(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110300971 B
(45)授权公告日 2022.07.15

(21)申请号 201880012203.9

(22)申请日 2018.02.13

(65)同一申请的已公布的文献号
申请公布号 CN 110300971 A

(43)申请公布日 2019.10.01

(30)优先权数据
1750188-3 2017.02.22 SE

(85)PCT国际申请进入国家阶段日
2019.08.15

(86)PCT国际申请的申请数据
PCT/SE2018/050130 2018.02.13

(87)PCT国际申请的公布数据
WO2018/156068 EN 2018.08.30

(73)专利权人 指纹卡安娜卡敦知识产权有限公司
地址 瑞典哥德堡

(72)发明人 克里斯蒂安·格尔曼

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 陈炜 李德山

(51)Int.Cl.
G06F 21/32(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
WO 2016128906 A1,2016.08.18
US 6751734 B1,2004.06.15
US 2015381616 A1,2015.12.31
US 2011037563 A1,2011.02.17
CN 101720540 A,2010.06.02
US 2010191967 A1,2010.07.29
US 2007165847 A1,2007.07.19
US 2016164682 A1,2016.06.09
KR 100824733 B1,2008.04.28
US 2011026781 A1,2011.02.03
US 2016173455 A1,2016.06.16
CN 102215223 A,2011.10.12
CN 104767624 A,2015.07.08
CN 101552776 A,2009.10.07
CN 101369892 A,2009.02.18
CN 105553657 A,2016.05.04 (续)

审查员 陈玲

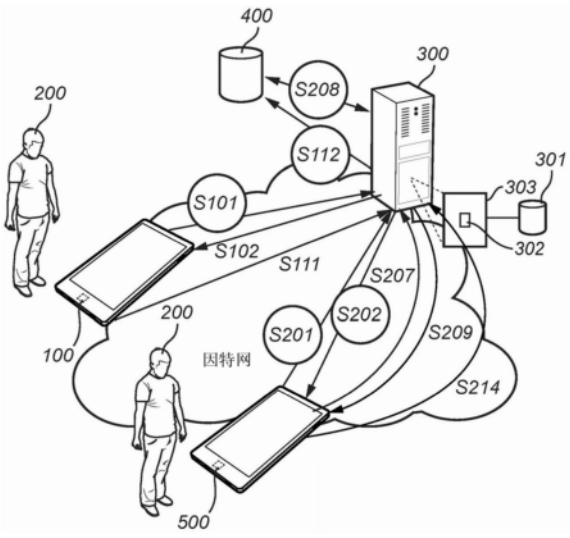
权利要求书6页 说明书10页 附图5页

(54)发明名称

基于生物特征的认证的方法、网络节点、客户端设备和存储介质

(57)摘要

本发明涉及用于使得能够基于生物特征数据对用户进行认证的方法和设备。在本发明的一个方面中，提供了一种由客户端设备(100)执行的、使得能够基于生物特征数据通过安全通信信道利用网络节点对客户端设备(100)的用户(200)进行认证的方法。此外，由客户端设备提供用于认证的注册集，其中，所述注册集包括模糊保险库，该模糊保险库包含注册的生物特征数据和第一秘密密钥。注册集还包括经转换的不可逆的生物特征数据、第二秘密密钥和秘密随机数。



CN 110300971 B

[转续页]

[接上页]

(56)对比文件

Tran Khanh Dang.Cancellable fuzzy vault with periodic transformation for biometric template protection.《IET Biometrics》.2016,第5卷(第3期),文章第2.1-2.2,3.1节.

Christian Rathgeb.A survey on biometric cryptosystems and cancelable biometrics.《Rathgeb and Uhl EURASIP Journal on Information Security 2011》.2011,全文.

Karthik Nandakumar.BioSAKE: Biometrics-based Secure Authentication and Key Exchange.《2013 ICB》.2013,全文.

1.一种由网络节点(300)执行的、使得能够基于生物特征数据通过安全通信信道对客户端设备(100)的用户(200)进行认证的方法,包括:

从客户端设备接收(S101)用于对在客户端设备(100)处捕获的用户(200)的生物特征数据进行注册的请求;

从客户端设备(100)接收(S111)以下内容:经转换的生物特征数据,所述生物特征数据已经被转换为不可逆的生物特征数据;包含客户端生成的第一秘密密钥的模糊保险库,使用用户的生物特征数据来锁定所述保险库;客户端生成的第二秘密密钥以及客户端生成的秘密随机数,根据客户端生成的秘密随机数与所述第一秘密密钥组合地生成所述第二秘密密钥;

从客户端设备(100)接收(S201)用于对用户进行认证的请求;

从客户端设备(100)接收(S207)经转换的进一步生物特征数据;

获取(S208)与经转换的进一步生物特征数据匹配的至少一个数据集,所述至少一个数据集包括:客户端生成的秘密随机数、客户端生成的第二秘密密钥、以及包含客户端生成的第一秘密密钥的模糊保险库;

向客户端设备(100)提交(S209)所述至少一个数据集中的所述模糊保险库和所述秘密随机数;以及

从客户端设备(100)接收(S214)客户端设备证明知晓所述第二秘密密钥的指示,在这种情况下,客户端设备能够使用进一步生物特征数据来解锁所述模糊保险库并且能够使用所述第一秘密密钥和所述秘密随机数来创建第二秘密密钥,其中,客户端设备(100)的用户(200)通过认证。

2.根据权利要求1所述的方法,还包括:

向客户端设备(100)提交(S102)使所述客户端设备能够将所述生物特征数据转换为不可逆的生物特征数据的特征转换密钥。

3.根据权利要求2所述的方法,还包括:

从客户端设备(100)接收(S104)所述特征转换密钥未通过随机性测试的指示,其中,终止所述生物特征数据的注册。

4.根据权利要求1至3中任一项所述的方法,其中,通过在伪随机函数中处理(S110)所述第一秘密密钥和所述秘密随机数来生成所述第二秘密密钥。

5.根据权利要求1至3中任一项所述的方法,还包括:

将所接收到的经转换的生物特征数据、模糊保险库、第二秘密密钥和秘密随机数存储(S112)在安全终端用户数据库(400)中。

6.根据权利要求1所述的方法,还包括:

向客户端设备(100)提交(S202)使客户端设备能够将所述进一步生物特征数据转换为不可逆的生物特征数据的特征转换密钥,其中,所接收(S207)到的经转换的进一步生物特征数据已经使用所接收到的特征转换密钥进行了转换。

7.根据权利要求1所述的方法,还包括:

从客户端设备(100)接收(S212)所述秘密随机数未通过随机性测试的指示,其中,终止对客户端设备的用户(200)的认证。

8.根据权利要求6所述的方法,还包括:

从客户端设备(100)接收(S212)所述秘密随机数未通过随机性测试的指示,其中,终止对客户端设备的用户(200)的认证。

9.根据权利要求1和7至8中任一项所述的方法,还包括:

使用所述第二秘密密钥来执行(S215)与客户端设备(100)的相互认证。

10.根据权利要求1和7至8中任一项所述的方法,还包括:

使用传输层安全预共享密钥TLS-PSK协议来执行(S215)与客户端设备(100)的相互认证。

11.根据权利要求1至3中任一项所述的方法,其中,请求认证的客户端设备(100)与请求注册的客户端设备(500)不同。

12.根据权利要求1所述的方法,其中,使用客户端设备与所述网络节点(300)之间的秘密的预先约定的转换在客户端设备(100)处对所述生物特征数据或所述进一步生物特征数据进行转换。

13.一种由客户端设备(100)执行的、使得能够基于生物特征数据通过安全通信信道利用网络节点(300)对客户端设备的用户(200)进行认证的方法,包括:

向所述网络节点(300)提交(S101)用于对在客户端设备(100)处捕获的用户(200)的生物特征数据进行注册的请求;

捕获(S105)用户的生物特征数据;

将所述生物特征数据转换(S106)为不可逆的生物特征数据;

生成(S107)第一秘密密钥;

创建(S108)包含所述第一秘密密钥的模糊保险库,使用用户(200)的生物特征数据来锁定所述保险库;

生成(S109)秘密随机数;

基于所述第一秘密密钥和所述秘密随机数创建(S110)第二秘密密钥;

向所述网络节点(300)提交(S111)经转换的生物特征数据、所述模糊保险库、所述第二秘密密钥和所述秘密随机数;

