



(12)发明专利

(10)授权公告号 CN 107209821 B

(45)授权公告日 2018.08.14

(21)申请号 201580056462.8

专利权人 乔鲍·伦杰尔 安塔尔·罗根

(22)申请日 2015.06.15

(72)发明人 巴拉兹·奇克 乔鲍·伦杰尔
安塔尔·罗根

(65)同一申请的已公布的文献号
申请公布号 CN 107209821 A

(74)专利代理机构 北京超凡志成知识产权代理
事务所(普通合伙) 11371

(43)申请公布日 2017.09.26

代理人 杨勇 董江虹

(30)优先权数据

P1400392 2014.08.18 HU

P1500259 2015.05.29 HU

(51)Int.Cl.

G06F 21/32(2013.01)

G06F 21/62(2013.01)

G06F 21/64(2013.01)

(85)PCT国际申请进入国家阶段日
2017.04.17

(86)PCT国际申请的申请数据

PCT/HU2015/000055 2015.06.15

(87)PCT国际申请的公布数据

W02016/027111 EN 2016.02.25

(56)对比文件

WO 0108352 A1,2001.02.01,

US 2011126024 A1,2011.05.26,

CN 103888442 A,2014.06.25,

CN 1419664 A,2003.05.21,

(73)专利权人 巴拉兹·奇克
地址 匈牙利布达佩斯

审查员 王平

权利要求书6页 说明书12页 附图8页

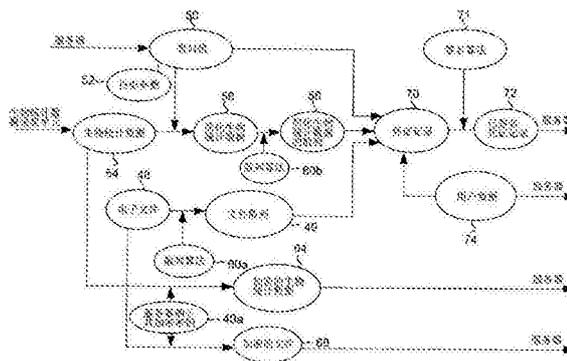
(54)发明名称

用于对电子文件进行数字签名的方法以及
认证方法

方法。

(57)摘要

本发明是一种用于对电子文件(48)进行数字签名的方法,包括通过服务器执行以下步骤:-生成包括投影参数(52)的查询值(50);-通过通信信道将查询值(50)传送到客户端设备;-通过通信信道从客户端设备接收凭证记录(70)、待签名的电子文件(48)以及用户的生物统计数据(54);-通过应用利用投影参数(52)的投影来生成简化生物统计验证数据;-生成验证凭证记录并将其与客户端设备发送的凭证记录(70)比较;-生成服务器证书;-应用服务器的私有签名密钥对服务器证书进行签名,由此生成已签名服务器证书;-通过将至少已签名服务器证书与电子文件(48)的散列(49)相关联来生成数字签名;以及将数字签名与电子文件(48)相关联,由此生成已数字签名的电子文件。本发明还是一种认证



CN 107209821 B

1. 一种用于对电子文件进行数字签名的方法,其特征在于,通过服务器执行以下步骤:
 - 生成包括投影参数(52)的查问值(50),
 - 通过通信信道(30)将所述查问值(50)传送到客户端设备(10),
 - 通过通信信道(30)从客户端设备(10)接收凭证记录(70)、待签名的电子文件(48)以及用户的生物统计数据(54),所述凭证记录(70)是由所述客户端设备(10)通过将以下关联而生成的:
 - 所述查问值(50),
 - 简化生物统计数据(56)的散列(58)、所述简化生物统计数据(56)是应用利用所述投影参数(52)的投影根据生物统计数据(54)生成的,以及
 - 所述电子文件(48)的散列(49),
 - 应用利用所述投影参数(52)的所述投影根据所述生物统计数据(54)生成简化生物统计验证数据(56'),
 - 生成所述简化生物统计验证数据(56')的散列(58'),
 - 生成所述电子文件(48)的散列(49),
 - 通过将所述查问值(50)、所述简化生物统计验证数据(56')的所述散列(58')以及所述电子文件(48)的所述散列(49)关联来生成验证凭证记录(70'),并且将所述验证凭证记录(70')与由所述客户端设备(10)发送的所述凭证记录(70)比较,并且只有当所述验证凭证记录(70')与由所述客户端设备(10)发送的所述凭证记录(70)相同时,继续所述数字签名的过程,
 - 识别所述客户端设备(10)的用户,并且定义至少一个用户数据(74)项,
 - 通过将至少所述电子文件(48)的散列(49)、所述至少一个用户数据(74)项以及至少与签名的时间相关的签名数据(78)关联来生成服务器证书(80),
 - 应用所述服务器的私有签名密钥(41)对所述服务器证书(80)进行签名,由此生成已签名服务器证书(82),
 - 通过将至少所述已签名服务器证书(82)和所述电子文件(48)的所述散列(49)关联来生成数字签名(85),以及
 - 将所述数字签名(85)和所述电子文件(48)关联,从而生成已数字签名的电子文件(86)。
2. 根据权利要求1所述的方法,其特征在于,代表所述用户对所述已数字签名的电子文件(86)进行签名。
3. 根据权利要求2所述的方法,其特征在于,用所述用户的私有签名密钥(42)进行签名。
4. 根据权利要求1或2所述的方法,其特征在于,通过单向映射由所述生物统计数据(54)生成视觉上可显示的生物统计数据(54a),其中,还将所述视觉上可显示的生物统计数据(54a)与所述服务器证书(80)以及与所述电子文件(48)的所述散列(49)相关联,用于生成所述数字签名(85)。
5. 根据权利要求1或2所述的方法,其特征在于,基于所述生物统计数据(54)对所述用户进行认证。
6. 根据权利要求5所述的方法,其特征在于,在认证期间,将所述生物统计数据(54)与

生物统计模板(45a)比较。

7. 根据权利要求1所述的方法,其特征在于,接收由所述客户端设备(10)签名的凭证记录(72)作为凭证记录(70),并验证所述签名。

8. 根据权利要求1所述的方法,其特征在于,接收由所述客户端设备(10)加密的生物统计数据(64)和/或由所述客户端设备加密的电子文件(68)作为生物统计数据(54)和/或作为电子文件(48),并且在生成所述简化生物统计数据(56)之前解密所述加密的生物统计数据(64)和/或加密的电子文件(68)。

9. 根据权利要求8所述的方法,其特征在于,接收用所述服务器的公共加密密钥(40a)加密的加密生物统计数据(64)和/或加密电子文件(68),并用所述服务器的私有加密密钥(40b)对其进行解密,或者接收用所述服务器的公共加密密钥(40a)加密的加密生物统计数据(64)和/或加密电子文件,并用所述服务器的私有加密密钥(40b)将加密对称密钥解密,随后用所述对称密钥将所述加密生物统计数据(64)和/或加密电子文件(68)解密。

10. 根据权利要求1所述的方法,其特征在于,通过将至少所述查问值(50)、所述生物统计数据(54)以及所述电子文件(48)的所述散列(49)关联来生成服务器凭证记录(90),用所述服务器的私有签名密钥(41)对所述服务器凭证记录(90)进行签名,并且存储得到的已签名服务器凭证记录(92)。

11. 根据权利要求1所述的方法,其特征在于,通过生物统计数据采集单元(18a)记录用户的生物统计数据(54),并且通过所述客户端设备(10):

-应用利用所述投影参数(52)的投影根据所述生物统计数据(54)生成简化生物统计数据(56),

-生成所述简化生物统计数据(56)的散列(58),

-生成所述电子文件(48)的散列(49),

-通过将至少所述查问值(50)、所述简化生物统计数据(56)的散列(58)以及所述电子文件(48)的散列(49)关联来生成凭证记录(70),以及

-通过所述通信信道(30)将所述凭证记录(70)、待签名的所述电子文件(48)以及所述生物统计数据(54)传送到所述服务器(20)。

12. 根据权利要求11所述的方法,其特征在于,通过所述客户端设备(10)对所述凭证记录(70)进行签名,并且通过所述服务器(20)验证所述签名。

13. 根据权利要求11或12所述的方法,其特征在于,在传送所述生物统计数据(54)和/或待签名的所述电子文件(48)之前,通过所述客户端设备(10)加密所述生物统计数据(54)和/或待签名的所述电子文件(48)。

14. 根据权利要求11所述的方法,其特征在于,所述生物统计数据采集单元(18a)是数字化平板,通过所述数字化平板接收手写签名并将该手写签名记录作为生物统计数据(54)。

15. 根据权利要求14所述的方法,其特征在于,将该手写签名记录作为选自以下组中的至少一种类型的生物统计数据(54):按压写入设备的位置的坐标、从所述写入设备抬起的位置的坐标、写入设备坐标的时间函数、写入设备速度的时间函数、写入设备加速度的时间函数、写入设备压力的时间函数。

16. 根据权利要求11所述的方法,其特征在于,所述生物统计数据采集单元(18a)是虹

膜扫描仪,通过所述虹膜扫描仪接收虹膜图像,并且将表示所述虹膜图像的数字数据存储作为生物统计数据(54)。

17. 根据权利要求11所述的方法,其特征在于,所述生物统计数据采集单元(18a)是指纹读取器,通过所述指纹读取器接收指纹,并且将表示所述指纹的数字数据存储作为生物统计数据(54)。

18. 一种用于对电子文件进行数字签名的方法,其特征在于:

