(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104823203 B
(45)授权公告日 2019.03.19

(21)申请号 201480003284.8
(22)申请日 2014.09.16
(65)同一申请的已公布的文献号
申请公布号 CN 104823203 A
(43)申请公布日 2015.08.05
(30)优先权数据
61/878,588 2013.09.16 US
61/902,911 2013.11.12 US
14/454,148 2014.08.07 US
(85)PCT国际申请进入国家阶段日
2015.06.01
(86)PCT国际申请的申请数据
PCT/US2014/055826 2014.09.16
(87)PCT国际申请的公布数据
WO2015/039084 EN 2015.03.19
(73)专利权人 眼验股份有限公司
地址 美国密苏里州
(72)发明人 R·R·德拉赫沙尼
V·格特木库拉 S·K·萨里帕勒
凯西·休利特
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 齐杨
(51)Int.Cl.
G06K 9/00(2006.01)
G06F 21/32(2006.01)
H04L 9/08(2006.01)
(56)对比文件
CN 101369892 A,2009.02.18,
US 2006/0029262 A1,2006.02.09,
US 2007/0217708 A1,2007.09.20,
Mohamed Khalil-Hani.Securing Cryptographic Key with Fuzzy Vault based on a new Chaff Generation Method.《High Performance Computing and Simulation (HPCS),IEEE》.2010,全文.
李芬等.基于Fuzzy Vault的身份认证.《武汉理工大学学报》.2011,第33卷(第3期),第1节.
审查员 刘娟

权利要求书2页 说明书19页 附图5页

(54)发明名称

生物特征模板安全性及密钥产生

(57)摘要

本发明提供用于保护生物特征模板及产生私密密钥的方法及系统。接收一或多个图像。基于所述已接收图像识别兴趣点,且基于所述兴趣点产生多个迷惑数据点。创建并存储基于所述兴趣点及所述迷惑数据点的经迷惑模板。可使用所述模板中的所述迷惑数据点中的至少一者的子集及所述兴趣点编码私密密钥。

CN 104823203 B

1.一种计算机实施方法,其包括:

接收一或多个图像;

基于所述已接收图像识别多个兴趣点,其中每个兴趣点都位于多个相邻图块中的各自的图块中;

基于所述兴趣点产生多个迷惑数据点,其中产生所述迷惑数据点使得所述兴趣点的空间分布和所述迷惑数据点的空间分布实质上与所述相邻图块中的每一者类似;

基于所述兴趣点及所述迷惑数据点创建经迷惑模板;

使用所述迷惑数据点中的至少一者的子集及所述兴趣点来编码密钥,其中所述子集中的每一点是基于所述兴趣点中的不同兴趣点经由不可逆的单向函数来确定的,所述函数以兴趣点为输入并以迷惑数据点或兴趣点为输出;以及

存储所述经迷惑模板。

2.根据权利要求1所述的方法,其进一步包括放弃所述经迷惑模板中的哪些点是所述兴趣点的记录。

3.根据权利要求1所述的方法,其中所述图像包括生物特征图像。

4.根据权利要求3所述的方法,其中所述图像包括眼睛的区域的图像,每一眼睛区域图像包括所述相应眼睛区域的脉管系统的视图,且其中所述兴趣点包括脉管兴趣点。

5.根据权利要求1所述的方法,其进一步包括使一或多个真实描述符与每一兴趣点相关联,其中每一真实描述符描述在所述对应兴趣点周围的一或多个位置。

6.根据权利要求5所述的方法,其进一步包括使一或多个合成描述符与每一迷惑数据点相关联,其中每一合成描述符包括与所述真实描述符的统计相似性。

7.根据权利要求6所述的方法,其进一步包括:

接收一或多个第二图像;

基于所述已接收第二图像识别第二多个兴趣点;

基于所述第二多个兴趣点创建验证模板;