向所述网络节点(300)提交(S201)用于对用户(200)进行认证的请求;

捕获(S205)用户的进一步生物特征数据;

将所述进一步生物特征数据转换(S206)为不可逆的生物特征数据;

向所述网络节点(300)提交(S207)利用特征转换密钥转换了的进一步生物特征数据;

从所述网络节点(300)接收(S209)至少一个模糊保险库和相关联的秘密随机数;

尝试(S210)使用捕获的进一步生物特征数据来解锁所接收到的至少一个模糊保险库;

基于被成功解锁的至少一个模糊保险库的第一秘密密钥和相关联的秘密随机数创建(S213)第二秘密密钥;以及

向所述网络节点(300)提交(S214)客户端设备(100)证明知晓所述第二秘密密钥的指示,其中,客户端设备的用户(200)通过认证。

14.根据权利要求13所述的方法,还包括:

从所述网络节点(300)接收(S102)特征转换密钥,其中,使用所接收到的特征转换密钥来将所述生物特征数据转换(S106)成不可逆的生物特征数据。

15.根据权利要求14所述的方法,还包括:

对所接收到的特征转换密钥执行(S103)随机性测试；

向所述网络节点(300)提交(S104)所述特征转换密钥未通过随机性测试的指示，其中，终止所述生物特征数据的注册。

16.根据权利要求13至15中任一项所述的方法，其中，通过在伪随机函数中处理所述第一秘密密钥和所述秘密随机数来创建(S110)所述第二秘密密钥。

17.根据权利要求13所述的方法，还包括：

从所述网络节点(300)接收(S202)所述特征转换密钥，其中，使用所接收到的特征转换密钥来将所述进一步生物特征数据转换(S206)成不可逆的生物特征数据。

18.根据权利要求17所述的方法，还包括：

对所接收到的特征转换密钥执行(S203)随机性测试；

向所述网络节点(300)提交(S204)所述特征转换密钥未通过随机性测试的指示，其中，终止对用户(200)的认证。

19.根据权利要求13和17至18中任一项所述的方法，还包括：

对至少一个所接收到的秘密随机数执行(S211)随机性测试；

向所述网络节点(300)提交(S212)所述至少一个所接收到的秘密随机数未通过随机性测试的指示，其中，终止对用户(200)的认证。

20.根据权利要求13和17至18中任一项所述的方法，还包括：

使用所述第二秘密密钥来执行(S215)与所述网络节点(300)的相互认证。

21.根据权利要求13和17至18中任一项所述的方法，还包括：

使用传输层安全预共享密钥TLS-PSK协议来执行(S215)与所述网络节点的相互认证。

22.根据权利要求13所述的方法，其中，使用客户端设备与所述网络节点(300)之间的秘密的预先约定的转换在客户端设备(100)处对所述生物特征数据或所述进一步生物特征数据进行转换。

23.一种被配置成使得能够基于生物特征数据通过安全通信信道对客户端设备(100)的用户(200)进行认证的网络节点(300)，信任的网络节点(300)包括处理单元(301)，所述处理单元(301)被配置成：

从客户端设备接收用于对在客户端设备(100)处捕获的用户(200)的生物特征数据进行注册的请求；

从客户端设备(100)接收以下内容：经转换的生物特征数据，所述生物特征数据已经被转换为不可逆的生物特征数据；包含客户端生成的第一秘密密钥的模糊保险库，使用用户的生物特征数据来锁定所述保险库；客户端生成的第二秘密密钥以及客户端生成的秘密随机数，根据所述客户端生成的秘密随机数与所述第一秘密密钥组合地生成所述第二秘密密钥；

从客户端设备(100)接收用于对用户进行认证的请求；

从客户端设备(100)接收经转换的进一步生物特征数据；

获取与所述经转换的进一步生物特征数据匹配的至少一个数据集，所述至少一个数据集包括：客户端生成的秘密随机数、客户端生成的第二秘密密钥、以及包含客户端生成的第一秘密密钥的模糊保险库；

向客户端设备(100)提交所述至少一个数据集中的所述模糊保险库和所述秘密随机

数;以及

从客户端设备(100)接收客户端设备证明知晓所述第二秘密密钥的指示,在这种情况下,客户端设备能够使用进一步生物特征数据来解锁所述模糊保险库并且能够使用所述第一秘密密钥和所述秘密随机数来创建所述第二秘密密钥,其中,客户端设备(100)的用户(200)通过认证。

24.根据权利要求23所述的网络节点(300),所述处理单元(301)还被配置成:

向客户端设备(100)提交使客户端设备能够将所述生物特征数据转换为不可逆的生物特征数据的特征转换密钥。

25.根据权利要求24所述的网络节点(300),所述处理单元(301)还被配置成:

从客户端设备(100)接收所述特征转换密钥未通过随机性测试的指示,其中,终止所述生物特征数据的注册。

26.根据权利要求23至25中任一项所述的网络节点(300),所述处理单元(301)还被配置成:

将所接收到的经转换的生物特征数据、模糊保险库、第二秘密密钥和秘密随机数存储在安全终端用户数据库(400)中。

27.根据权利要求23所述的网络节点(300),所述处理单元(301)还被配置成:

向客户端设备(100)提交(S202)使客户端设备能够将所述进一步生物特征数据转换为不可逆的生物特征数据的特征转换密钥,其中,所接收到的经转换的进一步生物特征数据已经使用所接收到的特征转换密钥进行了转换。

28.根据权利要求23或27所述的网络节点(300),所述处理单元(301)还被配成:

从客户端设备(100)接收所述秘密随机数未通过随机性测试的指示,其中,终止对客户端设备的用户(200)的认证。

29.根据权利要求23或27所述的网络节点(300),所述处理单元(301)还被配置成:

使用所述第二秘密密钥来执行与客户端设备(100)的相互认证。

30.根据权利要求23或27所述的网络节点(300),所述处理单元(301)还被配置成:

使用传输层安全预共享密钥TLS-PSK协议来执行与客户端设备(100)的相互认证。

31.根据权利要求23至25中任一项所述的网络节点(300),其中,请求认证的客户端设备(100)与请求注册的客户端设备(500)不同。

32.根据权利要求23所述的网络节点(300),其中,使用客户端设备与所述网络节点(300)之间的秘密的预先约定的转换在客户端设备(100)处对所述生物特征数据或所述进一步生物数据进行转换。

33.一种客户端设备(100),所述客户端设备被配置成使得能够基于生物特征数据通过安全通信信道利用网络节点(300)对所述客户端设备的用户(200)进行认证,所述客户端设备包括生物特征数据感测系统(101),所述生物特征数据感测系统(101)包括生物特征数据传感器(102)和处理单元(103),

所述处理单元(103)被配置成:

向所述网络节点(300)提交用于对在所述客户端设备(100)处捕获的用户(200)的生物特征数据进行注册的请求;

所述生物特征数据传感器(102)被配置成:

捕获用户的生物特征数据；

所述处理单元(103)还被配置成：

将所述生物特征数据转换为不可逆的生物特征数据；

生成第一秘密密钥；

创建包含所述第一秘密密钥的模糊保险库，使用用户(200)的生物特征数据来锁定所述保险库；

生成秘密随机数；

基于所述第一秘密密钥和所述秘密随机数创建第二秘密密钥；

向所述网络节点(300)提交经转换的生物特征数据、所述模糊保险库、所述第二秘密密钥和所述秘密随机数；

向所述网络节点(300)提交用于对用户(200)进行认证的请求；

所述生物特征数据传感器(102)还被配置成：

捕获用户的进一步生物特征数据；

所述处理单元(103)还被配置成：

将所述进一步生物特征数据转换为不可逆的生物特征数据；

向所述网络节点(300)提交利用特征转换密钥转换了的进一步生物特征数据；

从所述网络节点(300)接收至少一个模糊保险库和相关联的秘密随机数；

尝试使用所述进一步生物特征数据来解锁所接收到的至少一个模糊保险库；

基于被成功解锁的所述至少一个模糊保险库的第一秘密密钥和相关联的秘密随机数创建第二秘密密钥;以及

向所述网络节点(300)提交(S214)所述客户端设备(100)证明知晓所述第二秘密密钥的指示，其中，所述客户端设备的用户(200)通过认证。

34.根据权利要求33所述的客户端设备(100)，所述处理单元(103)还被配置成：

从所述网络节点(300)接收所述特征转换密钥，其中，使用所接收到的特征转换密钥来将所述生物特征数据转换(S106)为不可逆的生物特征数据。

35.根据权利要求34所述的客户端设备(100)，所述处理单元(103)还被配置成：

对所接收到的特征转换密钥执行随机性测试；

向所述网络节点(300)提交所述特征转换密钥未通过随机性测试的指示，其中，终止所述生物特征数据的注册。

36.根据权利要求33至35中任一项所述的客户端设备(100)，所述处理单元(103)还被配置成通过在伪随机函数中处理所述第一秘密密钥和所述秘密随机数来创建所述第二秘密密钥。