- 通过服务器(20)生成包括投影参数(52)的查问值(50),
- 经由通信信道(30)通过所述服务器(20)将所述查问值(50)传送到客户端设备(10),
- 通过生物统计数据采集单元(18a)记录生物统计数据(54),
- 通过应用利用所述投影参数(52)的投影,通过所述客户端设备(10)根据所述生物统计数据(54)生成简化生物统计数据(56),
- 通过所述客户端设备(10)生成所述简化生物统计数据(56)的散列(58),
- 通过所述客户端设备(10)生成所述电子文件(48)的散列(49),
- 通过将至少所述查问值(50)、所述简化生物统计数据(56)的散列(58)和所述电子文件(48)的散列(49)关联,由所述客户端设备(10)生成凭证记录(70),
- 经由所述通信信道(30)通过所述客户端设备(10)将所述凭证记录(70)、待签名的所述电子文件(48)和所述生物统计数据(54)传送到所述服务器(20),
- 通过所述服务器(20)应用利用投影参数(52)的投影根据所述生物统计数据(54)生成简化生物统计验证数据(56'),
- 通过所述服务器(20)生成所述简化生物统计验证数据(56')的散列(58'),
- 通过所述服务器(20)生成所述电子文件(48)的散列(49),
- 通过将所述查问值(50)、所述简化生物统计验证数据(56')的散列(58')以及所述电子文件(48)的散列(49)关联,由所述服务器(20)生成验证凭证记录(70'),并且用于将该验证凭证记录与由所述客户端设备(10)发送的所述凭证记录(70)比较,并且只有当所述验证凭证记录(70')与由所述客户端设备(10)发送的所述凭证记录(70)相同时,继续所述数字签名的过程,
- 通过所述服务器(20)识别所述客户端设备(10)的用户,并且定义至少一个用户数据(74)项,
- 通过将至少所述电子文件(48)的散列(49)、所述至少一个用户数据(74)项以及至少与签名的时间相关的签名数据(78)关联,由所述服务器(20)生成服务器证书(80),
- 通过所述服务器(20)应用所述服务器的私有签名密钥(41)对所述服务器证书(80)进行签名,从而生成已签名服务器证书(82),
- 通过将至少所述已签名服务器证书(82)和所述电子文件(48)的散列(49)关联,由所述服务器(20)生成数字签名(85),以及
- 通过所述服务器(20)将所述数字签名(85)与所述电子文件(48)关联,从而生成已数字签名的电子文件(86)。

19. 根据权利要求18所述的方法,其特征在于,通过所述服务器(20)代表所述用户对所述已数字签名的电子文件(86)进行签名。

20. 根据权利要求19所述的方法,其特征在于,用所述用户的私有签名密钥进行签名。

21. 根据权利要求18或19所述的方法,其特征在于,由所述服务器(20)通过单向映射由所述生物统计数据(54)生成视觉上可显示的生物统计数据(54a),其中,还将所述视觉上可显示的生物统计数据(54a)与所述服务器证书(80)以及与所述电子文件(48)的所述散列(49)相关联,用于生成所述数字签名(85)。

22. 根据权利要求18所述的方法,其特征在于,基于所述生物统计数据(54)通过所述服务器(20)对所述用户进行认证,在认证的过程中,将所述生物统计数据(54a)与生物统计模板(45a)比较。

23. 根据权利要求18所述的方法,其特征在于,通过将至少所述查询值(50)、所述生物统计数据(54)以及所述电子文件(48)的散列(49)关联,由所述服务器(20)生成服务器凭证记录(90),用所述服务器的私有签名密钥(41)对所述服务器凭证记录(90)进行签名,并存储得到的已签名服务器凭证记录(92)。

24. 根据权利要求18所述的方法,其特征在于,由所述客户端设备(10)对所述凭证记录进行签名,并且由所述服务器验证所述签名。

25. 根据权利要求18所述的方法,其特征在于,在传送所述生物统计数据(54)和/或所述电子文件(48)之前通过所述客户端设备(10)对所述生物统计数据(54)和/或所述电子文件(48)进行加密,从而生成加密生物统计数据(64)和/或加密电子文件(68),并且通过所述服务器(20)解密所述加密生物统计数据(64)和/或所述加密电子文件(68)。

26. 一种用于对电子文件进行数字签名的方法,其特征在于,通过服务器执行的下述步骤:

- 生成包括投影参数(52)的查询值(50),
- 通过通信信道(30)将所述查询值(50)传送到客户端设备(10),
- 通过通信信道(30)从所述客户端设备(10)接收凭证记录(70)、待签名的所述电子文件(48)以及根据所述投影参数(52)简化的用户的简化生物统计数据(56),所述凭证记录(70)是由所述客户端设备(10)通过将以下关联而生成的:
 - 所述查询值(50),
 - 简化生物统计数据(56)的散列(58),以及
 - 所述电子文件(48)的散列(49),
- 生成所述简化生物统计数据(56)的散列(58'),
- 生成所述电子文件(48)的散列(49),
- 通过将所述查询值(50)、所述简化生物统计数据(56)的所述散列(58')以及所述电子文件(48)的所述散列(49)关联来生成验证凭证记录(70'),并且将所述验证凭证记录与由所述客户端设备(10)发送的凭证记录(70)比较,并且只有当所述验证凭证记录(70')与由所述客户端设备(10)发送的所述凭证记录(70)相同时,继续所述数字签名的过程,
 - 识别所述客户端设备(10)的用户,并且定义至少一个用户数据(74)项,
- 通过将至少所述电子文件(48)的所述散列(49)、所述至少一个用户数据(74)项以及至少与签名的时间相关的签名数据(78)关联来生成服务器证书(80),
- 应用所述服务器的私有签名密钥(41)对所述服务器证书(80)进行签名,由此生成已签名服务器证书(82),
- 通过将至少所述已签名服务器证书(82)和所述电子文件(48)的散列(49)关联来生成

数字签名(85),以及

-将所述数字签名(85)和所述电子文件(48)关联,从而生成已数字签名的电子文件(86)。

27. 根据权利要求26所述的方法,其特征在于,基于所述简化生物统计数据(56)认证所述用户,在所述认证期间,将包括投影参数(52)的投影应用于根据所述用户的生物统计模板(45a)生成简化生物统计模板验证数据(56'');并将所述简化生物统计数据(56)与所述简化生物统计模板验证数据(56'')比较。

28. 根据权利要求27所述的方法,其特征在于,接收由所述客户端设备(10)加密的加密简化生物统计数据(65)作为简化生物统计数据(56),并且在认证之前解密所述加密简化生物统计数据(65)。

29. 根据权利要求26所述的方法,其特征在于,

-通过生物统计数据采集单元(18a)记录所述用户的简化生物统计数据(56),

-生成所述简化生物统计数据(56)的散列(58),

-生成所述电子文件(48)的散列(49),

-通过将至少所述查问值(50)、所述简化生物统计数据(56)的散列(58)以及所述电子文件(48)的散列(49)关联来生成凭证记录(70),以及

-通过所述通信信道(30)将所述凭证记录(70)、待签名的所述电子文件(48)以及所述简化生物统计数据(56)传送到所述服务器(20)。

30. 用于对电子文件进行数字签名的方法,其特征在于,

-通过服务器(20)生成包括投影参数(52)的查问值(50),

-经由通信信道(30)通过所述服务器(20)将所述查问值(50)传送到客户端设备(10),

-通过连接到所述客户端设备(10)的生物统计数据采集单元(18a),应用利用所述投影参数(52)的投影对简化生物统计数据(56)进行记录,

-通过所述客户端设备(10)生成所述简化生物统计数据(56)的散列(58),

-通过所述客户端设备(10)生成所述电子文件(48)的散列(49),

-通过将至少所述查问值(50)、所述简化生物统计数据(56)的散列(58)以及所述电子文件(48)的散列(49)关联,由所述客户端设备(10)生成凭证记录(70),

-经由所述通信信道(30)通过所述客户端设备(10)将所述凭证记录(70)、待签名的所述电子文件(48)以及所述简化生物统计数据(56)传送到所述服务器(20),

-通过所述服务器(20)生成所述简化生物统计数据(56)的散列(58'),

-通过所述服务器(20)生成所述电子文件(48)的所述散列(49),

-通过将所述查问值(50)、所述简化生物统计数据(56)的散列(58')以及所述电子文件(48)的散列(49)关联,由所述服务器(20)生成验证凭证记录(70'),并且将所述验证凭证记录与由所述客户端设备(10)发送的所述凭证记录(70)比较,并且只有当所述验证凭证记录(70')与由所述客户端设备(10)发送的所述凭证记录(70)相同时,继续所述数字签名的过程,

-借助所述服务器(20)识别所述客户端设备(10)的用户,并定义至少一个用户数据(74)项,

-通过将至少所述电子文件(48)的散列(49)、所述至少一个用户数据(74)项以及至少

与签名的时间相关的签名数据(78)关联,由所述服务器(20)生成服务器证书(80),

-通过所述服务器(20)应用所述服务器的私有签名密钥(41)对所述服务器证书(80)进行签名,由此生成已签名服务器证书(82),

-通过所述服务器(20),通过将至少所述已签名服务器证书(82)和所述电子文件(48)的散列(49)关联生成数字签名(85),以及

-通过所述服务器(20)将所述数字签名(85)和所述电子文件(48)关联,由此生成已数字签名的电子文件(86)。

31.根据权利要求30所述的方法,其特征在于,通过服务器(20)基于所述简化生物统计数据(56)对所述用户进行认证,在所述认证期间,将包括投影参数(52)的投影应用于根据所述用户的生物统计模板(45a)生成简化生物统计模板验证数据(56'');并将所述简化生物统计数据(56)与所述简化生物统计模板验证数据(56'')比较。

32.根据权利要求30所述的方法,其特征在于,在传送所述简化生物统计数据(56)之前,由所述客户端设备(10)对所述简化生物统计数据进行加密,从而通过所述服务器生成加密简化生物统计数据(65)。

用于对电子文件进行数字签名的方法以及认证方法

技术领域

[0001] 本发明涉及用于对电子文件进行数字签名的方法,并且涉及一种基于生物统计(biometrics,生物测定)的认证方法。

背景技术

[0002] 存在许多不同的用于对电子文件进行认证和签名的方法。W02007/034255公开了一种方法,其中一种集中数字签名提供系统用于代表远程用户使用包括用户的生物统计数据数字签名对其提交的电子文件进行数字签名。通过生物统计数据(例如,与手写签名相关的数据),可以将数字签名和签名人联系起来,同时该发明要求数字签名仅可以以受监督和认证的方式应用于电子文件。该方法具有以下缺点:由远程用户发回的数据的验证以及生物统计数据的管理都不够安全。