比较所述验证模板与所述经迷惑模板以识别多个匹配兴趣点;以及

基于所述匹配兴趣点认证用户。

8.根据权利要求7所述的方法,其中所述比较包括基于所述真实描述符及所述合成描述符中的一或多者识别所述匹配兴趣点。

9.根据权利要求7所述的方法,其进一步包括减小所述真实描述符及所述合成描述符的维数。

10.根据权利要求9所述的方法,其中所述比较包括基于所述减小维数描述符中的一或多者识别所述匹配兴趣点。

11.根据权利要求7所述的方法,其进一步包括等距地置乱所述真实描述符及所述合成描述符。

12.根据权利要求11所述的方法,其中所述比较包括基于所述经置乱描述符中的一或多者识别所述匹配兴趣点。

13.根据权利要求7所述的方法,其进一步包括基于所述匹配兴趣点的至少一子集来解码密钥。

14.一种包含指令的计算机可读介质,所述指令经由一或多个计算机执行以完成以下

操作：

接收一或多个图像；

基于所述已接收图像识别多个兴趣点，其中每个兴趣点都位于多个相邻图块中的各自的图块中；

基于所述兴趣点产生多个迷惑数据点，其中产生所述迷惑数据点使得所述兴趣点的空间分布和所述迷惑数据点的空间分布实质上与所述相邻图块中的每一者类似；

基于所述兴趣点及所述迷惑数据点创建经迷惑模板；

使用所述迷惑数据点中的至少一者的子集及所述兴趣点来编码密钥，其中所述子集中的每一点是基于所述兴趣点中的不同兴趣点经由不可逆的单向函数来确定的，所述函数以兴趣点为输入并以迷惑数据点或兴趣点为输出；以及

存储所述经迷惑模板。

15.根据权利要求14所述的计算机可读介质，其中所述操作进一步包括放弃所述经迷惑模板中的哪些点是所述兴趣点的记录。

16.根据权利要求14所述的计算机可读介质，其中所述图像包括生物特征图像。

17.根据权利要求16所述的计算机可读介质，其中所述图像包括眼睛的区域的图像，每一眼睛区域图像包括所述相应眼睛区域的脉管系统的视图，且其中所述兴趣点包括脉管兴趣点。

18.根据权利要求14所述的计算机可读介质，其中所述操作进一步包括使一或多个真实描述符与每一兴趣点相关联，其中每一真实描述符描述在所述对应兴趣点周围的一或多个位置。

19.根据权利要求18所述的计算机可读介质，其中所述操作进一步包括使一或多个合成描述符与每一迷惑数据点相关联，其中每一合成描述符包括与所述真实描述符的统计相似性。

20.根据权利要求19所述的计算机可读介质，其中所述操作进一步包括：

接收一或多个第二图像；

基于所述已接收第二图像识别第二多个兴趣点；

基于所述第二多个兴趣点创建验证模板；

比较所述验证模板与所述经迷惑模板以识别多个匹配兴趣点；以及

基于所述匹配兴趣点认证用户。

21.根据权利要求20所述的计算机可读介质，其中所述比较包括基于所述真实描述符及所述合成描述符中的一或多者识别所述匹配兴趣点。

22.根据权利要求20所述的计算机可读介质，其中所述操作进一步包括减小所述真实描述符及所述合成描述符的维数，且其中所述比较包括基于所述减小维数描述符中的一或多者识别所述匹配兴趣点。

23.根据权利要求20所述的计算机可读介质，其中所述操作进一步包括等距地置乱所述真实描述符及所述合成描述符，且其中所述比较包括基于所述经置乱描述符中的一或多者识别所述匹配兴趣点。

24.根据权利要求20所述的计算机可读介质，其中所述操作进一步包括基于所述匹配兴趣点的至少一子集来解码密钥。

生物特征模板安全性及密钥产生

[0001] 对相关申请案的交叉参考

[0002] 本申请案主张2014年8月7日申请且标题是“生物特征模板安全性及密钥产生(Biometric Template Security and Key Generation)”的第14/454,148号美国专利申请案的优先权利,所述申请案主张2013年9月16日申请且标题是“图像检测、认证及信息隐藏(Image Detection,Authentication,and Information Hiding)”的第61/878,588号美国临时专利申请案及2013年11月12日申请且标题是“检测、认证及信息隐藏(Detection,Authentication,and Information Hiding)”的第61/902,911号美国临时专利申请案的优先权利,所述申请案的全部内容是以引用方式并入本文中。

背景技术

[0003] 本发明大体上涉及生物特征认证,且更特定地说,涉及用于保护生物特征模板且使用生物特征模板编码及解码密钥的系统及方法。

[0004] 通常希望将对财产或资源的使用权限于特定个人。生物特征系统可用来认证个人的身份以授予或拒绝授予对资源的使用权。例如,虹膜扫描仪可由生物特征安全性系统使用来基于个人的虹膜中的独特结构识别个人。例如在登记过程期间从个人采集的生物特征数据可被存储作为随后用来验证个人身份的模板。模板可例如远程存储在认证服务器上或本地存储在具有采集生物特征读数的能力的装置(例如具有摄像头的移动电话)上。然而,将模板维持在其原始形式或可借以导出原始模板的形式产生将危及模板安全的风险。

