times 0}, g^{b \times 1}, g^{b \times 2}, \dots, g^{b \times \theta^2}\}$ 。

这里的预设欧式距离匹配阈值 θ 以及之前的样本生物特征向量、待匹配生物特征向量可为已经过等倍数整数化的数据，因此该匹配数据集中的元素数量是有限的。

在步骤 c12 中，服务器判断第二加密数据 $g^{b \sum_1^n (x_i - y_i)^2}$ 是否在匹配数据集 $\{g^{b \times 0}, g^{b \times 1}, g^{b \times 2}, \dots, g^{b \times \theta^2}\}$ 中，若存在，则确定待匹配生物特征向量与样本生物特征向量匹配成功；若不存在，则确定待匹配生物特征向量与样本生物特征向量匹配失败。

目标欧式距离为 $\sqrt{\sum_1^n (x_i - y_i)^2}$ ，由于第二加密数据为密态下的数据，无法直接比较目标欧氏距离和预设欧式距离匹配阈值，可通过第二加密数据 $g^{b \sum_1^n (x_i - y_i)^2}$ 是否在匹配数据集 $\{g^{b \times 0}, g^{b \times 1}, g^{b \times 2}, \dots, g^{b \times \theta^2}\}$ 中来确定匹配结果。 $g^{b \sum_1^n (x_i - y_i)^2}$ 存在于集合 $\{g^{b \times 0}, g^{b \times 1}, g^{b \times 2}, \dots, g^{b \times \theta^2}\}$ 中，表示 $b \sum_1^n (x_i - y_i)^2 \leq b \theta^2$ ，即，表示 $\sqrt{\sum_1^n (x_i - y_i)^2} \leq \theta$ ，可确定待匹配生物特征向量与样本生物特征向量匹配成功。

上述步骤 c5 至步骤 c12 属于生物特征的匹配流程。

在第二个示例中，计算算子包括点乘算子，生物特征的注册及匹配流程可包括以下步骤 d1 至步骤 d12。

在步骤 d1 中，终端设备采集样本生物数据，通过向量转化模型将样本生物数据转化为样本生物特征向量 $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ 。

在步骤 d2 中，终端设备生成随机数 a ，将随机数 a 作为第一私钥。

在步骤 d3 中，终端设备利用生成元 g 和第一私钥 a ，对样本生物特征向量 $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ 进行加密，得到第一加密数据。

第一加密数据可包括下式 (6) 中的数据 $ay_i g$ 和 SY2，或者，可包括下式 (6) 中的数据 $ay_i g$ 和 $ay_i^2 g$ ， $i=1, 2, \dots, n$ 。

$$\left\{ \begin{array}{l} y'_1 = ay_1 g \\ y'_2 = ay_2 g \\ \dots \dots \\ y'_n = ay_n g \\ SY2 = a(y_1^2 g + y_2^2 g + \dots + y_n^2 g) \end{array} \right\} \quad (6)$$

在步骤 d4 中，将第一加密数据发送至服务器，由服务器存储第一加密数据。

点乘算子的格式为 $g \times p$ ，可利用密码学领域中的椭圆曲线公钥算法问题，来保证第一加密数据的安全性。即在生成元为 g 的椭圆曲线群中，生成元 g 为曲线上某个点，给定整数 p ，计算 $g \times p = q$ 是容易的，但根据 g 和 q 计算 p 则是困难的。服务器无法得知第一私钥 a ，且由于椭圆曲线公钥算法问题，服务器得到 $ay_i g$ ，也无法破解得到 y_i ，第一加密数据在服务器是以密态形式来保存的。

上述步骤 d1 至步骤 d4 属于生物特征的注册流程。

在步骤 d5 中，终端设备采集待匹配生物数据，通过向量转化模型将待匹配生物数据转化为待匹配生物特征向量 $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$ 。

在步骤 d6 中，服务器生成随机数 b ，将随机数 b 作为第二私钥。

在步骤 d7 中，服务器利用第二私钥对第一加密数据加密，得到第一中间加密数据，并向终端设备发送第一中间加密数据。

第一中间加密数据可包括下式 (7) 中的 $aby_i g$ 。

$$\begin{cases} y''_1 = aby_1g \\ y''_2 = aby_2g \\ \dots \dots \\ y''_n = aby_ng \end{cases} \quad (7)$$

在步骤 d8 中，终端设备根据待匹配生物特征向量 $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$ 、第一中间加密数据和第一私钥，得到第二中间加密数据，并向服务器发送第二中间加密数据。

第二中间加密数据可包括下式 (8) 中的 $-2abx_iy_ig$ 和 ax_i^2g 。

$$\begin{cases} aby_1g \times (-2x_1) = -2abx_1y_1g \\ aby_1g \times (-2x_2) = -2abx_2y_2g \\ \dots \dots \\ aby_1g \times (-2x_n) = -2abx_ny_ng \\ ax_1^2g + ax_2^2g + \dots + ax_n^2g \end{cases} \quad (8)$$

在步骤 d9 中，服务器利用第二中间加密数据、第一加密数据和第二私钥 b ，得到第三中间加密数据，并向终端设备发送第三中间加密数据。

第三中间加密数据包括下式 (9) 中的 $abg \sum_1^n (x_i - y_i)^2$ 。

$$-2abx_1y_1g - 2abx_2y_2g + \dots - 2abx_ny_ng + ab(x_1^2g + x_2^2g + \dots + x_n^2g) + ab(y_1^2g + y_2^2g + \dots + y_n^2g) = abg \sum_1^n (x_i - y_i)^2 \quad (9)$$