[0003] 在US 6735695B1中公开了一种方案,其中仅使用生物统计数据的一部分而不是全部生物统计样本来执行认证。为了增强安全性,因此要求不传送完整的生物统计样本。也可以使用随机数来选择应用于认证的部分生物统计样本。这种已知方案的缺点是没有进行数据简化(转换),因此通过在通信线路上窃取部分生物统计信息,未经授权的人迟早可以捕获完整的生物统计信息。该方案的另一缺点是生物统计传感器记录了完整的生物统计样本,而且部分的生物统计信息选自完整样本。记录完整生物统计样本构成了显著的漏洞。

[0004] US2008/0209227A1公开了一种方案,其中,生成了一种转换、简化版本的生物统计样本。该简化生物统计数据或简化生物统计摘要数据可以包含生物统计样本的不同特有特征,诸如其线性部分。在US2010/0066493A1中,公开了一种涉及生物统计数据的随机投影转换的方案。这些已知的方案也都具有上述缺点。

发明内容

[0005] 本发明的目的是提供在最大可能程度上消除现有技术方案的缺点的、用于进行数字签名和用于进行认证的方法。

[0006] 通过根据本发明实施方案提供的方法实现本发明的目的。

附图说明

[0007] 将通过在附图中示出的优选实施方案进一步详细地解释本发明,附图中:

[0008] 图1为根据本发明的方法中应用的主要信息技术设备的示意性框图,

[0009] 图2为根据本发明的方法的概要流程图,

[0010] 图3为根据本发明的方法的第一实施方案的客户端步骤的示意性流程图,

[0011] 图4为根据本发明的方法的第一实施方案的服务器端验证和认证步骤的示意性流程图,

[0012] 图5为通过修改图3中示出的实施方案获得的另一实施方案的流程图,

[0013] 图6为通过修改图4中示出的实施方案获得的、与图5相关的服务器端流程图,

[0014] 图7为通过服务器对电子文件加密的示意性流程图,以及

[0015] 图8为产生服务器凭证记录并对其进行签名的示意性流程图。

具体实施方式

[0016] 在图1中示出了在根据本发明的方法中应用的主要信息技术设备和主部件。根据本发明的方法适于通过服务器20对客户端设备10上可用或生成的电子文件进行签名。客户端设备10可以通过通信信道30连接到服务器20。这种电子通信信道30可以建立在例如电子通信网络32内,诸如通过例如应用有线和/或无线局域网(LAN)、全球IT网络,特别是互联网、以及对应于3G或4G标准的移动通信网络、GSM网络等。

[0017] 客户端设备10可以实施为任何包括一个或多个处理器12、数据存储器14、客户端通信单元16和外围设备18的用户通信设备。例如,客户端设备10可以是台式机、膝上型或笔记本计算机、手机(移动电话)特别是智能电话、平板计算机等。

[0018] 在本实施方案中,数据存储器14被示出为客户端设备10的集成部分,但是数据存储器14也可以是外部数据存储装置,即,本文被称为数据存储器14的部件旨在包括客户端设备10能够访问的任何内部和外部数据存储装置。数据存储器14可以实施为任何类型的电子、磁性、光学或任何其它的数据存储装置(诸如内存、存储卡、硬盘、外部盘等)。数据存储器14优选地应用于存储PKI(公共密钥基础设施)密钥、至少对应于服务器20的服务器的公共加密密钥40a。还可以设想一种实施方案,其中,服务器的公共加密密钥40a不存储在数据存储器14中,但对于客户端设备10临时可用,为了加密过程的目的可从互联网临时下载。

[0019] 称为客户端通信单元16的部件旨在包括任何硬件和软件部件(即,网卡、网络连接件、WiFi适配器、天线等),客户端设备10可以通过所述客户端通信单元至少与服务器20建立电子通信信道30,通过该通信信道可以交换电子数据。

[0020] 客户端设备10包括生物统计数据采集单元18a以及优选地至少一个输入接口18b和至少一个输出接口18c,它们作为客户端设备的部件或者作为连接到客户端设备的外围设备18或者作为其他外部单元(即,以任何方式连接到客户端设备10)。

[0021] 例如,生物统计数据采集单元18a可以是能够接收和记录手写签名作为生物统计数据的数字化平板。数字化平板可以配有数码笔,但在特定情况下,用户的手指也可以用作由数字化平板检测的“写入设备”。

[0022] 例如,生物统计数据采集单元18a可以实现为虹膜扫描器,通过该虹膜扫描器接收虹膜图像,并且将表示虹膜图像的数字数据存储作为生物统计数据。

[0023] 生物统计数据采集单元18a还可以是指纹读取器,应用该指纹读取器接收指纹并且将表示指纹的数字数据存储作为生物统计数据。

[0024] 除此之外,生物统计数据采集单元18a可以是适于测量/登记生物统计标识符(例如,手掌静脉图案,DNS)并且适于记录所得数据的任何其他类型的设备。

[0025] 还可以设想一种实施方案,其中,生物统计数据采集单元18a同时还用作输入接口18b。例如,除了接收手写签名之外,数字化平板还可以应用于输入用户命令以操作在客户端设备10上运行的软件程序。

[0026] 客户端设备10优选地包括用作输出接口18c的至少一个屏幕。除此之外,可以考虑其它输出接口18c,例如适于写入不同数字介质(如CD、DVD、软盘、记忆棒、记忆卡等)的打印

机或设备。

[0027] 该至少一个输入接口18b可以实现为例如键盘、鼠标或其他普通输入设备。输出接口18c同时也可以作为输入接口18b,例如触摸屏。同样,数据承载介质写入器设备也可以同时用作输入接口18b,只要其能够读取和写入介质。键盘可以实现作为虚拟键盘,例如在应用触摸屏作为屏幕的情况下,虚拟键盘可以在其上显示,能应用作为输入接口18b。

[0028] 在触摸屏应用作为输入接口18b和输出接口18c的情况下,触摸屏还可以执行生物统计数据采集单元18a的功能,即在特定情况下,单个外围设备可以执行三重功能。

[0029] 服务器20旨在包括能够用作服务器的其他IT设备(诸如台式或膝上型计算机)。服务器20还包括一个或多个处理器22、数据存储单元24和服务器通信单元26。

[0030] 数据存储单元24可以实现为任何类型的电子、磁性、光学或任何其他数据存储装置。在本实施方案中,数据存储单元24被示出为服务器20的集成部分,但是数据存储单元24还可以包括服务器20能够访问的外部数据存储装置,诸如图1中示出的硬件安全模块24'(HSM)。因此数据存储单元24旨在包括服务器20能够直接地或间接地访问的任何内部和外部数据存储装置(诸如内置ROM和RAM、外部HSM、其他外部存储装置等)。

[0031] 服务器20优选地具有公共密钥基础设施(PKI)密钥和其他签名密钥,诸如对应于服务器20的服务器的私有加密密钥40b和服务器的私有签名密钥41以及对应于用户的用户私有签名密钥42,这些可以存储在数据存储单元24的密钥数据库43中,并且特别优选地存储在HSM 24'中。数据存储单元24还可以优选地存储用户数据库44,以及包括在用户数据库44中或与用户数据库44分立的、适于存储用户的生物统计模板45a的生物统计数据库45。

[0032] 用户的私有签名密钥42还可以例如是基于PKI基础设施的私有加密密钥,任何人都可以应用该私有加密密钥来解密用公共加密密钥加密的数据,但不基于加密的其他签名算法也是已知的。例如,HMAC(基于散列的消息认证码)类型的算法也可以用于进行签名。这些算法涉及用密钥的值和消息本身生成组合的散列值。所述散列具有两个作用:一方面它保护消息的同一性,另一方面它证明它只能由拥有密钥的人生成。与PKI(RSA)类型的签名过程相比的主要区别在于:该过程实质上涉及一种类型的密钥,即用户的私有签名密钥42,但是不涉及用户的公共签名密钥,并且签名算法包括散列生成而不是加密。

[0033] 如上所述,称为服务器通信单元26的部件旨在包括任何硬件和软件部件(即,网卡、网络连接件、WiFi适配器、天线等),服务器20可以通过服务器通信单元26建立至少与客户端设备10的电子通信信道30,通过该信道可以交换电子数据。

[0034] 在下文中,将参照上文描述的示例性硬件部件来呈现根据本发明的方法的两个实施方案。

[0035] 图2示出了根据本发明的方法的概述流程图。在图2至图8中更详细地示出了该方法的步骤以及在其过程中利用或生成的文档、数据、算法和文件。

[0036] 虽然为了简单起见,步骤已经连续地编号,但是在许多情况下步骤的顺序可以改变,或者某些步骤可以同时进行,可以合并或细分,以及在本文呈现的步骤之间可以包括另外的步骤,这对技术人员来说是明显的。

[0037] 在根据本发明的方法之前,方便地在客户端设备10和服务器20之间建立通信信道30。通信信道30优选地是安全信道,其可以例如应用SSL、TLS、SNPv3、VPN、HTTPS、FTPS、TelnetS、IMAPS、IPSec等协议来实施,这是本领域技术人员所熟知的。在该方法的过程中,

通信信道30——作为虚拟数据信道——可以断开和重建,可选地在客户端设备10和服务器20之间建立不止一个虚拟数据信道,但是为了简化起见,这些统称为通信信道30。

[0038] 待签名的电子文件48的提供也可以被认为是根据本发明的方法的起始点。可以利用客户端设备10生成电子文件48,并且因此该电子文件可以为例如在客户端设备10上生成的文档或由被应用作为输入接口18b的由客户端设备10的摄像机拍摄的图片文件。还可以设想,待由客户端设备10的用户签名的电子文件48不由客户端设备10自身生成,而是由客户端设备10从外部源(诸如经由电子邮件)接收的,或者该电子文件48是从互联网下载的或从应用写入器/读取器设备作为输入接口18b的数据存储介质(例如CD、DVD、记忆棒等)读取的,或者是从服务器20或者其他地方接收的。