发明内容

[0005] 本发明揭示用于保护生物特征模板且使用生物特征模板编码及解码密钥的系统及方法。一方面,一种计算机实施方法包括:接收一或多个图像;基于所述已接收图像识别多个兴趣点;基于所述兴趣点产生多个迷惑数据点;基于所述兴趣点及所述迷惑数据点创建经迷惑模板;及存储所述经迷惑模板。此方面的其它实施例包含对应系统及计算机程序。

[0006] 在一个实施方案中,产生所述迷惑数据点使得所述兴趣点的空间分布与所述迷惑数据点的空间分布实质上类似。

[0007] 在另一实施方案中,所述方法进一步包括使一或多个真实描述符与每一兴趣点相关联,其中每一真实描述符描述在所述对应兴趣点周围的一或多个位置。

[0008] 在另一实施方案中,所述方法进一步包括放弃所述经迷惑模板中的哪些点是所述兴趣点的记录。

[0009] 在又另一实施方案中,所述方法进一步包括使用所述迷惑数据点中的至少一者的子集及所述兴趣点来编码密钥。可基于所述兴趣点中的不同兴趣点确定所述子集中的每一点。

[0010] 在另一实施方案中,所述图像包括生物特征图像。所述图像可包括眼睛的区域的图像,每一眼睛区域图像包括所述相应眼睛区域的脉管系统的视图。所述兴趣点可包括脉管兴趣点。

[0011] 在一个实施方案中，所述方法进一步包括使一或多个合成描述符与每一迷惑数据点相关联，其中每一合成描述符包括与所述真实描述符的统计相似性。

[0012] 在另一实施方案中，所述方法进一步包括：接收一或多个第二图像；基于所述已接收第二图像识别第二多个兴趣点；基于所述第二多个兴趣点创建验证模板；比较所述验证模板与所述经迷惑生物特征模板以识别多个匹配兴趣点；及基于所述匹配兴趣点认证用户。所述比较可包括基于所述真实描述符及所述合成描述符中的一或多者识别所述匹配兴趣点。

[0013] 在另一实施方案中，所述方法进一步包括减小所述真实描述符及所述合成描述符的维数。所述比较可包含基于所述减小维数描述符中的一或多者识别所述匹配兴趣点。

[0014] 在另一实施方案中，所述方法进一步包括等距地置乱所述真实描述符及所述合成描述符。所述比较可进一步包括基于所述经置乱描述符中的一或多者识别所述匹配兴趣点。

[0015] 在又另一实施方案中，所述方法进一步包括基于所述匹配兴趣点的至少一子集来解码密钥。

[0016] 附图及以下描述中陈述本说明书中描述的标的物的一或多个实施方案的细节。根据描述、图式及权利要求书将明白所述标的物的其它特征、方面及优点。

附图说明

[0017] 在图式中，相似参考字符通常是指不同视图中的相同部分。此外，图式不一定按比例绘制，反而通常强调说明实施方案的原理。在以下描述中，参考以下图式描述各个实施方案，其中：

[0018] 图1描绘根据实施方案的用于生物特征模板安全性及密钥产生的系统的图。

[0019] 图2描绘根据实施方案的用于保护生物特征模板及编码/解码私密密钥的方法。

[0020] 图3描绘具有实例脉管兴趣点的眼睛图像。

[0021] 图4A描绘具有嵌入式迷惑数据点的图3的脉管兴趣点。

[0022] 图4B描绘来自图4A的经迷惑数据点叠加在图3的眼睛图像上。

[0023] 图5描绘具有标记点的子集的图4A的脉管兴趣点及迷惑数据点。

具体实施方式

[0024] 个人的眼白中的可见脉管系统的区别性特征可用来识别或认证个人。例如，可获得及分析用户的眼白的图像以比较眼睛的特征与生物特征模板以认证用户且授予或拒绝授予用户对资源的使用权。2013年2月5日发布且标题是“用于生物特征认证的纹理特征(Texture Features for Biometric Authentication)”的第8,369,595号美国专利及2014年5月9日申请且标题是“用于生物特征认证的特征提取及匹配(Feature Extraction and Matching for Biometric Authentication)的第14/274,385号美国专利申请案”中描述用于成像及图案匹配眼白中的血管且用于特征提取及匹配的解决方案的实施方案，所述专利及专利申请案的全部内容是以引用方式并入本文中。