37.根据权利要求33所述的客户端设备(100)，所述处理单元(103)还被配置成：

从所述网络节点(300)接收所述特征转换密钥，其中，使用所接收到的特征转换密钥来将所述进一步生物特征数据转换(S206)成不可逆的生物特征数据。

38.根据权利要求33或37所述的客户端设备(100)，所述处理单元(103)还被配置成：

对所接收到的特征转换密钥执行随机性测试；

向所述网络节点(300)提交所述特征转换密钥未通过随机性测试的指示，其中，终止对用户(200)的认证。

39.根据权利要求33或37所述的客户端设备(100),所述处理单元(103)还被配置成:

对至少一个所接收到的秘密随机数执行随机性测试;

向所述网络节点(300)提交至少一个所接收到的秘密随机数未通过随机性测试的指示,其中,终止对用户(200)的认证。

40.根据权利要求33或37所述的客户端设备(100),所述处理单元(103)还被配置成:

使用所述第二秘密密钥执行与所述网络节点(300)的相互认证。

41.根据权利要求33或37所述的客户端设备(100),所述处理单元(103)还被配置成:

使用传输层安全预共享密钥TLS-PSK协议来执行与所述网络节点的相互认证。

42.根据权利要求33所述的客户端设备(100),其中,使用所述客户端设备与所述网络节点(300)之间的秘密的预先约定的转换在所述客户端设备(100)处对生物特征数据或所述进一步生物数据进行转换。

43.一种计算机可读存储介质,其上存储有计算机程序(107),所述计算机程序(107)包括计算机可执行指令,当所述计算机可执行指令在被包括在生物特征数据感测系统(101)中的处理单元(103)上执行时,所述计算机可执行指令使所述生物特征数据感测系统(101)执行在权利要求13至22中任一项中所述的步骤。

44.一种计算机可读存储介质,其上存储有计算机程序(302),所述计算机程序(302)包括计算机可执行指令,当所述计算机可执行指令在被包括在信任的网络节点(300)中的处理单元(301)上执行时,所述计算机可执行指令使所述信任的网络节点(300)执行在权利要求1至12中任一项中所述的步骤。

基于生物特征的认证的方法、网络节点、客户端设备和存储介质

技术领域

[0001] 本发明涉及能够基于生物特征数据通过安全通信信道对客户端设备的用户进行认证的方法和设备。

背景技术

[0002] 基于生物特征的识别是对人类用户进行安全认证的用户友好的方式。当在分布式系统中出于识别目的使用生物特征数据时，与生物特征数据有关的一个主要问题是：模板生物特征数据必须在应该识别终端用户的计算机系统中的节点处可用。这在分布式计算机系统中构成了主要的安全设计挑战，因为这通常需要将原始的明文生物特征数据存储在中央节点处并分布在系统中。这样的解决方案非常容易受到原始生物特征数据受损的影响，并且在一个系统上受到损害的数据可能导致相同的生物特征数据在使用生物特征数据的所有其他系统上也受到损害的情况。由于在认证期间原始生物特征数据必须在远程位置处可用，因此简单地对生物特征数据进行加密将无法解决该问题。

[0003] 因此，需要提供允许基于生物特征识别进行远程认证但同时提供对原始生物特征数据的保护的解决方案。

发明内容

[0004] 本发明的目的是解决或至少减轻本领域中的这个问题，并且因此提供了一种能够基于生物特征数据通过安全通信信道对客户端设备的用户进行认证的改进的方法。

[0005] 在本发明的第一方面中，该目的通过由网络节点执行的能够通过安全通信信道基于生物特征数据对客户端设备的用户进行认证的方法来实现。该方法包括：从客户端设备接收用于对在客户端设备处捕获的用户的生物特征数据进行注册的请求；以及从客户端设备接收以下内容：经转换的生物特征数据；包含客户端生成的第一秘密密钥的模糊保险库，使用用户的生物特征数据来锁定保险库；客户端生成的第二秘密密钥以及客户端生成的秘密随机数，根据客户端生成的秘密随机数与第一秘密密钥结合地生成第二秘密密钥。

[0006] 在本发明的第二方面中，该目的通过被配置成能够通过安全通信信道基于生物特征数据对客户端设备的用户进行认证的网络节点来实现，信任的网络节点包括处理单元，处理单元被配置成：从客户端设备接收用于对在客户端设备处捕获的用户的生物特征数据进行注册的请求；以及从客户端设备接收以下内容：经转换的生物特征数据；包含客户端生成的第一秘密密钥的模糊保险库，使用用户的生物特征数据来锁定所述保险库；客户端生成的第二秘密密钥以及客户端生成的秘密随机数，根据客户端生成的秘密随机数与第一秘密密钥结合地生成第二秘密密钥。

[0007] 在本发明的第三方面中，该目的通过由客户端设备执行的能够通过安全通信信道利用网络节点基于生物特征数据对客户端设备的用户进行认证的方法来实现。该方法包括向网络节点提交用于对在客户端设备处捕获的用户的生物特征数据进行注册的请求；捕获

用户的生物特征数据;将生物特征数据转换为不可逆的生物特征数据;生成第一秘密密钥;以及创建包含第一秘密密钥的模糊保险库,使用用户的生物特征数据来锁定所述保险库。该方法还包括:生成秘密随机数;基于第一秘密密钥和秘密随机数创建第二秘密密钥;以及向网络节点提交经转换的生物特征数据、模糊保险库、第二秘密密钥和秘密随机数。

[0008] 在本发明的第四方面中,该目的通过被配置成能够通过安全通信信道利用网络节点基于生物特征数据对客户端设备的用户进行认证的客户端设备来实现,该客户端设备包括生物特征数据感测系统,该生物特征数据感测系统包括生物特征数据传感器和处理单元。处理单元被配置成:向网络节点提交用于对在客户端设备处捕获的用户的生物特征数据进行注册的请求。生物特征数据传感器被配置成捕获用户的生物特征数据。处理单元还被配置成:将生物特征数据转换为不可逆生物特征数据;生成第一秘密密钥;创建包含第一秘密密钥的模糊保险库,使用用户的生物特征数据来锁定保险库;生成秘密随机数;基于第一秘密密钥和秘密随机数创建第二秘密密钥;以及向网络节点提交经转换的生物特征数据、模糊保险库、第二秘密密钥和秘密随机数。

[0009] 在实现方式中,用户可以订阅由远程服务器提供的服务,例如,电子商务服务,其中,用户使用指纹数据替代个人识别码(PIN)来对她自己进行认证,例如,以实现对经由电子商务服务购买的货物的支付。最初,用户将必须通过安全信道利用远程服务器执行注册过程。

[0010] 在实施方式中,客户端设备通过安全信道(例如,经由因特网)向远程服务器300提交请求,远程服务器通过发送特征转换密钥来对该请求进行回复,特征转换密钥将由客户端设备使用以使用合适的特征转换方案将捕获的生物特征数据转换为经转换的生物特征数据集。

[0011] 所使用的转换方案应该产生经转换的生物特征数据,该经转换的生物特征数据为不可逆的,即,对于攻击者而言,即使在取得特征转换密钥和经转换的生物特征数据两者的情况下,也应该无法重建原始生物特征数据。

[0012] 在可替代实施方式中,设想客户端设备和远程服务器利用秘密的预先约定的转换来执行捕获的生物特征数据的转换,从而产生经转换的生物特征数据。在这样的实施方式中,将不需要特征转换密钥,因此在该替代实施方式中远程服务器不会将特征转换密钥发送到客户端设备。相反,客户端设备将使用共享转换(该共享转换在客户端设备与远程服务器之间保密) 来转换生物特征数据。