[0039] 在图3中详细地示出了在图2中呈现的根据本发明的方法的第一变型/实施方案的步骤1-8。

[0040] 作为根据本发明的方法的步骤1,利用服务器20生成查询值50。查询值50包括一个或多个投影参数52(通常为数字)。查询值50还可以可选地包含时间戳,该时间戳由服务器20自身生成或者在服务器20请求时由外部时间戳服务器例如根据RFC3161协议生成。

[0041] 在步骤2中,查询值50由服务器20通过通信信道30传送到客户端设备10。

[0042] 在步骤3中,客户端设备10被应用于从查询值50中提取一个或多个投影参数52。该步骤当然可以在使用投影参数52之前的任何时间进行,或者与其同时进行。

[0043] 在步骤4中,利用生物统计数据采集单元18a将用户的生物统计数据54记录在客户端10侧,所述生物统计数据可能包括基于用户的物理特征记录的一个或多个静态或动态数据项(数据集)。例如,在数字化平板被应用作为生物统计数据采集单元18a的情况下,使用数码笔或用户的手指作为写入设备产生的手写签名被接收并记录作为生物统计数据54。在这种情况下,生物统计数据54可以例如是将写入设备压在平板表面上的位置的坐标、将写入设备从平板表面上抬起的位置的坐标、写入设备坐标的时间函数、写入设备速度的时间函数、写入设备加速度的时间函数、写入设备压力的时间函数或不止一个这种数据的组合。

[0044] 在优选实施方案中,在输入手写签名期间,在应用作为输出设备18c的客户端设备10的屏幕上显示签名的图像,从而向用户提供视觉反馈。这在生物统计数据采集单元18a同时还用作屏幕的情况下是特别高效的,例如对于PDA-s、平板计算机、触摸屏手机等。

[0045] 如果生物统计数据采集单元被实现为虹膜扫描器,则接收虹膜图像,并且将表示虹膜图像的数字数据记录为生物统计数据54。在生物统计数据采集单元是指纹读取器的情况下,指纹被记录,并且表示指纹的数字数据被存储作为生物统计数据54。

[0046] 在步骤5中,客户端设备10被应用于生成凭证记录70。在此期间,客户端设备10被应用于利用单向安全散列算法60a生成电子文件48的散列49,该单向安全散列算法例如是SHA-256、SHA-512等算法。利用散列算法60a生成的散列49表示不可能由其推断出原始电子文件48的这种压缩数据。散列算法60a的特有特征在于,对原始电子文件48的任何部分的修改都会在散列49中导致雪崩效应,由此散列变得完全不同。通过再次生成散列49,可以检查是否已对电子文件48进行了(未授权的)改动,或者文件是否已经篡改。散列算法60a的另一重要特点是,不能由其产生数据文件,因为该算法会生成相同的散列49。

[0047] 凭证记录70的生成还涉及使用应用一个或多个投影参数52的投影算法由用户的生物统计数据54生成简化生物统计数据56。根据本发明,术语“投影”用于指代数据的单向

数学映射或其他简化,它们产生不能用于恢复原始数据的简化数据,同时简化数据只能由拥有原始数据和知道投影参数的人生成。应用投影(或者换言之,数据简化)参数的这种投影算法是本领域技术人员公知的,该算法包括例如在预定平面或轴线上对记录数据进行投影,或者通过神经网络处理该数据。在这种情况下,例如,可以由记录具有记录作为生物统计数据54的手写签名的动态签名数据生成静态签名图像(简化生物统计数据56)。

[0048] 简化生物统计数据56对于用户是特有的,但是不能应用于恢复原始生物统计数据54。简化生物统计数据56用作其生成器——在我们的实例中为客户端设备10——已经拥有原始生物统计数据54和与查询值50一起传送的投影参数52的凭证。

[0049] 随后,客户端设备10被应用于利用单向安全散列算法60b来生成简化生物统计数据56的散列58,该单向安全散列算法可以与散列算法60a相同或不同。

[0050] 然后,由客户端设备10通过将查询值50、简化生物统计数据56的散列58以及电子文件48的散列49关联来生成凭证记录70。可以应用任何已知的合适方法来进行数据关联,诸如按位异或(XOR)运算,其将这三个数据组合成使得它们中的任何一个都不能从结果中推断,但是保留了可验证性。如上所述,本文也可以应用适于通过连接这三个数据来生成散列(凭证记录70)的散列函数。

[0051] 凭证记录70可以另外包含其他数据。

[0052] 凭证记录70证明电子文件48和生物统计数据54源自给定的客户端设备10。在外部攻击者试图将先前记录的生物统计数据54与待签名的文档一起输入到系统中的情况下,他不能生成与其对应的凭证记录70,因为他不具有查询值50(查询值还可以可选地包含时间戳以防止篡改)。由于查询值50包含为每次签名事件生成的独特参数,所以生物统计数据54不能使用两次,无论是无意地还是故意地。

[0053] 接下来,在步骤6中,优选地利用客户端设备10应用数字签名算法71来对凭证记录70进行签名。签名算法71可以是例如基于PKI的(如RSA)、基于密码的、基于一次性密码的或任何其他可以适于适用给定情况的方案。签名过程产生已签名凭证记录72。

[0054] 在步骤7中,待签名的生物统计数据54和/或电子文件48优选地由客户端设备10签名,这可以使用服务器的公共加密密钥40a应用基于PKI的加密来进行,使得由此生成的加密生物统计数据64和加密电子文件68仅可以使用存储在服务器20的密钥数据库43中的服务器的私有加密密钥40b来解密。

[0055] 当然也可以应用其他方法来加密待签名的生物统计数据54和/或电子文件48。例如,特别是为了加密大文件,可能方便的是为每个加密事件生成独特的对称密钥,并使用该密钥(如,利用AES对称算法)将文件加密,其中所述对称密钥是利用服务器的PKI公共加密密钥40a来加密的并且通过客户端设备10被传送到服务器20。因此,在第一步骤中,在服务器端处,必须使用服务器的私有加密密钥40b来解密所述对称加密密钥,并且然后可以使用该对称密钥来将加密文件解密。这种两级加密过程的优点是对称算法比非对称加密算法快得多,同时加密数据文件的开销较小,所以甚至可以快速加密大型文件。

[0056] 在步骤8中,由客户端设备10通过通信信道30将已签名凭证记录72、优选加密生物统计数据64和优选加密电子文件68传送到服务器20。除此之外,在上述方法完成之前、期间或之后,优选地由客户端设备10向服务器20发送一个或多个用户数据74项(诸如用户标识符、用户PIN等)。例如,在生成凭证记录70期间,用户数据74也可以与上文列出的部件相关

联。然而,用户数据74可以与凭证记录70分开地被发送到服务器20(优选地为加密的),通常用于用户识别,这至少需要下述标识符数据,基于该标识符数据,服务器20可以例如从存储在密钥数据库43中的密钥中找出要使用哪个用户的私有签名密钥42,或者例如指定使用哪个用户的用户数据74生成存储在用户数据库44中的数据的数字签名(在下面详细描述),或者例如指定从生物统计数据库45中检索哪个用户的生物统计模板45a——对应于给定用户的独特生物统计样本(模板)。服务器20通过数据通信可用的其他信息还可以执行用户标识符的功能——用作用户数据74,诸如电话号码(如果将智能电话应用作为客户端设备10)或静态IP地址(在将台式计算机应用作为客户端设备10的情况下)等。

[0057] 在图4中详细地示出了在图2中呈现的根据本发明的方法的第一变型的步骤9-11。

[0058] 在步骤9中,服务器20应用于识别客户端设备10的用户,并且用于定义至少一个用户数据74项。后者可以是由客户端设备10发送的用户数据74,或者是基于由客户端设备发送的用户数据74从用户数据库44中检索的其他用户数据74项。

[0059] 与步骤9相关的事件可以是用户认证,在该用户认证期间,例如,验证由客户端设备10签名的凭证记录72的签名,并且由此认证用户。

[0060] 然而,在特别优选的实施方案中,认证是基于生物统计数据54执行的。为了执行认证,在步骤10中,首先用服务器的私有加密密钥40b解密由客户端设备10发送的加密生物统计数据64(或者,可选地,使用服务器的私有加密密钥40b解密的对称密钥)。接下来,从生物统计数据库45中检索用户数据74指定的对应于用户的生物统计模板45a,然后由服务器20使用合适的软件程序(例如,包括基于神经网络、基于投影、基于CRC或其他类似算法的软件程序)将生物统计模板45a与已解密的生物统计数据54进行比较。例如,由在服务器20上运行的程序使用给定用户的较早的样本签名作为生物统计模板45a来验证手写签名的真实性。在认证成功的情况下,即,所传送的生物统计数据54与为给定用户存储的一个或多个生物统计模板45a匹配,则过程继续,否则拒绝对电子文件48进行签名的请求,并且停止过程。

[0061] 使用生物统计数据54执行认证的优点是用户不必记住任何PIN码。使用手写签名作为生物统计数据54执行认证是特别优选的,因为它是与以习惯的方式对纸质文档进行签名最接近的情况。

[0062] 优选地,传送到服务器20的所有生物统计数据54存储在生物统计数据库45中作为对应于给定用户的相应生物统计模板45a,同时服务器20还检查当前提交的生物统计数据54是与先前存储的生物统计模板45a相同,还是与其部分相同,从而提供保护以防止重复提交先前的生物统计数据54。

[0063] 在步骤11中,根据以下内容利用服务器20生成验证凭证记录70'(参见图4):

[0064] 服务器20用于使用与在客户端处用于生成简化生物统计数据56相同的投影算法,从应用使用在查问值50中发送的投影参数52的投影获得的生物统计数据54生成简化生物统计验证数据56'。随后,使用在客户端处应用于生成简化生物统计数据56的散列58的相同散列算法60b来生成简化生物统计验证数据56'的散列58'。

[0065] 接下来,服务器20用于使用在客户端处用于生成电子文件48的散列49的相同散列算法60a生成电子文件48的散列49'。

[0066] 然后,通过将所述查问值50、简化生物统计验证数据56'的散列58'以及电子文件48的散列49'关联,由服务器20生成验证凭证记录70',并且将该验证凭证记录70'与由客户