需要说明的是，由于在生物特征匹配场景中，终端设备被认为是不可信方，因此，加密状态中的目标欧氏距离必须由服务器构建得到。

在步骤 d10 中，终端设备利用第一私钥，消除第三中间加密数据中的第一私钥，得到第二加密数据，并向服务器发送第二加密数据。

第二加密数据包括下式 (10) 中的 $bg \sum_1^n (x_i - y_i)^2$ 。

$$abg \sum_1^n (x_i - y_i)^2 \times \frac{1}{a} = bg \sum_1^n (x_i - y_i)^2 \quad (10)$$

由于终端设备无法得知第二私钥，因此终端设备无法构造出包括小于预设欧式距离匹配阈值的欧氏距离的计算算子，进一步提高了数据的安全性。

在步骤 d11 中，服务器根据第二私钥 b 和预设欧式距离匹配阈值 θ ，得到匹配数据集 $\{gb \times 0, gb \times 1, gb \times 2, \dots, gb \times \theta^2\}$ 。

这里的预设欧式距离匹配阈值 θ 以及之前的样本生物特征向量、待匹配生物特征向量可为已经过等倍数整数化的数据，因此该匹配数据集其中的元素数量是有限的。

在步骤 d12 中, 服务器判断第二加密数据 $bg \sum_1^n (x_i - y_i)^2$ 是否在匹配数据集 $\{gb \times 0, gb \times 1, gb \times 2, \dots, gb \times \theta^2\}$ 中, 若存在, 则确定待匹配生物特征向量与样本生物特征向量匹配成功; 若不存在, 则确定待匹配生物特征向量与样本生物特征向量匹配失败。

目标欧式距离为 $\sqrt{\sum_1^n (x_i - y_i)^2}$, 由于第二加密数据为密态下的数据, 无法直接比较目标欧氏距离和预设欧式距离匹配阈值, 可通过第二加密数据 $bg \sum_1^n (x_i - y_i)^2$ 是否在匹配数据集 $\{gb \times 0, gb \times 1, gb \times 2, \dots, gb \times \theta^2\}$ 中来确定匹配结果。 $bg \sum_1^n (x_i - y_i)^2$ 存在于集合 $\{gb \times 0, gb \times 1, gb \times 2, \dots, gb \times \theta^2\}$ 中, 表示 $b \sum_1^n (x_i - y_i)^2 \leq b\theta^2$, 即, 表示 $\sqrt{\sum_1^n (x_i - y_i)^2} \leq \theta$, 可确定待匹配生物特征向量与样本生物特征向量匹配成功。

上述步骤 d5 至步骤 d12 属于生物特征的匹配流程。

本申请第三方面提供一种终端设备。图 6 为本申请第三方面一实施例提供的终端设备的结构示意图, 如图 6 所示, 该终端设备 400 可包括第一通信模块 401 和第一加密模块 402。

第一通信模块 401 和第一加密模块 402 可用于与服务器基于第一私钥、获取的待匹配生物特征向量、预设的生成元、第二私钥和第一加密数据, 进行多次交互和处理, 得到第二加密数据。

第一私钥为终端设备的私钥。第二私钥为服务器的私钥。第一加密数据由终端设备预先利用生成元和第一私钥对样本生物特征向量加密得到并发送至服务器。第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子。目标欧式距离包括待匹配生物特征向量与样本生物特征向量的欧式距离。

在一些示例中, 计算算子包括模指数算子或点乘算子。

第一通信模块 401 还可用于向服务器发送第二加密数据, 以使服务器利用第二加密数据、生成元、第二私钥和预设欧式距离匹配阈值, 得到待匹配生物特征向量与样本生物特征向量的匹配结果。

在本申请实施例中, 终端设备与服务器可基于第一私钥、待匹配生物特征向量、生成元、第二私钥、第一加密数据进行多次交互和处理, 终端设备具有第一私钥、待匹配生物特征和生成元, 服务器具有第二私钥和第

一加密数据。通过终端设备利用第一私钥的加密处理、服务器利用第二私钥的加密处理、以及终端设备与服务器之间的数据交互，使终端设备能够得到包括第二私钥和能够表征待匹配生物特征向量与样本生物特征向量的欧式距离的目标欧氏距离的计算算子的第二加密数据，第二加密数据中包含第二私钥，终端设备无法得知第二私钥，难以破解得到待匹配生物特征向量和样本生物特征向量的明文，同理，服务器无法得知第一私钥，也难以破解第一加密私钥。且服务器是根据第二加密数据、生成元、第二私钥和预设欧式距离匹配阈值，来确定待匹配生物特征向量与样本生物特征向量的匹配结果的，可在不涉及待匹配生物特征向量的明文和样本生物特征向量的明文的条件下完成匹配，从而降低用户隐私数据的安全风险，提高生物特征匹配的安全性。由于终端设备和服务器也不会存储待匹配生物特征向量的明文和样本生物特征向量的明文，能够保证用户对个人隐私数据的控制权，从而限制个人隐私数据的使用场景，满足个人隐私数据的最小化使用原则，防止个人隐私数据被滥用。