[0013] 然而,在下文中,将讨论使用特征转换密钥的实施方式。

[0014] 客户端设备使用生物特征数据并应用适当的模糊保险库方案来生成包含在所谓的模糊保险库V中的第一秘密密钥。模糊保险库是加密结构,在该加密结构中,可以通过使用数据A的集合(在该特定发明中是生物特征数据集)来锁定秘密,并且模糊保险库只有在集合B类似于集合A时仅能由数据B的集解锁。

[0015] 此外,客户端设备生成随机数并且例如通过利用伪随机函数使用第一秘密密钥和秘密随机数来创建第二秘密密钥。

[0016] 然后,客户端设备将包括模糊保险库、经转换的生物特征数据、第二秘密密钥和秘密随机数的注册集连同任何用户数据(例如,用户的邮寄地址)一起通过安全信道提交至远程服务器。

[0017] 远程服务器将接收到的数据存储在位于远程服务器本地处或远离远程服务器的终端用户数据库中。

[0018] 有利地，通过使用模糊保险库，在不必将生物特征数据以明文形式存储在用户的信任客户端设备之外的情况下方便了用户的注册。

[0019] 在实施方式中，当用户希望利用远程服务器对她自己进行认证，以用于在进行注册过程的客户端设备上或者另一第二客户端设备上访问所提供的她已经注册的服务时，第二客户端设备将通过安全通道向远程服务器提交认证请求。

[0020] 同样，远程服务器将通过发送特征转换密钥来进行回复，该特征转换密钥由第二客户端设备使用以对在第二客户端设备处捕获的生物特征数据进行转换。可替选地，使用在注册客户端设备与远程服务器之间共享的秘密转换来转换生物特征数据，因此该秘密转换还必须与期望利用远程服务器00执行认证的任何其他客户端设备共享。

[0021] 因此，第二客户端设备使用特征转换密钥来对捕获的生物特征数据进行转换，从而产生经转换的生物特征数据，并且将经转换的生物特征数据提交至远程服务器，该远程服务器使用经转换的生物特征数据从终端用户数据库中取出一个或更多个匹配注册集。

[0022] 远程服务器从(一个或更多个)取出的注册集中推导出(一个或更多个)包括模糊保险库和随机数的候选集，并将推导出的候选集发送至第二客户端设备。

[0023] 现在，如果在第二设备处捕获的生物特征数据与最初由注册客户端设备捕获的并且在注册阶段期间所使用的生物特征数据匹配，则第二客户端设备将能够解锁模糊保险库并获取第一秘密密钥。

[0024] 然后，将所获取的第一秘密密钥与所接收到的秘密随机数一起使用，以生成第二秘密密钥K2。

[0025] 通过证明知晓先前注册的第二秘密密钥，最终第二客户端设备的用户将在远程服务器处通过认证。

[0026] 这可以通过与远程服务器进行相互认证处理来执行。例如，可以利用传输层安全预共享密钥(TLS-PSK)加密协议，其基于在通信方(在这种情况下是远程服务器与第二客户端设备)之间预先共享的对称密钥。

[0027] 有利地，利用本发明的该实施方式，在生物特征数据不以明文形式对远程服务器可用的情况下，用户通过远程服务器进行认证。

[0028] 将在详细描述中阐述本发明的其他实施方式。

[0029] 通常，除非本文另有明确定义，否则权利要求书中使用的所有术语将根据其在技术领域中的普通含义进行解释。除非另外明确说明，否则对“元件、装置、部件、手段、步骤等”的所有引用将被开放地解释为指代元件、装置、部件、手段、步骤等的至少一个实例。除非明确说明，本文公开的任何方法的步骤不必按所公开的确切顺序执行。

附图说明

[0030] 现在参考附图以举例的方式描述本发明，在附图中：

[0031] 图1示出了可以实现本发明的智能电话形式的电子设备；

[0032] 图2示出了用户将她的手指放在上面的指纹传感器的图；

[0033] 图3示出了作为根据实施方式的指纹感测系统的一部分的指纹传感器；

[0034] 图4示出了能够基于生物特征数据通过安全通信信道对客户端设备的用户进行认证的实施方式。

[0035] 图5示出了利用远程服务器执行用户的生物特征数据的注册的实施方式；

[0036] 图6示出了在远程服务器处的客户端设备的用户的认证的实施方式。

具体实施方式

[0037] 现在将参照附图在下文中更全面地地描述本发明，在附图中示出了本发明的某些实施方式。然而，本发明可以以许多不同的形式实施，而不应被解释为限于本文阐述的实施方式；更确切地，这些实施方式是通过示例的方式提供的，使得本公开内容将是全面和完整的，并且向本领域的技术人员充分传达本发明的范围。在整个说明书中，相同的附图标记指代相同的元件。

[0038] 图1示出了可以实现本发明的智能电话形式的客户端设备100。智能电话100配备有指纹传感器102和具有触摸屏界面106的显示单元104。例如，指纹传感器102可以用于解锁移动电话100和/或用于授权使用移动电话100执行的交易等。可替代地，指纹传感器102可以放置在移动电话 100的背面上。注意的是，指纹传感器102可以集成在显示单元/触摸屏中或形成为智能电话主页按钮的一部分。

[0039] 应当理解的是，根据本发明的实施方式的指纹传感器102可以在其他类型的电子设备(例如，膝上型电脑、遥控器、平板电脑、智能卡等)或者利用指纹感测的任何其他类型的现有的或将来的类似配置设备中实现。

[0040] 图2示出了用户将她的手指201放在上面的的指纹传感器102的略微放大图。在采用电容感测技术的情况下，指纹传感器102被配置成包括多个感测元件。在图2中，单个感测元件(也表示为像素)由附图标记202 表示。

[0041] 图3示出了作为指纹感测系统101的一部分的指纹传感器102。指纹感测系统101包括：指纹传感器102；以及用于控制指纹传感器102并用于分析捕获的指纹的处理单元103，例如，微处理器。指纹感测系统101 还包括存储器105。如图1中所例示的，指纹感测系统101又通常形成为电子设备100的一部分。

[0042] 现在，当对象接触指纹传感器102时，传感器102将捕获对象的图像，以使处理单元103通过将捕获的指纹与预先存储在存储器105中的一个或更多个经授权的指纹模板进行比较来确定该对象是否为经授权的用户的指纹。

[0043] 指纹传感器102可以使用包括例如电容、光学、超声或热感测技术的任何种类的当前或未来的指纹感测原理来实现。目前，电容式感测是最常用的，特别是在尺寸和功耗很重要的应用中。电容式指纹传感器提供在若干感测元件202与放置在指纹传感器102的表面上的手指201之间(参见图2)的电容的指示性测量。指纹图像的获取通常使用包括以二维方式布置的多个感测元件202的指纹传感器102来执行。

[0044] 在一般授权处理中，用户将她的手指201放置在传感器102上，用于使传感器捕获用户的指纹的图像。处理单元103评估所捕获的指纹并且将所捕获的指纹与存储在存储器105中的一个或更多个经认证的指纹模板进行比较。如果记录的指纹与预先存储的模板匹配，则用户通过认证并且处理单元103通常将指示智能电话100执行适当的动作，例如，从锁定模式转换到解锁模式，在解锁模式下，允许用户访问智能电话100。

[0045] 再次参照图3,由指纹感测系统101执行的方法的步骤(除了由传感器102执行的捕获图像之外)实际上由以一个或更多个微处理器形式实现的处理单元103执行,所述一个或更多个微处理器被布置成执行下载到与微处理器相关联的存储介质105(例如,随机存取存储器(RAM)、闪存或硬盘驱动器)的计算机程序107。处理单元103被布置成:当包括计算机可执行指令的合适的计算机程序107被下载到存储介质105并且由处理单元103执行时,使指纹感测系统101执行根据实施方式的方法。存储介质 105也可以是包括计算机程序107的计算机程序产品。可替选地,可以借助于合适的计算机程序产品(例如,数字多功能盘(DVD)或记忆棒)将计算机程序107传送到存储介质105。作为另一可替选方案,可以通过网络将计算机程序107下载到存储介质105。可替选地,处理单元103可以实现为数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、复杂可编程逻辑器件(CPLD)等形式。还应当理解的是,借助于处理单元103提供的功能的全部或部分可以至少部分地与指纹传感器102集成。