端设备10发送的凭证记录70比较。在验证凭证记录70'与由客户端设备10传送的凭证记录70相同的情况下,数字签名过程继续,否则拒绝该请求,并且停止该过程。

[0067] 在图5和图6中示出了根据本发明的方法的第二变型的对应步骤,其分别对应于图3和图4的修改形式。

[0068] 关于防止生物统计数据的窃取和再使用的保护,优选的是,如果不将与查问值一起提交的投影参数应用于随后对记录的生物统计的简化,而是根据对应于参数的简化进行简化数据记录。实际上,如果存储的生物统计数据能够访问,则可以从记录的生物统计数据针对任何参数值生成简化生物统计。然而,在参数值本身影响重新编码过程的情况下,那么记录的简化生物统计数据在之后不能用于产生对应于不同参数值的简化。

[0069] 在手写签名的情况下,示例性方案是其中参数的一部分包括将由签名者手写的文本,并且在同一文本从未写入两次的情况下,这就确保之后不会使用先前记录的固定文本生成对应于不同参数值(文本)的手写值。

[0070] 投影参数和与其对应的生物统计数据简化的实施可以分为三个主要类别。这些类别中的每一个均涉及根据参数进行的转换(这三个类别也可以应用于图3和图4示出的本发明的第一变型)。

[0071] 1. 简化生物统计,其中,由给定参数直接确定转换。示例:

[0072] -速度在给定方向的直线上的投影(签名),

[0073] -加速度在给定方向的直线上的投影(签名),

[0074] -使用给定的X、Y、Z值进行的采样(签名),

[0075] -从由参数确定的给定位置中检索到的图像信息(签名、指纹、虹膜),

[0076] -特征点在给定方向的直线上的投影(指纹、虹膜)。

[0077] 2. 简化生物统计,其中,参数用于选择认证算法(或同时选择不止一个算法)。在这种情况下,生物统计数据的验证结果由多个特有特征的各个验证结果组成。例如,检查X和Y方向速度和切向量的角度的暂时变化;并且基于由各个比较结果产生的分数做出最终决定。在这种情况下,简化参数仅确定待由记录设备进行的简化的类型。例如,如果参数指示使用X方向加速度和切向量的角度变化来进行认证,那么将记录这两个数据序列(=简化生物统计),根据这两个数据序列无法恢复原始生物统计。示例:

[0078] -切向量(签名),

[0079] -X和Y方向速度和加速度(签名),

[0080] -压力(签名)。

[0081] 3. 简化生物统计,其中,通过给定参数间接确定转换。例如,使用神经网络实施的方案属于该类别。例如,应用于认证的神经网络可以由3层组成。给定的神经网络具有固定的结构,并且通过其结构和权重被限定的同一网络总是被应用于对给定的人进行认证。对每个待认证的人训练出独特的神经网络,该网络只能用于辨识给定的人。参数值有利地包含神经网络的第一层的权重并可选地包含其它设置。在注册过程期间,基于由服务器发送的投影参数52来计算所有第二层的输入参数,这有效地构成了根据其无法恢复签名的简化生物统计。认证模块不必基于参数值再次计算神经网络(该网络对于模块来说是已知的,因为该网络是在签名注册过程期间构建的),并且因此服务器所要做的就是确保通过参数定义的第一层与已知的神经网络的第一层相同,并且如果相同,则第二层和第三层将在认证

模块中运行。

[0082] 如果网络具有5层并且所提交的参数包含前两层的数据,则将从客户端处接收的第三层的输入作为简化生物统计,并且服务器将在认证模块中运行第三层、第四层和第五层。

[0083] 在上述三种类别的情况下应用的生物统计模板如下所述。

[0084] 在类别1的情况下,生物统计数据库45和其中包含的生物统计模板45a通常包括早前记录的生物统计样本本身(如,签名),因为这些生物统计样本可以应用于计算在认证过程期间所需的所有信息。数据简化参数,诸如对于每个时期的投影线的参数化或其他选择决定的参数是不同的,并且还应该能够针对模板包含的样本/签名再次计算简化映射。这种情况的特殊子情形可以是当应用有限数量的预先记录的“投影”,即,简化生物统计(例如,在3个预定线上的投影)时,在这种情况下,不需要由认证模块使用完整生物统计数据集(在注册时记录的)重新计算参考数据序列,因为可以提前在注册过程期间计算该数据。因此,甚至可以执行这样的实施方案,其中,认证模块本身甚至也不知道完整的生物统计样本。

[0085] 因此,在类别1和类别2的情况下,给定的人的生物统计模板可以由预先计算的简化数据序列组成,因为这些数据可以在该人注册时生成。

[0086] 然而,对于类别3的神经网络变型,人的生物统计模板由具体针对给定的人训练的神经网络的权重值和设置构成。在提交参数值时神经网络必须存在(因为参数由网络的第一层构成),并且由于网络的性质,无法以与之前完全相同的方式再次生成(训练)网络。因此,神经网络的设置应存储在生物统计模板中。

[0087] 总而言之,因此可以设想,生物统计模板可以:

[0088] -包括注册期间记录的完整生物统计模板,

[0089] -包括仅某些预先计算的数据序列(简化生物统计),在这种情况下无法应用任意投影,或者

[0090] -包括完整生物统计样本和预先计算的数据序列的组合。

[0091] 当然,在生物统计标识符的验证期间,可能发生上述参数的所有可能组合,即,可能发生下述情况:如查问值50的投影参数52所规定的,对于认证X方向加速度的给定投影,需要按给定算法(例如,基于压力)获得的值以及对应于给定的人的神经网络的第二层的输入值。然后最终通过组合这些部分的认证来提供认证。

[0092] 图5示出了包括本发明的第二变型的客户端步骤的流程图。通过比较图3和图5,可以看出本发明的该第二变型与上述实施方案的不同之处在于,为了增强安全性,完整的生物统计数据不记录在客户端,而是查问值50携带的投影参数52已经确定记录生物统计数据的方式,即,在客户端仅记录简化生物统计数据56而不是完整生物统计。简化数据可以以不同的方式记录。在示例性的情况中,可以设想,将投影参数52考虑在内,生物统计数据采集单元18a只将简化生物统计数据56存储在其存储器中并传送下去进行进一步处理。也可以设想下述变型:其中,完整的生物统计数据临时存在于生物统计数据采集单元18a的存储器中,但是仅记录和提交通过投影参数52确定的部分内容。

[0093] 除此之外,根据图5的实施方案与图3所示实施方案的不同之处在于,在该方法的过程中,仅简化生物统计数据56可用于提交给服务器20,优选地以加密形式提交,即,作为加密的简化生物统计数据65。

[0094] 根据上文在根据本发明的方法的任何和所有实施方案中所述的, 查问值50中包括的投影参数52的数据内容可以非常广泛地变化。可以设想一种情况, 其中, 查问值50由投影参数52本身构成, 该投影参数仅由单个参数组成。还可以设想, 查问值50包含除了投影参数52之外的另外的数据, 该另外的数据不参与数据简化过程。投影参数52可以是单个参数或者甚至是参数集, 因为在由神经网络进行数据处理的情况下, 这是输入层、层的权重以及可选地网络的其它参数所需的。在本申请的上下文中, 投影参数52是指在最广泛的可能意义上的上述任何参数或参数集。在本文中, 术语“投影”不暗示数据简化只能狭义地通过投影来进行, 而是投影参数52指可以通过其进行生物统计样本的数据简化的任何参数。因此, 对于投影参数52, 应以最广泛的可能意义理解为任何类型的数据简化参数或参数集。

[0095] 在图6中示出了与图5所示的本发明的第二变型的服务器端步骤相关的处理。通过比较图6和图4, 可以看出, 在该第二实施方案中, 在服务器端没有接收完整的生物统计数据集, 而只接收——优选加密的——加密简化生物统计数据65。使用服务器的私有加密密钥40b来根据这些数据解密出——在应用了加密的情况下——简化生物统计数据56, 并且该简化生物统计数据随后可以应用于生成验证凭证记录70'或优选地用于认证目的。

[0096] 在根据图6的过程中, 简化生物统计数据56在服务器端是可用的, 不需要用投影参数52来产生它们。如可以看出的, 本发明的该实施方案比根据图3和图4的实施方案更安全, 因为此处没有传达完整的生物统计样本, 甚至不是加密形式的。

[0097] 在本实施方案中, 简化生物统计数据56可以用于在服务器端的认证。利用对应的用户数据74, 在生物统计数据库45中存储的生物统计模板45a中识别出与给定用户对应的生物统计模板45a, 然后通过查问值50携带的投影参数52根据给定的生物统计模板45a产生简化生物统计模板验证数据56”。因此, 可以通过比较简化生物统计数据56(以加密形式从客户端处接收然后解密)和简化生物统计模板验证数据56”来进行认证。

[0098] 在图7中详细地示出了根据本发明的方法的步骤12-16。在步骤12中, 服务器20被应用于通过将所述电子文件48的至少散列49、至少一个用户数据74项以及与签名的时间相关的至少签名数据78关联来生成服务器证书80。

[0099] 该至少一个用户数据74项可以是客户端设备10发送的用户数据74, 或者是基于客户端设备发送的用户数据74从用户数据库44中检索的其他数据。应用于生成服务器证书80的用户数据74通常包括以下数据项中的一个或多个: 用户(签名人)的姓名、出生数据、出生地、母亲姓名、地址、身份证号码等。

[0100] 签名数据78是描述签名事件的“情况”的元数据, 其通常包括以下中的一个或多个: 签名日期、客户端设备10上的信息、服务器20上的信息、已签名电子文件48的名称等等。

[0101] 在步骤13中, 服务器证书80优选地由具有服务器的私有签名密钥41的服务器20来进行签名, 以产生已签名服务器证书82, 该已签名服务器证书随后可以用于明确地认定签名源自服务器20。该服务器的私有签名密钥41可以与在先前步骤期间应用的服务器的私有加密密钥40b相同。然而, 可以利用不同的密钥或不同的签名算法来生成已签名服务器证书82, 可应用的签名算法例如包括HMAC(基于散列的消息认证码)类型的算法。