[0025] 例如，个人的可见脉管系统的独特结构可反映在个人眼白的图像的纹理特征中。图像可经分段以识别眼白上的区域以供纹理分析，且可应用一组筛选器以确定此类区域中

的个人脉管系统的纹理特征的描述符。从筛选器输出导出的描述符的向量可被汇编为描述符向量。接着，在认证或识别操作期间，可比较针对用户确定的描述符向量与来自已登记个人的所存储生物特征记录的对应描述符向量以确定用户与已登记个人之间的匹配的似然率。

[0026] 本文中描述的模板安全性及密钥产生技术的各个实施方案是基于使用极多个或充足数目的“干扰片”或不可区分的噪音元素对生物特征模板的隐写迷惑。在装置特定置乱空间中进行成功验证之后可被识别的干扰片元素的子集被用来求解产生经编码机密的方程组。此类令牌是高熵、可撤销的，且不会显露关于用户的生物学特性的任何信息。

[0027] 图1说明用于产生安全的生物特征模板、执行用户验证及基于生物特征模板编码及解码私密密钥的局部化系统的一个实施方案。用户装置100可包含图像传感器130、处理器140、存储器150、生物特征硬件及/或软件160，及将包含存储器150的各个系统组件耦合到处理器140的系统总线。用户装置100可包含(但不限于)智能电话、智能手表、智能眼镜、平板计算机、便携式计算机、电视机、游戏装置、音乐播放器、移动电话、膝上型计算机、掌上型计算机、智能或非智能终端、网络计算机、个人数字助理、无线装置、信息设备、工作站、迷你计算机、大型计算机或作为可执行本文中描述的功能的通用计算机或专用硬件装置操作的其它计算装置。

[0028] 生物特征硬件及/或软件160包含用于对由图像传感器130采集的图像执行操作的图像处理模块162。例如，图像处理模块162可对用户110的眼睛的图像执行分段及增强以辅助隔离脉管结构。模板安全性模块166基于脉管系统图像创建生物特征模板，且如本文中所述般对模板执行各种迷惑及置乱操作，以增加模板安全性同时维持可用性。验证模块174通过在采集生物特征读数之后形成的生物特征验证模板与先前存储的登记模板之间执行匹配操作来确证用户110的身份。密钥模块178可基于生物特征登记模板来编码用户110的私密密钥，且在使用验证模板成功地验证用户身份之后解码密钥。

[0029] 本文中描述的系统的实施方案可使用适当硬件或软件；例如，系统可在能够运行操作系统的硬件上执行，所述操作系统例如微软Windows®操作系统、Apple OS X®操作系统、AppleiOS®平台、Google Android™平台、Linux®操作系统及UNIX®操作系统的其它变体，等等。系统可包含存储在存储器150中且在处理器140上执行的多个软件处理模块(例如，图像处理模块162、模板安全性模块166、验证模块174及密钥模块178)。举例来说，程序模块可呈一或多个适当的编程语言的形式，其被转换为机器语言或目标代码以允许处理器执行指令。软件可呈用适当的编程语言或框架实施的独立应用程序的形式。

[0030] 此外或替代地，可在云中远程地或经由服务型软件(software-as-a-service)执行一些或全部功能。例如，可在一或多个远程服务器或与用户装置通信的其它装置上执行某些功能(例如图像处理、模板创建、模板匹配等等)。远程功能可在服务器级计算机上执行，服务器级计算机具有足够多的存储器、数据存储装置及处理能力且运行服务器级操作系统(例如，Oracle® Solaris®、GNU/Linux®及Microsoft® Windows®操作系统系列)。例如，服务器与用户装置之间的通信可发生在媒体(例如标准的电话线、LAN或WAN链路(例如，T1、T3、56kb、X.25)、宽频连接(ISDN、帧中继、ATM)、无线链路(802.11(Wi-Fi)、蓝牙、GSM、CDMA等等))上。预期其它通信媒体。网络可携载TCP/IP协议通信，及由网络浏览器作出的HTTP/HTTPS请求，且用户装置与服务器之间的连接可通过此类TCP/IP网络传达。预期其它

通信协议。

[0031] 本文中描述的技术的方法步骤可由执行一或多个计算机程序的一或多个可编程处理器执行以通过对输入数据进行操作及产生输出来执行功能。方法步骤还可由专用逻辑电路(例如FPGA(现场可编程门阵列)或ASIC(专用集成电路))执行,且模块可被实施为所述专用逻辑电路。模块可能是指实施所述功能的计算机程序及/或处理器/特殊电路的部分。