而且，本申请实施例中是对待匹配生物特征向量、样本生物特征向量进行加密处理，以及通过加密处理后的数据的比对来确定匹配结果，待匹配生物数据和样本生物数据的种类不同，可采用的向量转化模型也可不同，但本申请实施例中是通过特征向量的相似度来描述生物数据的相似度。本申请实施例的生物特征的匹配过程中对个人隐私数据的保护流程与待匹配生物数据转化为待匹配生物特征向量、样本生物数据转换为样本生物特征向量的转化流程可相互独立，从而实现了向量转化模型与生物特征匹配模型的可组装、可插拔的技术方案，即实现了向量转化模型与生物特征匹配模型的解耦。

在一些实施例中，第一通信模块 401 可用于接收服务器发送的第一中间加密数据。

第一中间加密数据由服务器利用第二私钥对第一加密数据加密得到。第一中间加密数据中形成包括第一私钥、第二私钥与样本生物特征向量中元素的乘积的计算算子。

第一加密模块 402 可用于根据第一中间加密数据、待匹配生物特征向

量、生成元、第一私钥，得到第二中间加密数据，

第二中间加密数据中形成包括第一私钥、第二私钥和待匹配生物特征向量中元素的乘积的计算算子。

第一通信模块 401 和第一加密模块 402 可用于与服务器基于第二中间加密数据、第一加密数据、第一私钥和第二私钥进行交互和处理，消除处理后的数据中的第一私钥，得到第二加密数据。

在一些示例中，第二中间加密数据包括第一中间加密子数据和第二中间加密子数据。

第一加密模块 402 可用于：根据第一中间加密数据和待匹配生物特征向量，得到第一中间加密子数据；根据第一私钥、生成元和待匹配生物特征向量，得到第二中间加密子数据。

第一中间加密子数据中形成包括第一私钥、第二私钥、样本生物特征向量中元素与待匹配生物特征向量中元素的乘积的计算算子。第二中间加密子数据中形成包括第一私钥与待匹配生物特征向量中元素的乘积的计算算子。

在一些示例中，第一通信模块 401 可用于向服务器发送第二中间加密数据，以使服务器基于第二中间加密数据、第一加密数据和第二私钥，得到第三中间加密数据；接收服务器发送的第三中间加密数据。

第三中间加密数据中形成包括第一私钥、第二私钥与目标欧式距离的乘积的计算算子。

第一加密模块 402 可用于利用第一私钥，消除第三中间加密数据中的第一私钥，得到第二加密数据。

在一些实施例中，在第二加密数据属于匹配数据集合的情况下，匹配结果包括匹配成功。在第二加密数据不属于匹配数据集合的情况下，匹配结果包括匹配失败。其中，匹配数据集合中元素的最大值基于第二私钥和预设欧式距离匹配阈值得到。

在一些示例中，待匹配生物特征向量中的元素、样本生物特征向量中的元素以及预设欧式距离匹配阈值等倍数整数化。匹配数据集合中形成包括第二私钥分别与 0 至整数化后的预设欧式距离匹配阈值的平方的乘积的

计算算子。

在一些示例中，在 K 个目标哈希值在预先建立的布隆过滤器查找表中对应位置的数值均为 1 的情况下，第二加密数据属于匹配数据集合。在 K 个目标哈希值在布隆过滤器查找表中对应位置的数值至少一处为 0 的情况下，第二加密数据不属于匹配数据集合。其中， K 个目标哈希值基于第二加密数据根据 K 个哈希函数计算得到，布隆过滤器查找表中的数值基于匹配数据集合中的元素根据 K 个哈希函数计算得到， K 为正整数。

在一些实施例中，终端设备 400 还可包括第一获取模块。

第一获取模块用于获取样本生物特征向量。

第一加密模块 402 还可用于利用生成元和第一私钥对样本生物特征向量加密，得到第一加密数据。

第一加密数据中形成包括第一私钥与样本生物特征向量中元素的乘积的计算算子。

第一通信模块 401 还可用于向服务器发送第一加密数据。

本申请第四方面提供一种服务器。图 7 为本申请第四方面一实施例提供的服务器的结构示意图，如图 7 所示，该服务器 500 可包括第二通信模块 501、第二加密模块 502 和匹配模块 503。

第二通信模块 501 和第二加密模块 502 可用于与终端设备基于第二私钥、第一加密数据、第一私钥、预设的生成元和终端设备获取的待匹配生物特征向量，进行多次交互和处理，以使终端设备得到第二加密数据。

第一私钥为终端设备的私钥。第二私钥为服务器的私钥。第一加密数据由终端设备预先利用生成元和第一私钥对样本生物特征向量加密得到并发送至服务器。第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子。目标欧式距离包括待匹配生物特征向量与样本生物特征向量的欧式距离。