[0102] 在步骤14中(其可以在步骤12和13之前), 服务器20用于用单向映射算法84可选地根据生物统计数据54(或者在根据图5和6的实施方案的情况下, 根据简化生物统计数据56)生成视觉上可显示的生物统计数据54a。例如, 根据记录的手写签名的动态数据产生静态签

名图像。还可以设想,根据其他类型的生物统计数据54(诸如指纹、手掌静脉图像、虹膜图像)产生视觉上可显示的生物统计数据54a,但是在这些生物统计数据类型的情况下,通常不产生视觉上可显示的生物统计数据54a。可选地,映射算法84还可以基于使用投影参数52进行的投影算法。

[0103] 在步骤15中,服务器20用于通过将已签名服务器证书82、电子文件48的散列49以及视觉上可显示的生物统计数据54(在其可用的情况下)关联来生成数字签名85。在该步骤期间,优选地通过将数据封装在数据包中来进行数据关联。随后,将数字签名85与电子文件48关联,例如通过将电子签名嵌入电子文件中或者通过将这二者包括在共同的标准(例如,XML)文件中,从而产生已数字签名的电子文件86。嵌入优选地被执行为使得在打开已数字签名的电子文件86时所述视觉上可显示的生物统计数据54a可以作为签名图像查看。数字签名85当然也可以包含其他数据。

[0104] 优选地,在步骤16中,还利用服务器20例如应用用户的私有签名密钥42代表用户对已数字签名的电子文件86进行签名,以获得双重签名的电子文件88。使用用户的公共签名密钥,任何人都可以确保所述双重签名的电子文件88是用对应于给定用户(签字人)的用户私有签名密钥42进行了签名。

[0105] 在图8中详细地示出了根据本发明的方法的步骤17。

[0106] 在步骤17中,服务器20用于通过将至少查问值50、生物统计数据54(或者在根据图5和6的实施方案中,简化生物统计数据56)以及电子文件48的散列49(例如通过上述的按位XOR运算,或者用散列算法)关联来生成服务器凭证记录90,然后用服务器的私有签名密钥41对所述服务器凭证记录90进行签名,并且存储因此获得的已签名服务器凭证记录92。使用服务器的公共签名密钥40a可以由已签名服务器凭证记录92获知签名事件的情况以及在其过程中使用的数据。服务器凭证记录90可以在之后(甚至多年后)用于证明确实发生了具有给定内容的给定签名事务。例如法院诉讼可能需要这种证明。在这种情况下,可能需要完整的生物统计数据54,因此优选地,服务器凭证记录90中包括完整的生物统计数据集,而不仅仅是简化生物统计数据56、其散列58或可视生物统计数据54a。

[0107] 可以在多个签名者的情况下进行上述过程,当然,当使用生物统计数据采集单元18a记录不止一个用户的生物统计数据54时,对每个生物统计数据54集进行相应的操作,而在服务器端根据所有生物统计数据54集产生可视生物统计数据54a,并且所述可视生物统计数据全部包括在数字签名85中。

[0108] 根据上文的讨论可以理解,本发明与优选简化的一般工程方法相反。通常的工程常识表明,应对生物统计数据和原始文档应用公共数字签名,从而以真实的方式“链接”二者。在这种情况下,只要生物统计和文档是已知的,则可以验证给定的生物统计是否对应于给定文档。然而,如果一个人拥有生物统计,则通过复制生物统计,他可以使用生物统计来产生另一个文档。本发明使这种常规方案更加安全;为了防止生物统计被披露,以加密/简化形式存储和使用生物统计。

[0109] 在现有技术中,仅可以通过被授权用于去除生物统计的加密的可信实体来验证生物统计和文档的对应关系。然而,被视为非信任的实体也可以试图进行验证。根据本发明的方案还允许非信任实体验证文档的真实性(而不将加密的生物统计解密)。

[0110] 因此,根据本发明的方案通过以下方式与简化原则相反:

[0111] 该方案适于产生基于查问的简化生物统计,该简化生物统计包括在使用文档和查问参数两者签名的凭证记录中。已签名凭证记录和简化生物统计可以移交给任何非信任实体,因为由于投影算法的特征所述已签名凭证记录和简化生物统计不能应用于恢复原始生物统计,而简化值对于每个签名都将是独特的,由于简化值仅可以每次使用不同的参数生成(即,即使在相同的生物统计的情况下也不需要应用两个相同的简化图像)。由于已签名凭证记录的真实性的可以由非信任实体验证,所以该实体可以确保合适的生物统计是与给定文档链接的。

[0112] 根据本发明的认证方法还包括上述步骤,其中,上述优选的实施方案的任何一个都适用于该认证方法。在根据本发明的认证方法的过程中:

[0113] -通过通信信道30将包括投影参数52的查问值50从服务器20传送到客户端设备10,

[0114] -连接到客户端设备10的生物统计数据采集单元18a用于应用利用投影参数52的投影来记录简化生物统计数据56,

[0115] -客户端设备10用于通过通信信道30将简化生物统计数据56传送到服务器20,

[0116] -服务器20用于识别客户端设备10的用户,

[0117] -应用包括投影参数52的投影根据用户的生物统计模板45a生成简化生物统计模板验证数据56”,并且通过将简化生物统计数据56与简化生物统计模板验证数据56”比较来进行认证。

[0118] 在优选实施方案中,基于简化生物统计数据56来识别用户。

[0119] 由于在图5和6中可以找到上述步骤,所以没有单独示出该认证方法。该认证方法基于客户端-服务器生物统计数据采集架构,其中,通过连接到客户端或结合在客户端中的生物统计数据采集单元使用服务器发送的查问值来记录简化生物统计数据。

[0120] 生物统计数据采集单元可以例如是平板设备或手机(智能电话)以及在其上运行的软件,即,生物统计数据采集单元内置在客户端中。服务器可以例如是下述中央服务,该中央服务适于基于设备记录的生物统计识别用户,并且适于根据识别的结果准许访问特定服务。所述生物统计可以例如由触摸屏上的手写签名、设备的摄象机拍摄的虹膜图像、设备记录的指纹(只要设备具有必要的能力)或使用设备的摄象机进行的手势识别构成。在该实施方案的情况下,通过在平板上运行的软件方便地执行简化。

[0121] 生物统计数据采集设备可以是“签名板”(具有笔的数字化平板,其也可以具有自己的显示器,基本上与平板设备相同),其通过USB连接器连接到PC。在这种情况下,“服务器”甚至可以是PC本身,运行适于利用记录的手写签名数据的软件应用。在这种情况下,当经由通信链路将数据发送到服务器的是PC时,当然也可以应用远程服务器。在该实施方案中,最有利地,在“签名板”设备内已经进行了数据简化过程,因为在这种情况下,不会从物理封闭且受保护的设备中获得完整的生物统计。

[0122] 生物统计数据采集单元还可以是连接到PC的简单的计算机鼠标。软件应用可以应用于在网页浏览期间记录用户的鼠标移动。可以将鼠标/手的移动视为表征给定个体的生物统计数据。基于所记录的数据,还可以获得用户的心理特征,这甚至可以被应用于显示针对该用户的定制广告。作为替代方案,PC连接的摄象机可以应用于记录用户的眼睛移动(作为生物统计数据)。在这些示例中,数据简化方便地由在PC上运行的软件应用进行。

[0123] 在特定情况下,在签名事件期间可以从签名板设备获得两种类型的信息:

[0124] -简化生物统计(之后将由服务器用于识别人),

[0125] -签名的静态图像(可以可视化地复制到文档,但是不适于在其本身中复制签名生物统计)。

[0126] 这是有利的,因为不能从设备获得关键的生物统计数据,只能获得识别所需的简化信息集,但仍然可以产生签名图像。在这种情况下,查问值将包括:

[0127] -确定识别人所需的简化的参数(或参数集),以及

[0128] -适于将动态生物统计数据简化为静态生物统计数据的另一参数(即,实际上从原始数据集中删除了时间和压力参数,由剩余的一系列点绘制图像,并且优选地将该图像转换为预定大小)。

[0129] 在这种情况下,简化生物统计是两种类型的简化信息的聚合,其中服务器以两种不同的方式使用这两个部分。

[0130] 基于简化生物统计的认证方法具有下述优点,其允许由下述实体/服务进行个人识别:

[0131] -由于法律禁止不允许拥有完整的生物统计数据的实体/服务,或者

[0132] -不处于允许它们保护个人身份的安全级别的实体/服务;或者

[0133] -作为服务提供者,不被待识别的人充分信任的实体/服务。

[0134] 根据本发明的认证方法还适用于构建匿名识别系统,因为适用于身份窃取的生物统计数据不存储在客户端中并且不在系统内传送。在优选实施方案中,可以在商场的商店和走廊内安装多个摄象机。摄象机系统可以收集关于个人的简化面部/身体形状/移动信息,仅将该简化信息传送到服务器。基于该简化信息,服务器尝试辨识该人。在未辨识出该人的情况下,则将其识别为新顾客,对应的生物统计样本(简化数据)与相关联的识别号存储在一起。随后,系统监视该人在购物中心中的移动(他或她进入了哪个商店、他或她在哪个商店橱窗前面停下、他或她在某些位置花费多少时间,他或她在哪个餐馆用餐、他或她购买哪些产品——后者可以是使用收银台摄象机和收银机信息确定的),即,系统可以识别顾客的习惯和偏好。基于先前辨识和识别的人的顾客偏好,该系统能够在任何地方(例如,在动态电视墙上)显示个性化广告。辨识/识别系统允许各个商店在顾客进入商店时向顾客呈现个性化的销售提议。