[0032] 适用于执行计算机程序的处理器包含例如通用微处理器及专用微处理器两者。通常,处理器将从只读存储器或随机存取存储器或两者接收指令及数据。计算机的基本元件是用于执行指令的处理器及用于存储指令及数据的一或多个存储器装置。适用于具体体现计算机程序指令及数据的信息载体包含全部形式的非易失性存储器,包含例如半导体存储器装置,例如EPROM、EEPROM及快闪存储器装置;磁盘,例如内部硬盘或可抽换式磁盘;磁-光盘;及CD-ROM及DVD-ROM光盘。一或多个存储器可存储指令,其在由处理器执行时形成本文中描述的模块及其它组件且执行与组件相关联的功能。处理器及存储器可由专用逻辑电路增补或并入专用逻辑电路中。

[0033] 系统还可在分布式计算环境中实践,在分布式计算环境中,由通过通信网络链接的远程处理装置执行任务。在分布式计算环境中,程序模块可位于包含存储器存储装置的本地及远程计算机存储媒体中。取决于装置容量及所需数据处理能力的大小,还可使用除了本文中描述的系统硬件及软件之外的其它类型的系统硬件及软件。系统还可实施于一或多个虚拟机上,所述一或多个虚拟机执行例如上文提及的虚拟化操作系统且在具有例如本文中描述的硬件的一或多个计算机上操作。

[0034] 还应注意,系统及方法的实施方案可被提供作为在一或多个制品上或一或多个制品中具体体现的一或多个计算机可读程序。程序指令可在人工产生的传播信号(例如机器产生的电信号、光学信号或电磁信号)上编码,所述信号经产生以编码信息以传输到适当接收器设备以供数据处理设备执行。计算机存储媒体可为计算机可读存储装置、计算机可读存储衬底、随机或串行存取存储器阵列或装置或其中的一或两者的组合,或包含在其中。此外,虽然计算机存储媒体并非传播信号,但是计算机存储媒体可为编码在人工产生的传播信号中的计算机程序指令的源或目的地。计算机存储媒体还可为一或多个分离物理组件或媒体(例如,多个CD、磁盘或其它存储装置)或包含在其中。

[0035] 参考图2,在一个实施方案中,用于保护生物特征模板的方法开始于接收用户的一只、两只眼睛及/或其一或多个区域的图像(步骤202)。可使用具有图像传感器130的装置100(例如具有前置摄像头的电话或平板计算机)采集图像。如果接收多个图像,那么可基于图像对于生物特征识别的适用性而自动地选择单个图像,或可自动地选择或平均化一些或全部图像以产生单个组合图像(步骤206)。由图像处理模块162以若干标度的蓝-绿色层分段、锐化、增强对比度及/或滤波含有白膜或眼白的图像区域以提供眼白中可见的脉管图案的最优描绘(步骤212)。

[0036] 在步骤218中,基于脉管图案的描绘,模板安全性模块166识别脉管兴趣点且在步骤222中,模块166使每一位置中的一系列图像描述符与对应的脉管兴趣点相关联以为每一兴趣点创建位置-描述符结构。在此阶段处,可放弃眼睛图像(步骤226)。所得的脉管兴趣点集合及其相关局部图像描述符形成基本生物特征模板(步骤230)。如果希望将模板用于登记用户,那么可以如下文描述的既私密又安全的方式将模板本地保存在装置100上(例如,

保存在存储器150中)。

[0037] 为了保护生物特征模板,模板安全性模块166将位置描述符结构“隐藏”在多个已产生的“干扰片”元素内或可类似地结构化且在统计学上与实际脉管兴趣点不可区分的迷惑数据点内(步骤234)。在步骤242中放弃干扰片对非干扰片(即,真实脉管兴趣点)元素的全部记录之前,每一脉管兴趣点“标记”干扰片点(或另一脉管兴趣点)(步骤238)。具体来说,密钥模块178将脉管兴趣点输入到安全的单向函数中,所述单向函数将要标记的干扰片点(或脉管兴趣点)指定作为输出。如下文进一步描述,此类标记点可由密钥模块178使用来吸收且编码长随机密钥的线性投影(步骤250)以及在成功验证用户身份之后解码密钥。