[0046] 图4示出了能够基于生物特征数据通过安全通信信道对客户端设备的用户进行认证的实施方式。

[0047] 因此,例如,客户端设备100以参照图1至图3描述的方式获取用户 200的生物特征数据T。

[0048] 例如,假设用户200订阅由远程服务器300提供的服务,例如,电子商务服务,其中,用户200使用指纹数据而不是个人识别码(PIN)来对她自己进行认证,以实现对经由电子商务服务购买的商品的支付。最初,用户200必须通过安全信道利用远程服务器300来执行注册过程。

[0049] 在实施方式中,在步骤S101中,客户端设备100通过安全信道(例如,经由因特网)向远程服务器300提交请求,在步骤S102中,远程服务器 300通过发送特征转换密钥R来进行回复,该特征转换密钥R将由客户端设备100使用以使用合适的特征转换方案将捕获的生物特征数据T转换为经转换的生物特征数据集TP。所使用的转换方案应该产生经转换的生物特征数据TP,该经转换的生物特征数据TP是不可逆的,即对于攻击者而言,即使在取得特征转换密钥R和经转换的生物特征数据TP两者的情况下,也应该无法重建原始生物特征数据T。

[0050] 在可替代实施方式中,设想客户端设备100和远程服务器300利用秘密的预先约定的转换来执行捕获的生物特征数据T的转换,从而产生经转换的生物特征数据TP。在这样的实施方式中,将不需要特征转换密钥R。然而,在下文中,将说明使用特征转换密钥R的实施方式。

[0051] 客户端设备100使用生物特征数据并应用模糊保险库方案(例如,在 D.Juels和M.Sudan的,“Afuzzy vault scheme”,Des.Codes Cryptography, Vol.38,No.2,pp.237-257,2006中提出的方案)来生成包含在所谓的模糊保险库V中的第一秘密密钥K_1。

[0052] 模糊保险库是加密结构,在该加密结构中,可以通过使用数据A的集合(在该特定发明中是生物特征数据集)来锁定秘密,并且模糊保险库只有在集合B类似于集合A时仅能由数据B的集合解锁。

[0053] 模糊保险库将被表示为$V=U(T,K_1)$,意味着模糊保险库V是通过使用生物特征数据T作为锁定保险库的数据集借助于模糊保险库方案U将 K_1锁定到保险库中而创建的。

[0054] 此外，客户端设备100生成随机数N并且使用第一秘密密钥K_1和秘密随机数N来创建第二秘密密钥K_2，例如，通过使用被表示为K_2＝PRF (K_1,N)的伪随机函数。

[0055] 然后，在步骤S111中，客户端设备100将模糊保险库V、经转换的生物特征数据TP、第二秘密密钥K_2和秘密随机数N连同任何用户数据(诸如，例如用户的帐单地址)通过安全信道一起提交至远程服务器300。在下面，数据集{TP,V,K_2,N}将被称为注册集。

[0056] 在步骤S112中，远程服务器300将在步骤S111中接收的数据存储在位于远程服务器300的本地处或远离远程服务器300的终端用户数据库400 中。

[0057] 有利地，通过使用模糊保险库V，生物特征数据不以明文形式存储在用户信任的客户端设备100之外。

[0058] 现在，当用户200希望利用远程服务器300对她自己进行认证，以用于在进行过注册过程的客户端设备100或者第二客户端设备500上访问所提供的她已经注册的服务时，在步骤S201中，第二客户端设备500将通过安全信道向远程服务器300提交针对认证的请求。

[0059] 同样，在步骤S202中，远程服务器300将通过发送特征转换密钥R 来进行回复，该特征转换密钥R由第二客户端设备500使用以对在第二客户端设备500处捕获的生物特征数据T’进行转换。

[0060] 可替选地，使用在客户端设备100与远程服务器300之间共享的秘密转换来转换生物特征数据T’，因此该秘密转换还必须与期望利用远程服务器300执行认证的任何其他客户端设备共享。

[0061] 因此，第二客户端设备500使用特征转换密钥R来对捕获的生物特征数据T’进行转换，从而产生经转换的生物特征数据TP’，并且在步骤S207 中将经转换的生物特征数据TP’提交至使用经转换的生物特征数据TP’的远程服务器300，以在步骤S208中从终端用户数据库400中取出一个或更多个匹配注册集。

[0062] 远程服务器300从(一个或更多个)取出的注册集{TP,V,K_2,N} 中推导出(一个或更多个)候选集{V,N}，并且在步骤S209中将推导出的候选集{V,N}发送至第二客户端设备500。

[0063] 现在，如果在第二设备处捕获的生物特征数据与最初由客户端设备100 捕获的并且在注册阶段期间所使用的生物特征数据匹配，则第二客户端设备500将能够解锁模糊保险库V并获取第一秘密密钥K_1。

[0064] 然后，将所获取的第一秘密密钥K_1与所接收到的秘密随机数N一起使用，以生成第二秘密密钥K_2:K_2＝PRF(K_1,N)。

[0065] 在步骤S214中，通过证明知晓先前注册的第二秘密密钥K_2，最终第二客户端设备500的用户将在远程服务器300处通过认证。这可以通过与远程服务器300进行相互认证处理来执行。例如，使用对称的第二秘密密钥K_2，可以针对两个操作在一面对共享秘密(例如，N)进行加密并且在另一面对共享秘密(例如，N)进行解密。如果解密成功，则加密方也被认为成功通过认证。

[0066] 甚至更优选的是使用基于在通信方(在这种情况下是远程服务器300 和第二客户端设备500)之间预先共享的对称密钥的传输层安全预共享密钥(TLS-PSK)加密协议。

[0067] 有利地，利用参照图4所示的本发明的实施方式，在生物特征数据本身不以明文形式提供给远程服务器300情况下，用户200通过远程服务器 300进行认证。

[0068] 参照图4,由远程服务器300执行的方法的步骤实际上由以一个或更多个微处理器的形式实现的处理单元301执行,一个或更多个微处理器被布置成执行下载至与微处理器相关联的存储介质303(例如,随机存取存储器(RAM)、闪存或硬盘驱动器)的计算机程序302。处理单元301被布置成当包括计算机可执行指令的合适的计算机程序302被下载到存储介质 303并且由处理单元301执行时使远程服务器300执行根据实施方式的方法。存储介质303还可以是包括计算机程序302的计算机程序产品。可替选地,可以借助于合适的计算机程序产品(例如,数字多功能盘(DVD) 或记忆棒)将计算机程序302传送到存储介质303。作为另一可替选方案,可以通过网络将计算机程序302下载到存储介质303。可替选地,处理单元301可以实现为数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、复杂可编程逻辑器件(CPLD)等形式。

[0069] 图5示出了利用远程服务器300执行用户的生物特征数据的注册以便随后能够例如借助于如先前参照图1至图3所讨论的指纹感测经由捕获用户的生物特征数据的客户端设备认证用户的更详细的实施方式。

[0070] 因此,在客户端设备100与远程服务器300之间建立安全通信信道,即,在保密性和完整性方面受到保护的通信信道。

[0071] 在步骤S101中,客户端设备100代表客户端设备100的用户200发出用于向由远程服务器300处理认证的远程系统所提供的服务注册用户200 的请求。

[0072] 对该请求进行回复,在步骤S102中,远程服务器300提交能够使客户端设备100将生物特征数据转换为不可逆的生物特征数据的特征转换密钥 R。密钥R可以根据生成的随机数创建。使用特征转换密钥R对由系统中的远程服务器300处理的所有用户的生物特征数据进行转换。

[0073] 在实施方式中,在步骤S103中,客户端设备100(使用任何适当的统计分析算法)对所接收到的特征转换密钥R执行随机性测试,并且如果密钥未通过随机性测试,即,如果密钥不呈现真的随机特性,客户端设备100 则在步骤S104中向远程服务器300指示错误消息,在这种情况下,注册处理由客户端设备100或远程服务器300终止。有利地,可以避免恶意远程服务器发送不具有随机特性的特征转换密钥让所使用的转换更容易攻击的情况。

[0074] 同样,在替代实施方式中,设想客户端设备100和远程服务器300利用秘密的预先约定的转换来执行捕获的生物特征数据T的转换。在这样的实施方式中,将不需要特征转换密钥R。

[0075] 在该特定示例实施方式中,假设在步骤S103中特征转换密钥R通过了随机性测试,因此,在步骤S105中客户端设备100例如借助于利用指纹感测继续捕获用户的生物特征数据T,即使在进行注册请求之前也可以执行生物特征数据T的捕获。