[0135] 将容易理解本领域技术人员可以想到替代上文详述的实施方案的其他方案,这些方案均落入所附权利要求限定的保护范围。

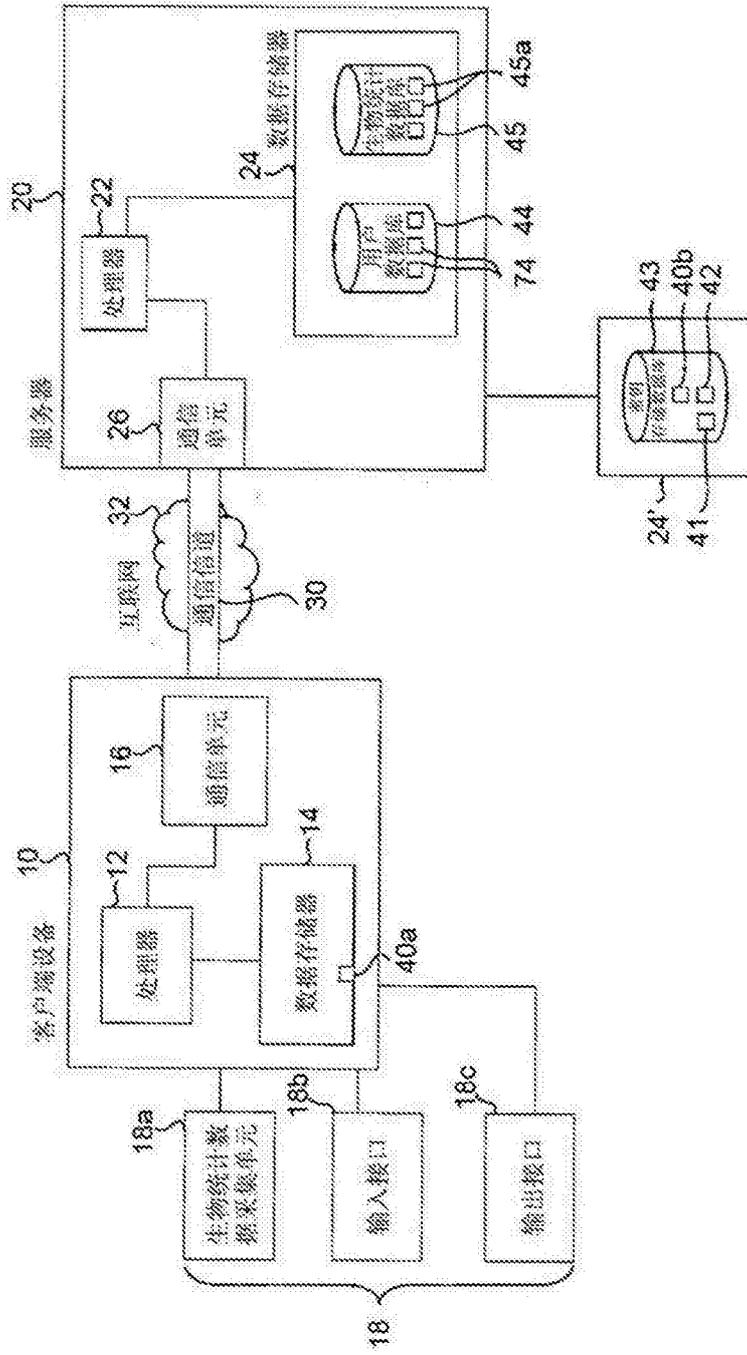


图1

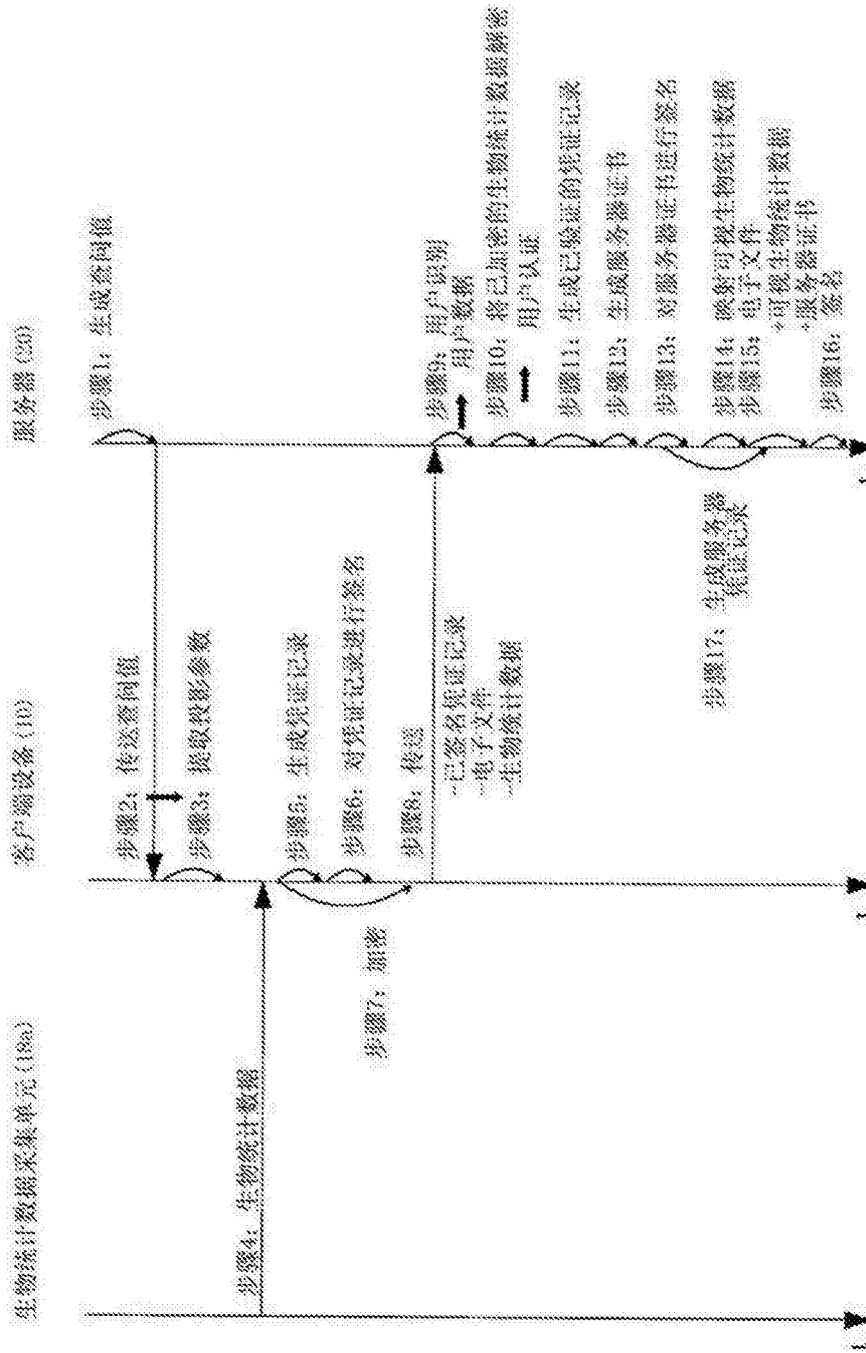


图2