在一些示例中，计算算子包括模指数算子或点乘算子。

第二通信模块 501 还用于接收终端设备发送的第二加密数据。

匹配模块 503 可用于利用第二加密数据、第二私钥、生成元和预设欧式距离匹配阈值，得到待匹配生物特征向量与样本生物特征向量的匹配结

果。

在本申请实施例中，服务器与终端设备可基于第一私钥、待匹配生物特征向量、生成元、第二私钥、第一加密数据进行多次交互和处理，终端设备具有第一私钥、待匹配生物特征和生成元，服务器具有第二私钥和第一加密数据。通过终端设备利用第一私钥的加密处理、服务器利用第二私钥的加密处理、以及终端设备与服务器之间的数据交互，使终端设备能够得到包括第二私钥和能够表征待匹配生物特征向量与样本生物特征向量的欧式距离的目标欧氏距离的计算算子的第二加密数据，第二加密数据中包含第二私钥，终端设备无法得知第二私钥，难以破解得到待匹配生物特征向量和样本生物特征向量的明文，同理，服务器无法得知第一私钥，也难以破解第一加密私钥。且服务器是根据第二加密数据、生成元、第二私钥和预设欧式距离匹配阈值，来确定待匹配生物特征向量与样本生物特征向量的匹配结果的，可在不涉及待匹配生物特征向量的明文和样本生物特征向量的明文的条件下完成匹配，从而降低用户隐私数据的安全风险，提高生物特征匹配的安全性。由于终端设备和服务器也不会存储待匹配生物特征向量的明文和样本生物特征向量的明文，能够保证用户对个人隐私数据的控制权，从而限制个人隐私数据的使用场景，满足个人隐私数据的最小化使用原则，防止个人隐私数据被滥用。

而且，本申请实施例中是对待匹配生物特征向量、样本生物特征向量进行加密处理，以及通过加密处理后的数据的比对来确定匹配结果，待匹配生物数据和样本生物数据的种类不同，可采用的向量转化模型也可不同，但本申请实施例中是通过特征向量的相似度来描述生物数据的相似度。本申请实施例的生物特征的匹配过程中对个人隐私数据的保护流程与待匹配生物数据转化为待匹配生物特征向量、样本生物数据转换为样本生物特征向量的转化流程可相互独立，从而实现了向量转化模型与生物特征匹配模型的可组装、可插拔的技术方案，即实现了向量转化模型与生物特征匹配模型的解耦。

在一些实施例中，第二加密模块 502 可用于利用第二私钥对第一加密数据加密，得到第一中间加密数据。

第一中间加密数据中形成包括第一私钥、第二私钥与样本生物特征向量中元素的乘积的计算算子。

第二通信模块 501 可用于向终端设备发送第一中间加密数据，以使终端设备根据第一中间加密数据、待匹配生物特征向量、生成元和第一私钥得到第二中间加密数据。

第二中间加密数据中形成包括第一私钥和待匹配生物特征向量中元素的乘积的计算算子。

第二通信模块 501 与第二加密模块 502 可用于与终端设备基于第二中间加密数据、第一加密数据、第一私钥和第二私钥进行交互和处理，以使终端设备消除处理后的数据中的第一私钥，得到第二加密数据。

在一些示例中，第二中间加密数据包括第一中间加密子数据和第二中间加密子数据。

第一中间加密子数据由终端设备根据第一中间加密数据和待匹配生物特征向量得到。第一中间加密子数据中形成包括第一私钥、第二私钥、样本生物特征向量中元素与待匹配生物特征向量中元素的乘积的计算算子。

第二中间加密子数据由终端设备根据第一私钥、生成元和待匹配生物特征向量得到。第二中间加密子数据中形成包括第一私钥与待匹配生物特征向量中元素的乘积的计算算子。

在一些示例中，第二通信模块 501 可用于接收终端设备发送的第二中间加密数据。

第二加密模块 502 可用于基于第二中间加密数据、第一加密数据和第二私钥，得到第三中间加密数据。

第三中间加密数据中形成包括第一私钥、第二私钥与目标欧式距离的乘积的计算算子。

第二通信模块 501 可用于向终端设备发送第三中间加密数据，以使终端设备利用第一私钥消除第三中间加密数据中的第一私钥，得到第二加密数据。

在一些实施例中，匹配模块 503 可用于：基于第二私钥、生成元和预设欧式距离匹配阈值，得到匹配数据集合，匹配数据集合中元素的最大值

基于第二私钥和预设欧式距离匹配阈值得到；在第二加密数据属于匹配数据集合的情况下，确定匹配结果包括匹配成功；在第二加密数据不属于匹配数据集合的情况下，确定匹配结果包括匹配失败。

在一些示例中，待匹配生物特征向量中的元素、样本生物特征向量中的元素以及预设欧式距离匹配阈值等倍数整数化。

匹配模块 503 可用于：分别计算第二私钥与 0 至整数化后的预设欧式距离匹配阈值的平方的乘积；根据第二私钥与 0 至整数化后的预设欧式距离匹配阈值的平方的乘积和生成元，得到匹配数据集合。

在一些示例中，匹配模块 503 还可用于：基于第二加密数据，根据 K 和哈希函数，计算得到 K 个目标哈希值；在 K 个目标哈希值在预先建立的布隆过滤器查找表中对应位置的数值均为 1 的情况下，确定第二加密数据属于匹配数据集合；在 K 个目标哈希值在布隆过滤器查找表中对应位置的数值至少一处为 0 的情况下，确定第二加密数据不属于匹配数据集合。

其中，K 个目标哈希值基于第二加密数据根据 K 个哈希函数计算得到，布隆过滤器查找表中的数值基于匹配数据集合中的元素根据 K 个哈希函数计算得到，K 为正整数。

在一些实施例中，服务器 500 还可包括查找表生成模块，该查找表生成模块可用于：利用 K 个哈希函数，对匹配数据集合中的每个元素进行计算，得到每个元素对应的 K 个哈希值；将每个元素对应的 K 个哈希值映射至值均为 0 的二进制数组中的 K 个位置，并将每个元素对应的 K 个位置的数值更新为 1，将更新后的二进制数组确定为布隆过滤器查找表。

本申请第五方面还提供了一种终端设备。图 8 为本申请第五方面一实施例提供的终端设备的结构示意图。如图 8 所示，终端设备 600 包括存储器 601、处理器 602 及存储在存储器 601 上并可在处理器 602 上运行的计算机程序。