[0038] 此类干扰片代理操作进一步从真实模板元素解耦各种功能(例如替代性生物特征验证及密钥产生)以增加私密性、安全性及可撤销性。模板安全性模块166在步骤246中通过凭借例如统计解除相关及标准化及/或装置特定等距加盐(salting)及尺寸改组对描述符置乱来进一步保护经干扰片迷惑的模板,从而保证不显露生物特征导出的信息(尤其如果被传输远离装置100)。验证模块174可在身份验证期间在此独特的装置特定及置乱空间中执行生物特征模板匹配,从而给本地匹配及密钥产生常式增加另一层安全性、私密性及可撤销性。在步骤254中,将经干扰片迷惑、经置乱描述符模板本地存储在装置上(或在其它实施方案中,远程存储模板)。

[0039] 在用户身份的验证期间,由图像处理模块162实行相同或类似图像采集、分段及增强步骤。类似地,寻找脉管兴趣点且计算其本地描述符,且接着由模板安全性模块166使用登记期间使用的独特装置及软件特定签名置乱其本地描述符(步骤258),从而创建验证模板(步骤262)。此保证登记及验证只可发生在相同装置及软件实例上。在步骤266中,在真实验证成功的情况中,由验证模块174完成于置乱空间中的匹配程序通过比较验证模板与经迷惑模板来识别最少数目的真实脉管兴趣点。已识别的真实脉管兴趣点继而又显露早期在登记程序中标记的携带信息的干扰片点的足够大的子集(步骤268)。真实点及因此标记干扰片点的此最少数目与密钥编码方程组的次数相同。密钥模块178可接着使用来自标记干扰片点的信息以求解方程组且获得解密密钥(步骤272)。在一个实施方案中,密钥是稳定的、512位长且具有至少64位的熵。

[0040] 应明白,虽然本文中呈现的各种系统及方法利用由可见脉管系统导出的生物特征眼睛图像及兴趣点,但是预期所揭示技术的其它实施方案及应用。例如,在其它实施方案中,在其它生物特征图像数据(例如指纹或脸部扫描)中识别特征及/或兴趣点。可执行类似成像处理过程以增强且隔离图像中的有趣的特征/点,且一旦识别特征/点,可应用与本文描述相同或实质上类似的迷惑、置乱、验证及/或密钥编码/解码技术。应进一步注意,本文中呈现的各种系统及方法无需结合生物特征成像及认证使用。相反地,本文中揭示的技术同样可适用于其它类型的图像、视频帧等等。

[0041] 登记

[0042] 图像采集

[0043] 在一个实施方案中,用图像传感器以适用于本文中描述的图像处理功能的图像质量(例如720p、1080p或等效/更高分辨率)采集一或多个眼睛图像(及/或眼睛区域图像)。图像传感器可为例如1百万像素或更好的图像传感器,例如通常在蜂窝电话及平板计算机中找到的前置摄像头。可使用例如维奥拉-琼斯(Viola-Jones)方法检测用户的眼睛,且可检

测用户的视线方向，所述检测全部是实时的。在检测到稳定的视线及至少一只眼睛之后，采集用户的眼睛的图像堆叠。

[0044] 平均化来自输入堆叠的空间配准图像以降低传感器噪音，且使用无参考图像质量度量选择最佳所得平均化截图。在低或无光状况下，装置屏幕的背光加上归因于前述平均化的多帧减噪使得能够实行本文中描述的生物特征处理操作。在一个实例中，实时配准且平均化不超过可接受方差大小(归因于运动及眨眼)的多个连续图像帧(例如，3个、4个、5个或更多个)。可使用基于高斯-拉普拉斯(LoG)的质量度量(锐化图像减去原始图像的标准偏差)对图像堆叠排名，且保留前n个以供进一步处理(例如，多达两个用于验证，多达四到六个用于登记)。

[0045] 分段及增强

[0046] 在图像采集(及平均化(如果执行))之后，可对选定图像进行色彩处理以在绿色-蓝色光谱中更好地显露血管，且将选定图像分段以描绘眼白部分，此后称作兴趣区域(ROI)。在一个实施方案中，通过将多个圆锥截面曲线拟合到眼睑及角膜缘边界来分段图像。检查分段有效性(例如，遮罩应为ROI的边界框的至少40％)。一系列脉管增强图像滤波、锐化及自适应性对比度操作提供更特定生物特征模板所需的改善图像。例如，可使用LoG乘以原始图像的对比度受限自适应直方图均衡化(CLAHE)以及均匀伽柏(Gabor)滤波器的经特殊调谐组来增强图像的绿色(无红色)层。接着可在下一步骤使用经增强图像的一系列多标度及经特殊滤波调适。