[0076] 在步骤S106中,客户端设备100使用所接收到的特征转换密钥R来执行生物特征数据T的不可逆转换F(T,R),从而产生不可逆的经转换的生物特征数据TP,即TP＝F(T,R)。应当理解的是,要使用的转换函数F是系统定义的。可替选地,步骤S106中使用秘密的预先约定的转换在客户端设备100处转换生物特征数据T。

[0077] 可以设想许多不同的转换函数F,例如,笛卡尔、极坐标或函数变换,或者基于近似消息认证码(MAC)方案建立的不可逆变换函数。

[0078] 在步骤S107中,客户端设备100使用例如随机数发生器继续生成第一秘密密钥K_1,

并且在步骤S108中进一步生成所谓的模糊保险库V:V＝U (T,K_1),该保险库V包含第一秘密K_1并且由用户200的生物特征数据T 锁定。特别地,函数U可以由概率确定性算法确定。

[0079] 此外,在步骤S109中,客户端设备100生成随机数N,并且在步骤 S110中通过在伪随机函数K_2＝PRF(K_1,N)中处理第一秘密密钥K_1和随机数N来计算第二秘密密钥K_2。

[0080] 最后,在步骤S111中,客户端设备100通过建立的安全信道将注册集 {TP,V,K2,N}连同任何适当的用户数据(例如,用户的帐单地址、个人资料信息、信用卡信息等)一起提交至远程服务器300。

[0081] 在步骤S112中,远程服务器300将所接收到的注册集存储在安全终端用户数据库400中。

[0082] 图6示出了基于生物特征数据使用远程服务器300执行用户200的认证,以便例如允许用户200经由如参照图5所讨论的执行注册的客户端设备100或者通过不同客户端设备(例如,第二客户端设备500)使用由远程服务器300提供的电子商务服务进行购买的更详细的实施方式。

[0083] 同样,在客户端设备100与远程服务器300之间建立安全通信信道,即,在保密性和完整性方面受到保护的通信信道。

[0084] 在步骤S201中,客户端设备100代表客户端设备100的用户200发出用于在处理对由系统提供的服务进行认证的远程服务器300处对用户200 进行认证的请求。

[0085] 对该请求进行回复,在步骤S202中,远程服务器300提交能够使客户端设备100将生物特征数据转换为不可逆的生物特征数据的特征转换密钥 R。密钥R可以根据生成的随机数创建。使用特征转换密钥R对由系统中的远程服务器300处理的所有用户的生物特征数据进行转换。可替选地,使用不需要特征转换密钥R的秘密的预先约定的转换在客户端设备100处对生物特征数据进行转换。

[0086] 在实施方式中,如前面所描述的,在步骤S203中,客户端设备100(使用任何适当的统计分析算法)对所接收到的特征转换密钥R执行随机性测试,并且如果密钥未通过随机性测试,即,如果密钥不呈现真的随机特性,则在步骤S204中客户端设备100向远程服务器300指示错误消息,在这种情况下,注册处理由客户端设备100或远程服务器300终止。有利地,可以避免恶意远程服务器发送不具有随机特性的特征转换密钥让所使用的转换更容易攻击的情况。

[0087] 在该特定示例实施方式中,假设在步骤S203中特征转换密钥R通过随机性测试,因此在步骤S205中客户端设备100例如借助于利用指纹感测继续捕获用户的生物特征数据T',即使在进行认证请求之前也可以执行生物特征数据T'的捕获。

[0088] 如前面所提到的,在替代实施方式中,在不需要特征转换密钥R的情况下,利用秘密的预先约定的转换来执行转换。

[0089] 在步骤S206中,客户端设备100使用所接收到的特征转换密钥R来执行生物特征数据T'的不可逆转换F(T',R),从而产生不可逆的经转换的生物特征数据TP',即,TP＝F(T',R)。应当理解的是,要使用的转换函数F是系统定义的。

[0090] 同样,可以设想许多不同的转换函数F,例如,笛卡尔、极坐标或函数变换,或基于近似MAC方案建立的不可逆变换函数。

[0091] 在步骤207中,客户端设备100将经转换的生物特征数据TP'提交至使用经转换的

生物特征数据TP'的远程服务器300,以在步骤S208中从终端用户数据库400中取出一个或更多个匹配注册集{TP,V,K_2,N},其中 TP'与TP匹配。

[0092] 远程服务器300使用合适的匹配算法来在终端用户数据库中搜索与所接收到的经转换的生物特征数据集TP'匹配的存储的经转换的生物特征数据集。例如,这可以是基于哈希树(hash tree)的搜索,其结合距离匹配度量函数(例如,基于汉明距离的度量或基于欧几里德(Euclidian)的度量)。所使用的确切匹配函数将取决于系统中使用的所选的特定特征转换。

[0093] 远程服务器300推导出一个或更多个匹配候选集{V,N}=({V_0,N_0}, {V_1,N_1},...,(V_{k-1},N_{k-1})}并且在步骤S209中将推导出的候选集发送至客户端设备100。

[0094] 在步骤S210中,客户端设备100将尝试使用捕获的生特征数据T'来打开模糊保险库V_0,V_1,V_{k-1}中的每一个。在该示例中,假设客户端设备 100成功打开模糊保险库V_i,并且使用索引i访问包含在保险库中的第一秘密密钥。即,K_{1i}=UI(T',V_i),其中UI表示与注册阶段的保险库锁定函数U对应的保险库打开函数。

[0095] 在实施方式中,如先前针对特征转换密钥R进行的,在步骤S211中,客户端设备100(使用任何适当的统计分析算法)对所接收到的随机数N_i执行随机性测试,并且如果密钥未通过随机性测试,即,如果密钥不呈现真的随机特性,则在步骤S212中向远程服务器300指示错误消息,在这种情况下,认证处理由客户端设备100或远程服务器300终止。有利地,可以避免恶意远程服务器发送不具有随机特性的特征转换密钥让所使用的转换更容易攻击的情况。

[0096] 在该特定示例实施方式中,假设在步骤S211中随机数N_i通过随机性测试。

[0097] 现在,由于在客户端设备100处捕获的生物特征数据T'与最初由客户端设备100捕获的并且在注册阶段期间使用远程服务器300注册的生物特征数据T'匹配,因此客户端设备100能够解锁模糊保险库V_i并获取第一秘密密钥K_{1i}。

[0098] 然后,在步骤S213中将所获取的第一秘密密钥K_{1i}与所接收到的秘密随机数N_i一起使用,以生成第二秘密密钥K_{2i}:K_{2i}=PRF(K_{1i},N_i)。

[0099] 在步骤S214中,通过证明知晓先前注册的第二秘密密钥K_2,最终客户端设备100的用户将在远程服务器300处通过认证。这可以通过提交索引i来执行,从而向远程服务器300指示与包含在未解锁的保险库V_i中的第一秘密密钥K_{1i}对应的第二秘密密钥K_{2i}。

[0100] 在实施方式中,在步骤S215中,这可以使用例如预共享密钥传输层安全(TLS)通过进行相互认证处理的客户端设备100和远程服务器300来进一步加强,由此客户端设备100的用户200通过远程服务器300进行认证。

[0101] 本发明可以用于用户想要登录服务的大量远程生物特征识别使用的情况中。有利地,利用本发明的解决方案,使用生物特征信息,用户200不仅被识别而且还使用利用模糊保险库方案的生物特征数据加密系统对用户 200进行认证。这意味着用户可以通过向支持远程认证过程的任意(信任的)设备呈现她的生物特征信息来登录到提供根据本发明的登录过程的远程Web服务。因此,对于用户来说,不需要记住任何用户名和/或密码或没有携带某个硬件令牌的任何需求,或者不需要具有存储在客户端设备上的用于登录的特殊目的识别程序或凭证。此外,在实施方式中,在远程服务器300与客户端设备100之间应用相互认证,即,相互认证还可以用于对于客户端设备来说确保客户端设备连接至正确的服务器是

很重要的应用。

[0102] 有利地，明文生物特征数据不存储在远程服务器处，这可以显著地增加在使用系统中的用户信任。

[0103] 上面主要参照一些实施方式描述了本发明。然而，如本领域的技术人员容易理解的，除了上面公开的实施方式以外的其他实施方式同样可以在如所附的专利的权利要求书限定的本发明的范围内。