在一些示例中，上述处理器 602 可以包括中央处理器（CPU），或者特定集成电路（Application Specific Integrated Circuit，ASIC），或者可以被配置成实施本申请实施例的一个或多个集成电路。

存储器 601 可包括只读存储器 (Read-Only Memory, ROM), 随机存取存储器 (Random Access Memory, RAM), 磁盘存储介质设备, 光存储介质设备, 闪存设备, 电气、光学或其他物理/有形的存储器存储设备。因此, 通常, 存储器包括一个或多个编码有包括计算机可执行指令的软件的有形 (非暂态) 计算机可读存储介质 (例如, 存储器设备), 并且当该软件被执行 (例如, 由一个或多个处理器) 时, 其可操作来执行参考根据本申请第一方面实施例中生物特征匹配方法所描述的操作。

处理器 602 通过读取存储器 601 中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序, 以用于实现上述第一方面实施例中的生物特征匹配方法。

在一些示例中, 终端设备 600 还可包括通信接口 603 和总线 604。其中, 如图 8 所示, 存储器 601、处理器 602、通信接口 603 通过总线 604 连接并完成相互间的通信。

通信接口 603, 主要用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。也可通过通信接口 603 接入输入设备和/或输出设备。

总线 604 包括硬件、软件或两者, 将终端设备 600 的部件彼此耦接在一起。举例来说而非限制, 总线 604 可包括加速图形端口 (Accelerated Graphics Port, AGP) 或其他图形总线、增强工业标准架构 (Enhanced Industry Standard Architecture, EISA) 总线、前端总线 (Front Side Bus, FSB)、超传输 (Hyper Transport, HT) 互连、工业标准架构 (Industry Standard Architecture, ISA) 总线、无限带宽互连、低引脚数 (Low pin count, LPC) 总线、存储器总线、微信道架构 (Micro Channel Architecture, MCA) 总线、外围组件互连 (Peripheral Component Interconnect, PCI) 总线、PCI-Express (PCI-E) 总线、串行高级技术附件 (Serial Advanced Technology Attachment, SATA) 总线、视频电子标准协会局部 (Video Electronics Standards Association Local Bus, VLB) 总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下, 总线 604 可包括一个或多个总线。尽管本申请实施例描述和示出了特定的总线, 但本申请考虑任何合适的总线或互连。

本申请第六方面还提供了一种服务器。图 9 为本申请第六方面一实施例提供的服务器的结构示意图。如图 9 所示，服务器 700 包括存储器 701、处理器 702 及存储在存储器 701 上并可在处理器 702 上运行的计算机程序。

在一些示例中，上述处理器 702 可以包括中央处理器（CPU），或者特定集成电路（Application Specific Integrated Circuit，ASIC），或者可以被配置成实施本申请实施例的一个或多个集成电路。

存储器 701 可包括只读存储器（Read-Only Memory，ROM），随机存取存储器（Random Access Memory，RAM），磁盘存储介质设备，光存储介质设备，闪存设备，电气、光学或其他物理/有形的存储器存储设备。因此，通常，存储器包括一个或多个编码有包括计算机可执行指令的软件有形（非暂态）计算机可读存储介质（例如，存储器设备），并且当该软件被执行（例如，由一个或多个处理器）时，其可操作来执行参考根据本申请第二方面实施例中生物特征匹配方法所描述的操作。

处理器 702 通过读取存储器 701 中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述第二方面实施例中的生物特征匹配方法。

在一些示例中，终端设备 700 还可包括通信接口 703 和总线 704。其中，如图 9 所示，存储器 701、处理器 702、通信接口 703 通过总线 704 连接并完成相互间的通信。

通信接口 703，主要用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。也可通过通信接口 703 接入输入设备和/或输出设备。

总线 704 包括硬件、软件或两者，将服务器 700 的部件彼此耦接在一起。举例来说而非限制，总线 704 可包括加速图形端口（Accelerated Graphics Port，AGP）或其他图形总线、增强工业标准架构（Enhanced Industry Standard Architecture，EISA）总线、前端总线（Front Side Bus，FSB）、超传输（Hyper Transport，HT）互连、工业标准架构（Industry Standard Architecture，ISA）总线、无限带宽互连、低引脚数（Low pin count，LPC）总线、存储器总线、微信道架构（Micro Channel Architecture，MCA）总线、外围组件互连（Peripheral Component Interconnect，PCI）总

线、PCI-Express (PCI-E) 总线、串行高级技术附件 (Serial Advanced Technology Attachment, SATA) 总线、视频电子标准协会局部 (Video Electronics Standards Association Local Bus, VLB) 总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下, 总线 704 可包括一个或多个总线。尽管本申请实施例描述和示出了特定的总线, 但本申请考虑任何合适的总线或互连。

本申请第七方面提供一种生物特征匹配系统, 该生物特征匹配系统可包括上述实施例中的终端设备和服务器, 终端设备可执行上述第一方面实施例中的生物特征匹配方法, 服务器可执行上述第二方面实施例中的生物特征匹配方法, 具体内容可参见上述实施例中的相关说明, 在此不再赘述。