[0047] 兴趣点检测及特征提取

[0048] 对于每一ROI，识别兴趣点的位置(x_i,y_i)，数目通常取决于图像质量在100到400之间变化。图3描绘具有眼睛300的脉管系统315的已识别兴趣点320的实例眼睛图像。兴趣点320可使用例如2014年5月9日申请且标题是“用于生物特征认证的特征提取及匹配(Feature Extraction and Matching for Biometric Authentication)”的第14/274,385号美国申请案中描述的脉管点检测器识别，所述申请案的全部内容是以引用方式并入本文中。检测兴趣点的其它方式是可能的。

[0049] 接着，计算以统计学(但是并非确切或唯一地)描述脉管兴趣点位置(x_i,y_i)周围的局部图像片的$\vec{V}_i^1,\vec{V}_i^2,\ldots\vec{V}_i^d$描述符向量集合。图像片描述符实例包含(但不限于)快速鲁棒性特征(SURF)、多半径扩展图案局部二进制图案(的直方图)(H LBP)及多半径扩展图案中心对称局部二进制图案(的直方图)(H CS LBP)。对于每一ROI，包含已检测的脉管兴趣点VPD的朴素(不受保护)生物特征模板T_{VPD}接着被定义为：

[0050] $$T_{VPD}=\{t_i\},\ t_i=\left[(x_i,y_i),\vec{V}_i^1,\vec{V}_i^2,\ldots\vec{V}_i^d\right],\ i=1、2、\ldots\ldots、n(T_{VPD})$$

[0051] 在验证时，将用于所主张身份的所存储登记模板与所呈现的验证模板匹配。在一个实施方案中，如果相似度分数高于预设阈值(还必须配对跨登记及验证模板的某个最小数目的元素)，那么接受主张人的主张且发布匹配决定。注意，可在创建模板之后立即放弃眼睛图像，且只存储登记模板。

[0052] 迷惑及编码

[0053] 干扰片点添加及标记

[0054] 在一个实施方案中，保护生物特征模板的初始步骤包含将来自T_{VPD}的要存储的登

记模板元素隐藏在看上去相同或实质上类似于真实脉管兴趣点的大量人工合成元素之中。此类合成元素在本文中称作“干扰片”。在一个实施方案中，干扰片的数目逼近真实模板元素的数目n(T_{VPD})的3到7倍。然而，预期其它倍数。例如，更高的干扰片密度可提供更高等级的迷惑，不过是以增加计算涉及面(footprint)为代价的。

[0055] 干扰片元素可通过以下算法插入：保证所有数据点(干扰片及非干扰片(即，实际脉管兴趣点))的空间分布是均匀的或遵循与脉管兴趣点相同或实质上类似图案或分布。在一个实例中，直到给定区域颗粒或图块，(x_i,y_i)的局部空间密度大约相同，且描述符内容或空间关系并未将空间粒度内的干扰片与真实非干扰片(实际脉管兴趣点)区分开来。图4A描绘针对适当3x干扰片对非干扰片放置的来自图3的脉管兴趣点(圆形)在干扰片点(正方形)内的嵌入。图4B是来自图4A的迷惑点叠加在来自图3的原始眼睛图像上的视觉化。然而，应注意，可在此迷惑阶段之前且在计算T_{VPD}之后立即放弃眼睛图像。

[0056] 每一模板点t_i(无论是否真实(脉管兴趣点)或合成(干扰片))可包含两种类型的信息：位置(x,y)及片统计数据V。用于干扰片数据点的不可区分性的注入干扰片的模板的空间均匀性可通过若干方式实现。在一个实施方案中，使用以下两步干扰片(x,y)位置产生过程。在步骤1(粗略干扰片放置)中：鉴于登记模板的空间跨度内的典型图块化(例如，4x5)，开始于放置均衡每个图块的总模板点(干扰片及非干扰片)的平均值(大于任何图块中的VPD点的最大数目的目标数)所需的干扰片的第一部分。继续直到达到每个图块具有约50％的脉管兴趣点VPD+干扰片点密度目标为止。对此粗略加干扰片步骤使用所有数据点(干扰片或脉管兴趣点)间的初始最小距离要求(例如三个像素)。在步骤2(精细干扰片放置)中：继续插入干扰片的剩余部分，减小最小距离阈值(例如，减小到1个像素)直到实现每个图块具有100％的所需均匀脉管兴趣点VPD+干扰片点密度目标为止。