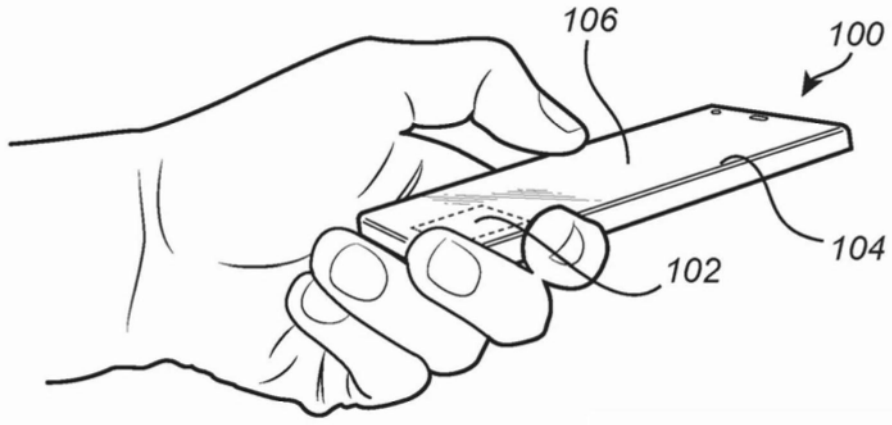


图1

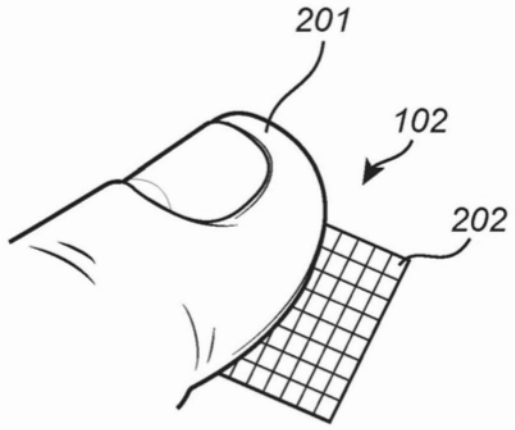


图2

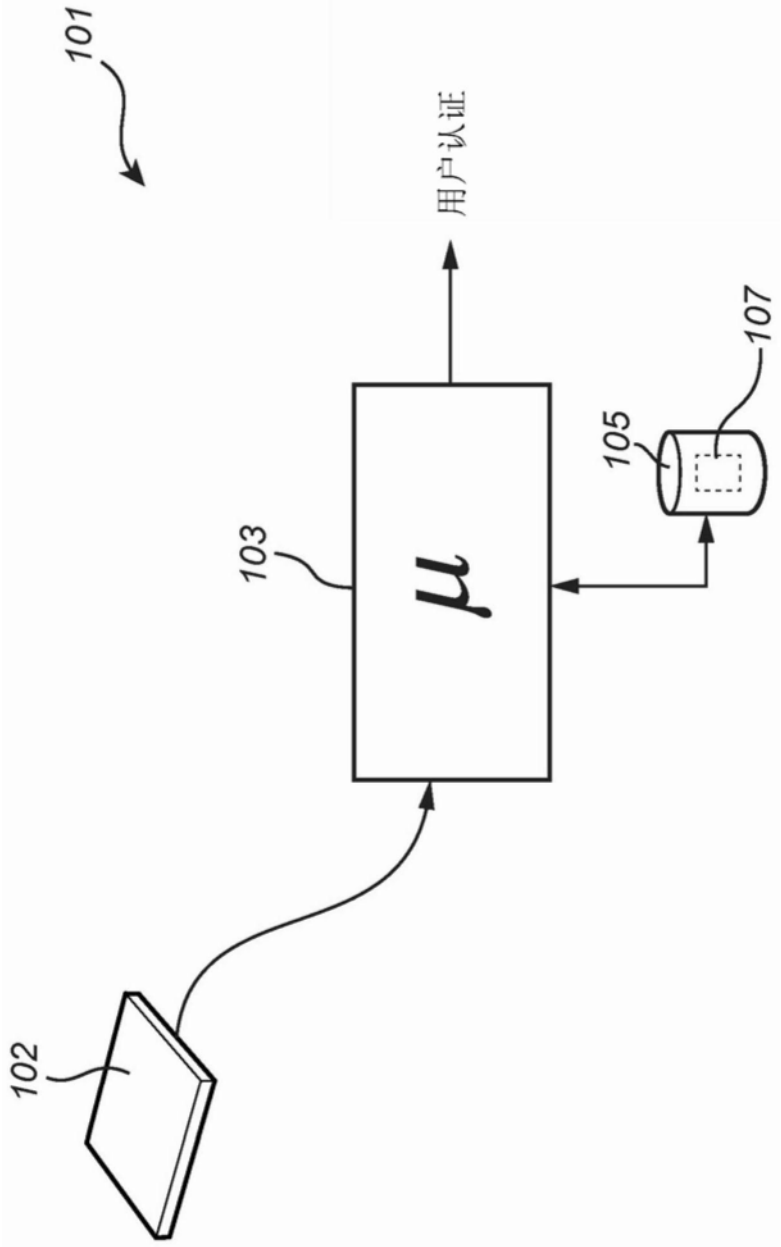


图3

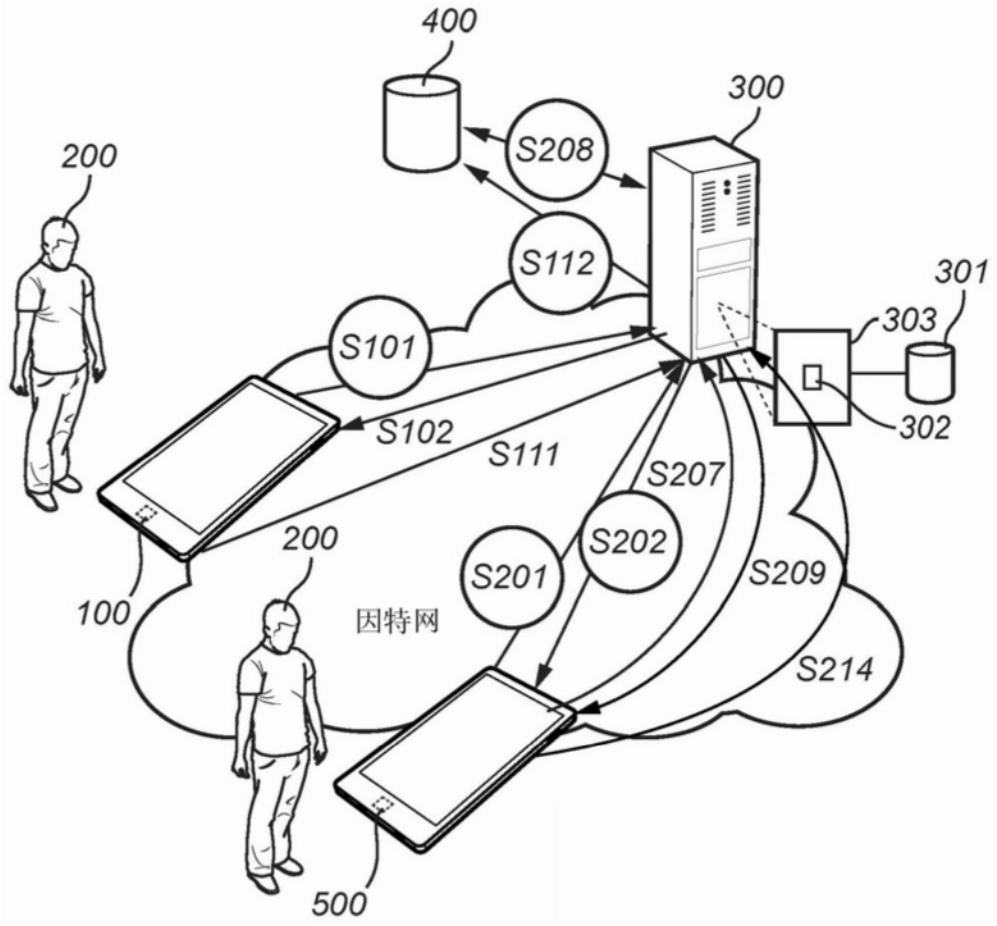

400
300
200
S208
S112
301
303
S101
S102
S111
S207
302
200
S202
S201
S209
100
因特网
S214
500