本申请第八方面还提供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指令, 该计算机程序指令被处理器执行时可实现上述第一方面实施例中的生物特征匹配方法或第二方面实施例中的生物特征匹配方法, 且能达到相同的技术效果, 为避免重复, 这里不再赘述。其中, 上述计算机可读存储介质可包括非暂态计算机可读存储介质, 如只读存储器 (Read-Only Memory, 简称 ROM)、随机存取存储器 (Random Access Memory, 简称 RAM)、磁碟或者光盘等, 在此并不限定。

本申请实施例还可提供一种计算机程序产品, 该计算机程序产品中的指令由电子设备的处理器执行时, 使得该电子设备可执行第一方面实施例中的生物特征匹配方法或第二方面实施例中的生物特征匹配方法, 具体内容可参见上述实施例中的相关说明, 且能达到相同的技术效果, 为避免重复, 这里不再赘述。

需要明确的是, 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或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。对于终端设备实施例、服务器实施例、系统实施例、计算机可读存储介质实施例、计算机程序产品实施例而言, 相关之处可以参见方法实施例的说明部分。本申请并不局限于上文所描述并在图中示出的特定步骤和结构。本领域的技术人员可以在领会本申请的精神之后, 作出各种改变、修改和添加, 或者改变步骤之间的顺序。并且, 为

了简明起见，这里省略对已知方法技术的详细描述。

上面参考根据本申请的实施例的方法、装置（系统）和计算机程序产品的流程图和/或框图描述了本申请的各方面。应当理解，流程图和/或框图中的每个方框以及流程图和/或框图中各方框的组合可以由计算机程序指令实现。这些计算机程序指令可被提供给通用计算机、专用计算机、或其它可编程数据处理装置的处理器，以产生一种机器，使得经由计算机或其它可编程数据处理装置的处理器执行的这些指令使能对流程图和/或框图的一个或多个方框中指定的功能/动作的实现。这种处理器可以是但不限于是通用处理器、专用处理器、特殊应用处理器或者现场可编程逻辑电路。还可理解，框图和/或流程图中的每个方框以及框图和/或流程图中的方框的组合，也可以由执行指定的功能或动作的专用硬件来实现，或可由专用硬件和计算机指令的组合来实现。

本领域技术人员应能理解，上述实施例均是示例性而非限制性的。在不同实施例中出现的不同技术特征可以进行组合，以取得有益效果。本领域技术人员在研究附图、说明书及权利要求书的基础上，应能理解并实现所揭示的实施例的其他变化的实施例。在权利要求书中，术语“包括”并不排除其他装置或步骤；数量词“一个”不排除多个；术语“第一”、“第二”用于标示名称而非用于表示任何特定的顺序。权利要求中的任何附图标记均不应被理解为对保护范围的限制。权利要求中出现的多个部分的功能可以由一个单独的硬件或软件模块来实现。某些技术特征出现在不同的从属权利要求中并不意味着不能将这些技术特征进行组合以取得有益效果。

权 利 要 求 书

1. 一种生物特征匹配方法，应用于终端设备，所述方法包括：

与服务器基于第一私钥、获取的待匹配生物特征向量、预设的生成元、第二私钥和第一加密数据，进行多次交互和处理，得到第二加密数据，所述第一私钥为所述终端设备的私钥，所述第二私钥为所述服务器的私钥，所述第一加密数据由所述终端设备预先利用所述生成元和所述第一私钥对样本生物特征向量加密得到并发送至所述服务器，所述第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子，所述目标欧氏距离包括所述待匹配生物特征向量与所述样本生物特征向量的欧式距离；

向所述服务器发送所述第二加密数据，以使所述服务器利用所述第二加密数据、所述生成元、所述第二私钥和预设欧式距离匹配阈值，得到所述待匹配生物特征向量与所述样本生物特征向量的匹配结果。

2. 根据权利要求1所述的方法，其中，所述与服务器基于第一私钥、获取的待匹配生物特征向量、预设的生成元、第二私钥和第一加密数据，进行多次交互和处理，得到第二加密数据，包括：

接收所述服务器发送的第一中间加密数据，所述第一中间加密数据由所述服务器利用所述第二私钥对所述第一加密数据加密得到，所述第一中间加密数据中形成包括所述第一私钥、所述第二私钥与所述样本生物特征向量中元素的乘积的计算算子；

根据所述第一中间加密数据、所述待匹配生物特征向量、所述生成元、所述第一私钥，得到第二中间加密数据，所述第二中间加密数据中形成包括所述第一私钥、所述第二私钥和所述待匹配生物特征向量中元素的乘积的计算算子；

与所述服务器基于所述第二中间加密数据、所述第一加密数据、所述第一私钥和所述第二私钥进行交互和处理，消除处理后的数据中的所述第一私钥，得到所述第二加密数据。

3. 根据权利要求2所述的方法，其中，所述第二中间加密数据包括第一中间加密子数据和第二中间加密子数据，

所述根据所述第一中间加密数据、所述待匹配生物特征向量、所述生成元、所述第一私钥，得到第二中间加密数据，包括：

根据所述第一中间加密数据和所述待匹配生物特征向量，得到所述第一中间加密子数据，所述第一中间加密子数据中形成包括所述第一私钥、所述第二私钥、所述样本生物特征向量中元素与所述待匹配生物特征向量中元素的乘积的计算算子；

根据所述第一私钥、所述生成元和所述待匹配生物特征向量，得到所述第二中间加密子数据，所述第二中间加密子数据中形成包括所述第一私钥与所述待匹配生物特征向量中元素的乘积的计算算子。