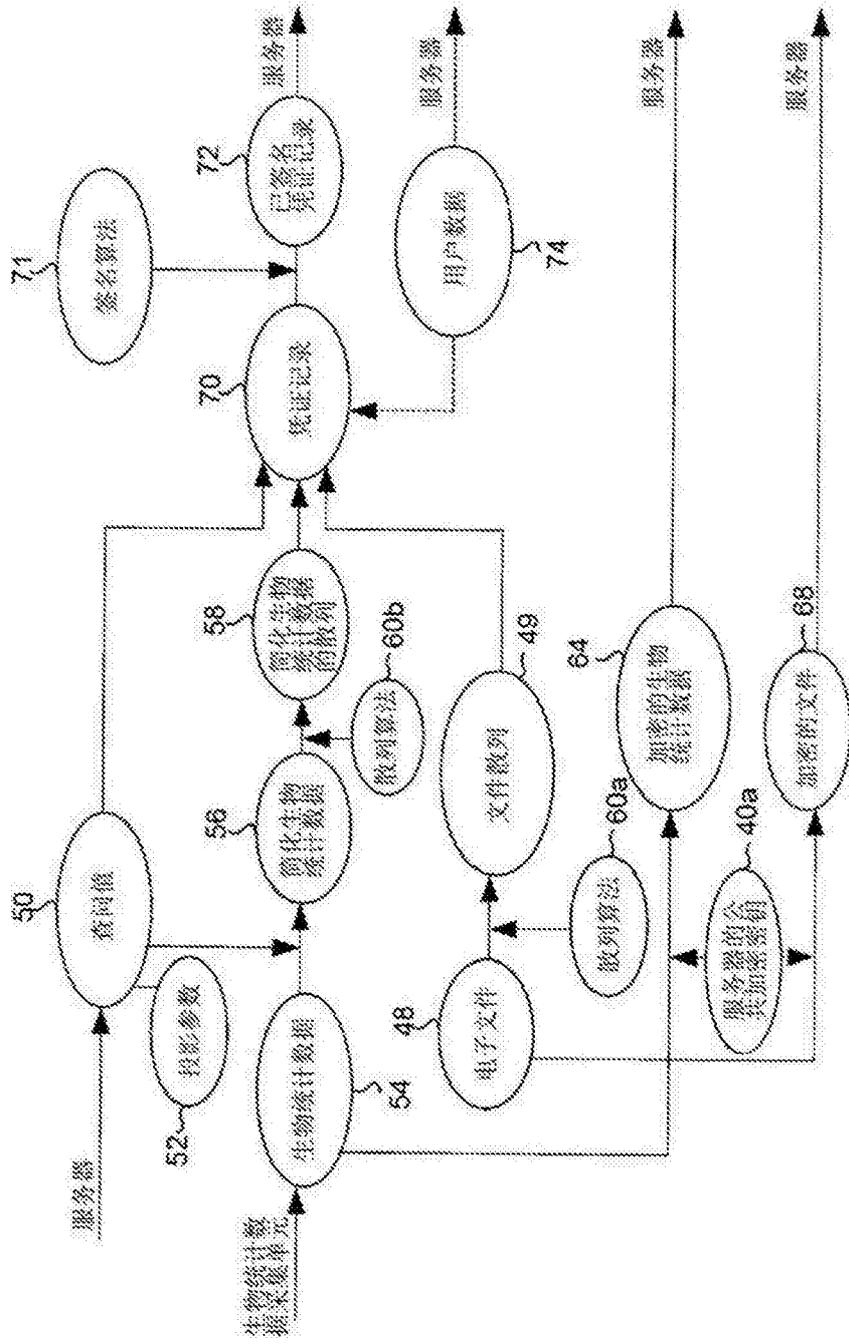


图3

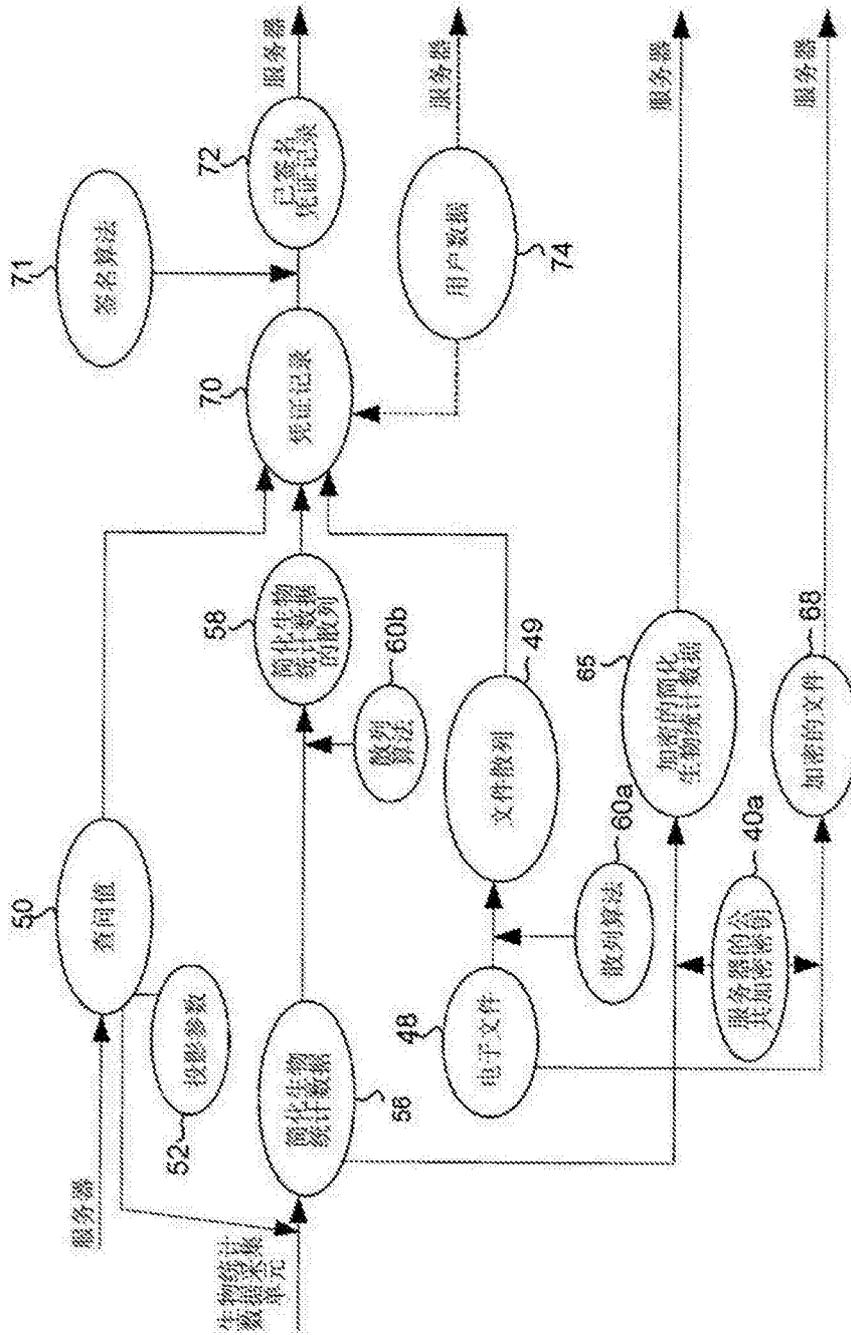


图5

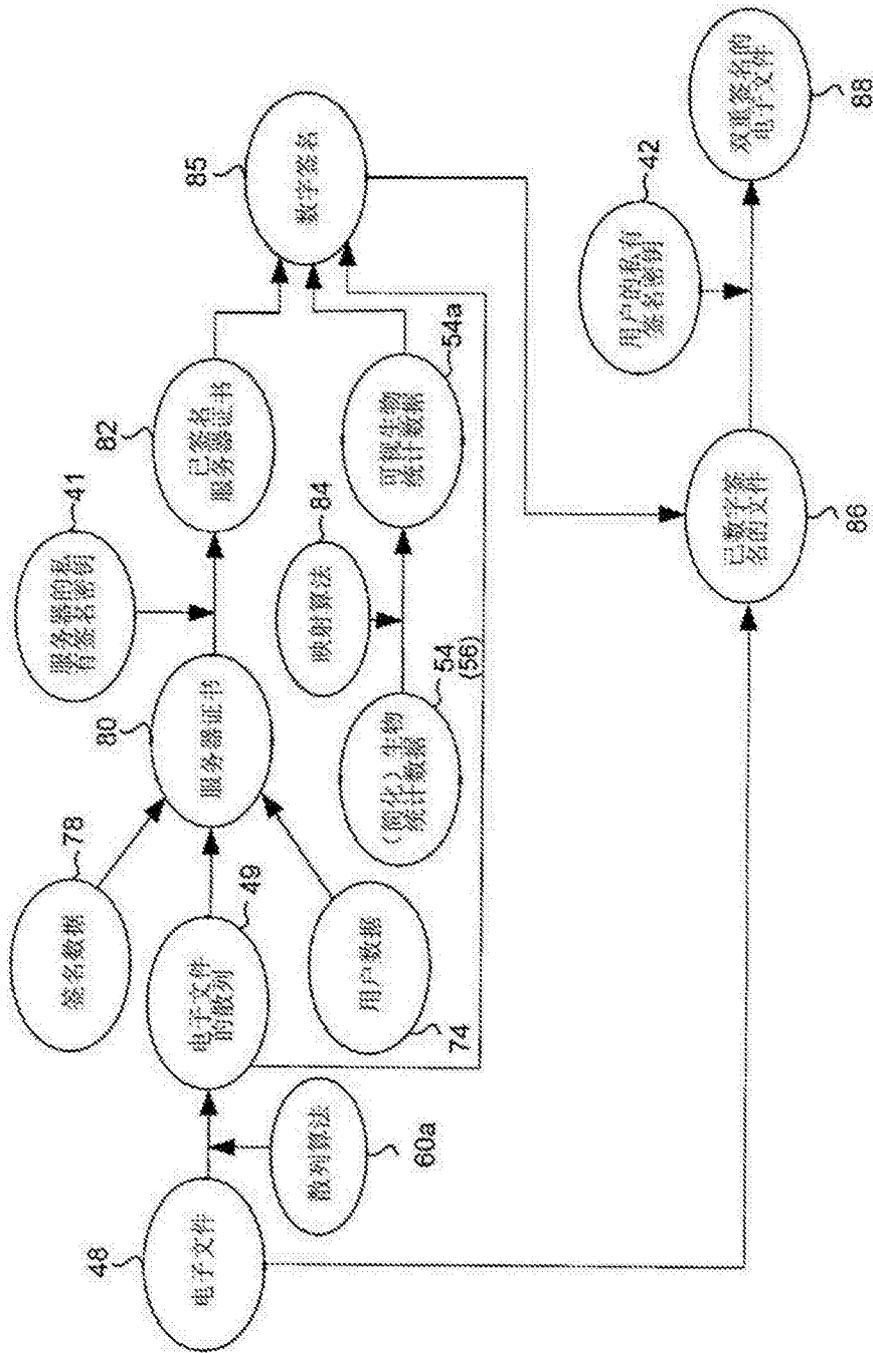


图7

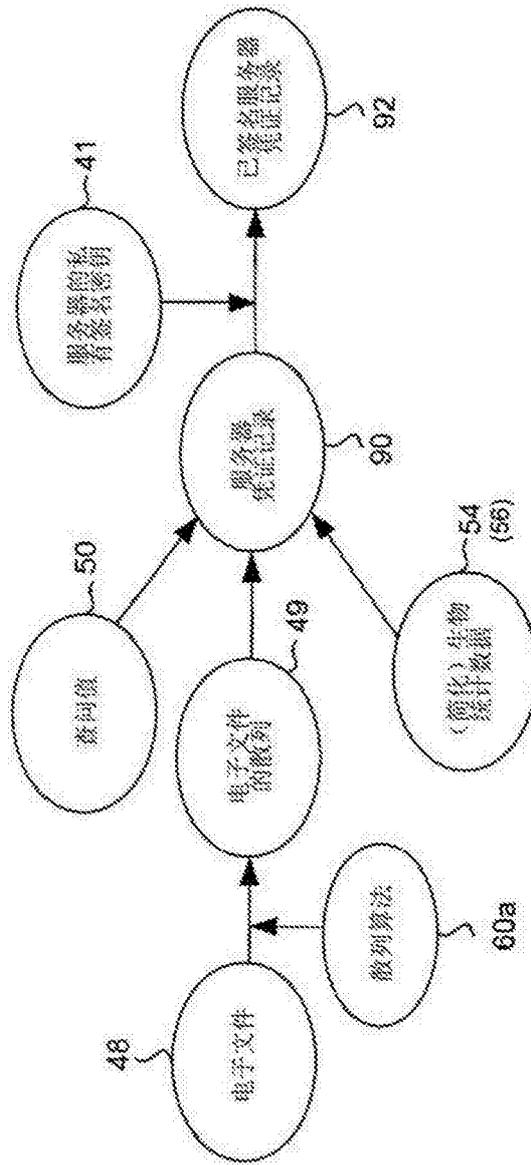


图8