图4

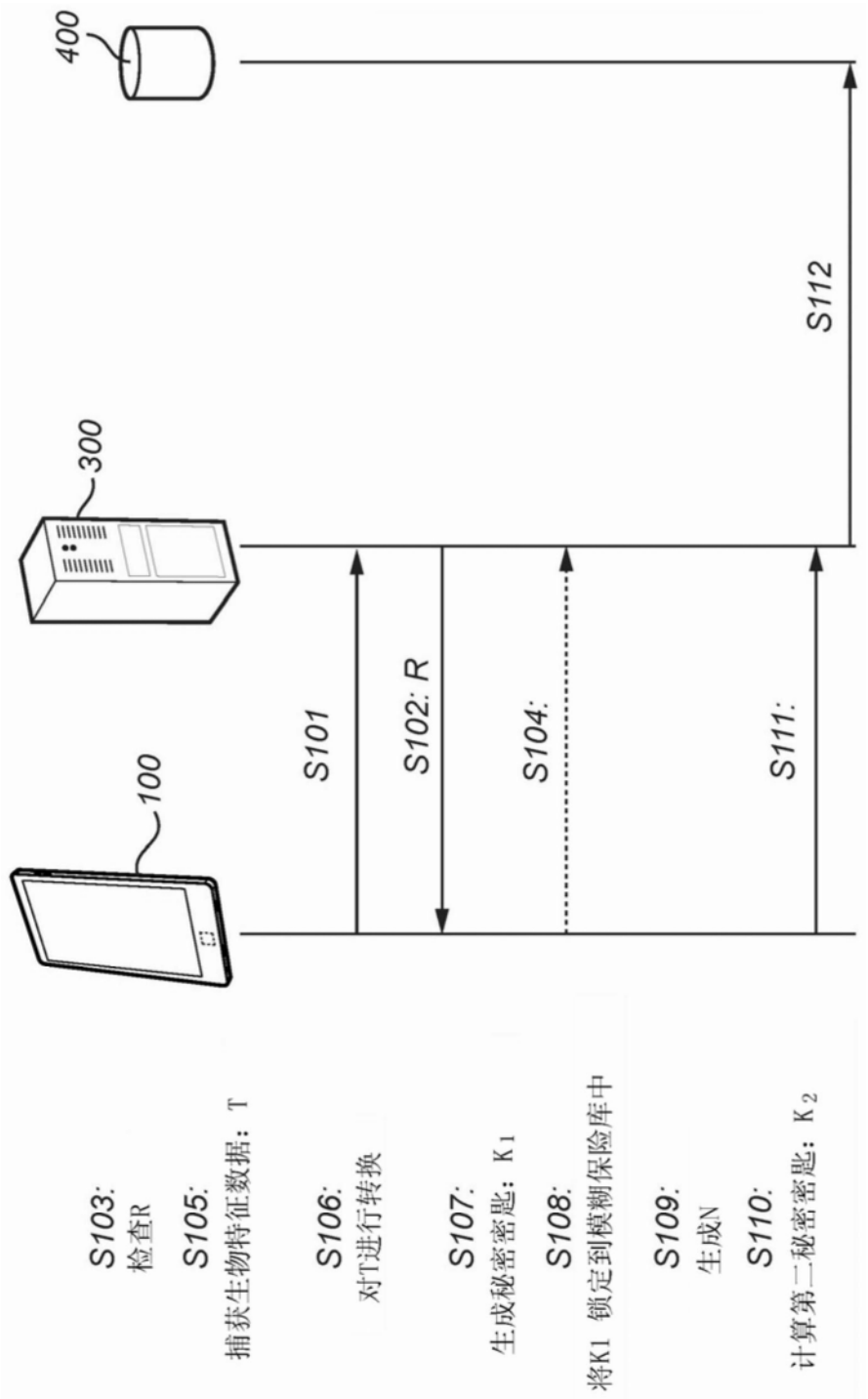

400
300
100
S101
S102: R
S104:
S111:
S112
S103:
检查R
S105:
捕获生物特征数据：T
S106:
对T进行转换
S107:
生成秘密密匙：K1
S108:
将K1 锁定到模糊保险库中
S109:
生成N
S110:
计算第二秘密密匙：K2

图5

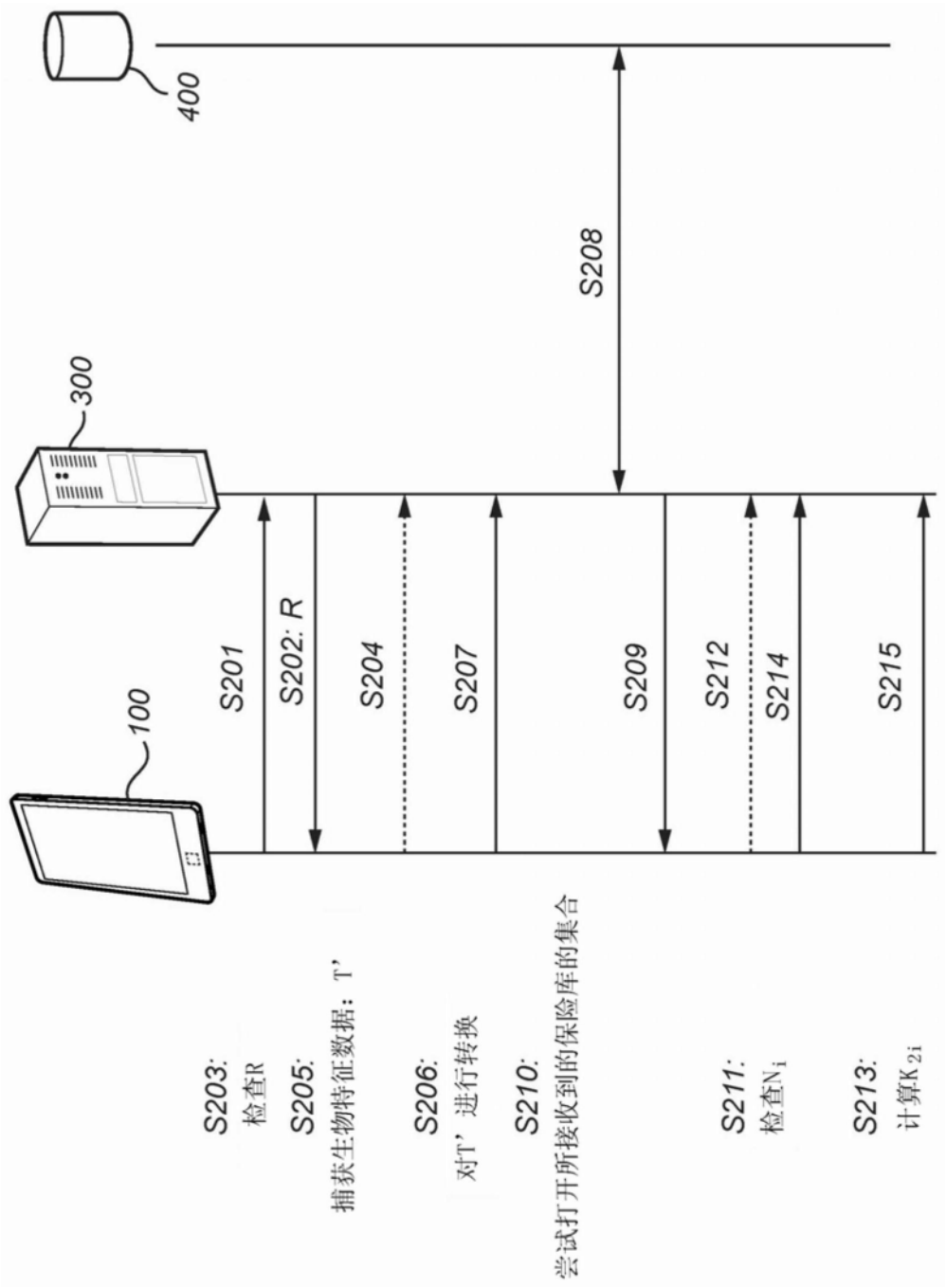

400
300
100
S208
S201
S202: R
S204
S207
S209
S212
S214
S215
S203:
检查R
S205:
捕获生物特征数据：T’
S206:
对T’进行转换
S210:
尝试打开所接收到的保险库的集合
S211:
检查N_i
S213:
计算K_{2i}

图6