4. 根据权利要求3所述的方法，其中，所述与所述服务器基于所述第二中间加密数据、所述第一加密数据、所述第一私钥和所述第二私钥进行交互和处理，消除处理后的数据中的所述第一私钥，得到所述第二加密数据，包括：

向所述服务器发送所述第二中间加密数据，以使所述服务器基于所述第二中间加密数据、所述第一加密数据和所述第二私钥，得到第三中间加密数据，所述第三中间加密数据中形成包括所述第一私钥、所述第二私钥与所述目标欧式距离的乘积的计算算子；

接收所述服务器发送的所述第三中间加密数据；

利用所述第一私钥，消除所述第三中间加密数据中的所述第一私钥，得到所述第二加密数据。

5. 根据权利要求1所述的方法，其中，

在所述第二加密数据属于匹配数据集合的情况下，所述匹配结果包括匹配成功；

在所述第二加密数据不属于所述匹配数据集合的情况下，所述匹配结果包括匹配失败；

其中，所述匹配数据集合中元素的最大值基于所述第二私钥和所述预设欧式距离匹配阈值得到。

6. 根据权利要求5所述的方法，其中，

所述待匹配生物特征向量中的元素、所述样本生物特征向量中的元素

以及所述预设欧式距离匹配阈值等倍数整数化，

所述匹配数据集合中形成包括所述第二私钥分别与 0 至整数化后的所述预设欧式距离匹配阈值的平方的乘积的计算算子。

7. 根据权利要求 5 所述的方法，其中，

在 K 个目标哈希值在预先建立的布隆过滤器查找表中对应位置的数值均为 1 的情况下，所述第二加密数据属于所述匹配数据集合；

在 K 个目标哈希值在所述布隆过滤器查找表中对应位置的数值至少一处为 0 的情况下，所述第二加密数据不属于所述匹配数据集合；

其中，K 个目标哈希值基于所述第二加密数据根据 K 个哈希函数计算得到，所述布隆过滤器查找表中的数值基于所述匹配数据集合中的元素根据所述 K 个哈希函数计算得到，K 为正整数。

8. 根据权利要求 1 所述的方法，其中，在所述与服务器基于第一私钥、获取的待匹配生物特征向量、第二私钥和第一加密数据，进行多次交互和处理，得到第二加密数据之前，还包括：

获取所述样本生物特征向量；

利用所述生成元和所述第一私钥对所述样本生物特征向量加密，得到所述第一加密数据，所述第一加密数据中形成包括所述第一私钥与所述样本生物特征向量中元素的乘积的计算算子；

向所述服务器发送所述第一加密数据。

9. 根据权利要求 1 至 8 中任意一项所述的方法，其中，计算算子包括模指数算子或点乘算子。

10. 一种生物特征匹配方法，应用于服务器，所述方法包括：

与终端设备基于第二私钥、第一加密数据、第一私钥、预设的生成元和所述终端设备获取的待匹配生物特征向量，进行多次交互和处理，以使所述终端设备得到第二加密数据，所述第一私钥为所述终端设备的私钥，所述第二私钥为所述服务器的私钥，所述第一加密数据由所述终端设备预先利用所述生成元和所述第一私钥对样本生物特征向量加密得到并发送至所述服务器，所述第二加密数据中形成包括所述第二私钥和目标欧氏距离的计算算子，所述目标欧式距离包括所述待匹配生物特征向量与所述样本

生物特征向量的欧式距离；

接收所述终端设备发送的所述第二加密数据；

利用所述第二加密数据、所述第二私钥、所述生成元和预设欧式距离匹配阈值，得到所述待匹配生物特征向量与所述样本生物特征向量的匹配结果。

11. 根据权利要求 10 所述的方法，其中，所述与终端设备基于第二私钥、第一加密数据、第一私钥、预设的生成元和所述终端设备获取的待匹配生物特征向量，进行多次交互和处理，以使所述终端设备得到第二加密数据，包括：

利用所述第二私钥对所述第一加密数据加密，得到所述第一中间加密数据，所述第一中间加密数据中形成包括所述第一私钥、所述第二私钥与所述样本生物特征向量中元素的乘积的计算算子；

向所述终端设备发送所述第一中间加密数据，以使所述终端设备根据第一中间加密数据、所述待匹配生物特征向量、所述生成元和所述第一私钥得到第二中间加密数据，所述第二中间加密数据中形成包括所述第一私钥和所述待匹配生物特征向量中元素的乘积的计算算子；

与所述终端设备基于第二中间加密数据、所述第一加密数据、所述第一私钥和所述第二私钥进行交互和处理，以使所述终端设备消除处理后的数据中的所述第一私钥，得到所述第二加密数据。

12. 根据权利要求 11 所述的方法，其中，所述第二中间加密数据包括第一中间加密子数据和第二中间加密子数据，

所述第一中间加密子数据由所述终端设备根据所述第一中间加密数据和所述待匹配生物特征向量得到，所述第一中间加密子数据中形成包括所述第一私钥、所述第二私钥、所述样本生物特征向量中元素与所述待匹配生物特征向量中元素的乘积的计算算子，

所述第二中间加密子数据由所述终端设备根据所述第一私钥、所述生成元和所述待匹配生物特征向量得到，所述第二中间加密子数据中形成包括所述第一私钥与所述待匹配生物特征向量中元素的乘积的计算算子。

13. 根据权利要求 12 所述的方法，其中，所述与所述终端设备基于第

二中间加密数据、所述第一加密数据、所述第一私钥和所述第二私钥进行交互和处理，以使所述终端设备消除处理后的数据中的所述第一私钥，得到所述第二加密数据，包括：

接收所述终端设备发送的所述第二中间加密数据；

基于所述第二中间加密数据、所述第一加密数据和所述第二私钥，得到第三中间加密数据，所述第三中间加密数据中形成包括所述第一私钥、所述第二私钥与所述目标欧式距离的乘积的计算算子；

向所述终端设备发送所述第三中间加密数据，以使所述终端设备利用第一私钥消除所述第三中间加密数据中的所述第一私钥，得到所述第二加密数据。

14. 根据权利要求 10 所述的方法，其中，所述利用所述第二加密数据、所述第二私钥、所述生成元和预设欧式距离匹配阈值，得到所述待匹配生物特征向量与所述样本生物特征向量的匹配结果，包括：

基于所述第二私钥、所述生成元和所述预设欧式距离匹配阈值，得到匹配数据集合，所述匹配数据集合中元素的最大值基于所述第二私钥和所述预设欧式距离匹配阈值得到；

在所述第二加密数据属于匹配数据集合的情况下，确定所述匹配结果包括匹配成功；

在所述第二加密数据不属于所述匹配数据集合的情况下，确定所述匹配结果包括匹配失败。

15. 根据权利要求 14 所述的方法，其中，所述待匹配生物特征向量中的元素、所述样本生物特征向量中的元素以及所述预设欧式距离匹配阈值等倍数整数化，

所述基于所述第二私钥、所述生成元和所述预设欧式距离匹配阈值，得到匹配数据集合，包括：

分别计算所述第二私钥与 0 至整数化后的所述预设欧式距离匹配阈值的平方的乘积；

根据所述第二私钥与 0 至整数化后的所述预设欧式距离匹配阈值的平方的乘积和所述生成元，得到所述匹配数据集合。

16. 根据权利要求 14 所述的方法，还包括：

基于所述第二加密数据，根据 K 和哈希函数，计算得到 K 个目标哈希值；

在 K 个目标哈希值在预先建立的布隆过滤器查找表中对应位置的数值均为 1 的情况下，确定所述第二加密数据属于所述匹配数据集合；

在 K 个目标哈希值在所述布隆过滤器查找表中对应位置的数值至少一处为 0 的情况下，确定所述第二加密数据不属于所述匹配数据集合；

其中， K 个目标哈希值基于所述第二加密数据根据 K 个哈希函数计算得到，所述布隆过滤器查找表中的数值基于所述匹配数据集合中的元素根据所述 K 个哈希函数计算得到， K 为正整数。

17. 根据权利要求 16 所述的方法，还包括：

利用所述 K 个哈希函数，对所述匹配数据集合中的每个元素进行计算，得到每个元素对应的 K 个哈希值；

将每个元素对应的 K 个哈希值映射至值均为 0 的二进制数组中的 K 个位置，并将每个元素对应的所述 K 个位置的数值更新为 1，将更新后的二进制数组确定为所述布隆过滤器查找表。

18. 根据权利要求 10 至 17 中任意一项所述的方法，其中，计算算子包括模指数算子或点乘算子。

19. 一种终端设备，包括第一通信模块和第一加密模块；

所述第一通信模块和所述第一加密模块用于与服务器基于第一私钥、获取的待匹配生物特征向量、预设的生成元、第二私钥和第一加密数据，进行多次交互和处理，得到第二加密数据，所述第一私钥为所述终端设备的私钥，所述第二私钥为所述服务器的私钥，所述第一加密数据由所述终端设备预先利用所述生成元和所述第一私钥对样本生物特征向量加密得到并发送至所述服务器，所述第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子，所述目标欧氏距离包括所述待匹配生物特征向量与所述样本生物特征向量的欧式距离；

所述第一通信模块还用于向所述服务器发送所述第二加密数据，以使所述服务器利用所述第二加密数据、所述生成元、所述第二私钥和预设欧

式距离匹配阈值，得到所述待匹配生物特征向量与所述样本生物特征向量的匹配结果。

20. 一种服务器，包括第二通信模块、第二加密模块和匹配模块；

所述第二通信模块和所述第二加密模块用于与终端设备基于第二私钥、第一加密数据、第一私钥、预设的生成元和所述终端设备获取的待匹配生物特征向量，进行多次交互和处理，以使所述终端设备得到第二加密数据，所述第一私钥为所述终端设备的私钥，所述第二私钥为所述服务器的私钥，所述第一加密数据由所述终端设备预先利用所述生成元和所述第一私钥对样本生物特征向量加密得到并发送至所述服务器，所述第二加密数据中形成包括所述第二私钥和目标欧氏距离的计算算子，所述目标欧式距离包括所述待匹配生物特征向量与所述样本生物特征向量的欧式距离；

所述第二通信模块还用于接收所述终端设备发送的所述第二加密数据；

所述匹配模块用于利用所述第二加密数据、所述第二私钥、所述生成元和预设欧式距离匹配阈值，得到所述待匹配生物特征向量与所述样本生物特征向量的匹配结果。

21. 一种终端设备，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 1 至 9 中任意一项所述的生物特征匹配方法。

22. 一种服务器，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 10 至 18 中任意一项所述的生物特征匹配方法。

23. 一种生物特征匹配系统，包括如权利要求 21 所述的终端设备和如权利要求 22 所述的服务器。

24. 一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现如权利要求 1 至 18 中任意一项所述的生物特征匹配方法。