[0057] 在一个实施方案中，由1.2MP摄像头创建的数据点位置的(x,y)范围的下端是大约80x100个像素+/-20。然而，应注意，此数目可基于摄像头的视野、物距及其它因素而改变。下文在标题是“样本干扰片产生及标记函数实施方案(Sample chaff Generation and Tagging Function Implementations)”的章节中描述此方法及其它替代方法的细节。

[0058] 在干扰片放置之后，干扰片描述符向量$\vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d$经合成以类似于与真实脉管兴趣点VPD相关联的描述符。即，被指派给干扰片点的描述符的内容经形成以统计上类似且与针对真实兴趣点VPD导出的描述符的内容不可区分。干扰片描述符与真实脉管描述符的前述不可区分性可以各种方式实现。在一个实施方案中，为了在登记期间产生各种干扰片描述符，应用小的随机循环移位及相加噪声于真实脉管描述符以取得遵循与其真实对应物相同的统计分布的干扰片描述符。如下文描述，此类特征可随后被“置乱”。

[0059] 当创建登记模板时，干扰片点及其合成描述符被结构化为模板的真实VPD横跨部分：

[0060] $$T_{CHF} = \{t_i\},\ t_i = \left[(x_i, y_i), \vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d\right],\ i=1、2\ldots\ldots、n(T_{CHF})$$

[0061] 注入干扰片的经迷惑模板因此呈由下式给出的(无序)集合的形式：

[0062] $T_A = T_{VPD} \cup T_{CHF}$

[0063] “标记”函数是一个模板元素到另一者的单向映射。具体来说，鉴于来自经干扰片迷惑模板的任何其它数据点，标记函数可用来寻找或“标记”所述模板中的模板点。在一个

实施方案中，标记函数f_T满足以下性质：(1)其域含有$\{[(x_i,y_i),\vec{V}_i^1,\vec{V}_i^2,\ldots\vec{V}_i^d]\}$；(2)其是非平凡的且多对一(或以其它方式不可逆或无已知或实际倒数)(例如，基于SHA512散列函数，其可用于置乱及编码/解码状态以及用于标记)；及(3)在给出登记模板内，范围最小程度地与脉管兴趣点的集合相交(即，模板的脉管兴趣点子集内存在最少的自标记)：

[0064] $$\frac{n(f_T(VPD)\cap VPD)}{n(VPD)}\ll 1$$

[0065] 标题是“样本干扰片产生及标记函数实施方案(Sample Chaff Generation and Tagging Function Implementations)”的章节中描述此类函数的当前及替代实施方案。鉴于模板的VPD部分的标称值，此类标记函数通常针对其输入处的每一脉管兴趣点标记其输出处的大约一个点。在一个实施方案中，标记函数可用来标记干扰片的密钥编码子集(参见下文)及干扰片的携带信任服务器签名的子集(参见下文的“信任服务器功能”)。此类两个标记函数可包含其范围的小重叠。

[0066] 例如本文中描述的标记函数f_K可用来寻找模板的真实T_{VPD}部分映射到的模板点T_K(鉴于标记函数的第三性质，大部分为干扰片)，使得$T_K=f_K(T_{VPD})$。图5描绘具有标记点的子集(实心圆及正方形)的来自图4A的真实点(圆形)及迷惑点(正方形)。视情况，可使用在设计或元数据参数方面不同于f_K的第二标记函数f_S来标记模板的另一类似(但并不相同)子集以产生$T_S=f_S(T_{VPD})$，其可用于可选的信任服务器功能。

[0067] T_K可接着用来编码私密密钥。注意，T_{VPD}只有在登记过程期间及其在T_{CHF}中的迷惑之前才已知。不保留的T_{VPD}的记录且在成功的真实生物特征验证期间只显露T_{VPD}的子集。

[0068] 置乱描述符

[0069] 在一个实施方案中，为了减小维数、改善匹配的准确度及速度且为了解除相关且因此进一步“平坦化”且加强经干扰片迷惑的登记模板的均匀性，使用大的代表性训练集合预计算用于不同特征向量$\{\vec{V}_i^1,\vec{V}_i^2,\ldots\vec{V}_i^d\}$，i＝1、2、……n($T_A$)的主分量分析(PCA)投影的负载且加以存储。接着，注入干扰片的模板中的描述符被减小到其原始长度的一部分(例如大约30％)，同时使用斯克里(Scree)图表分析保持其原始已解释变化的大部分(例如大于80％)。在平均值减法之后对PCA投影的可选方差标准化创建白化的存储模板，其具有跨所有其特征的对角线标准化协方差矩阵。鉴于PCA的性质，结果保留了进行匹配所需的大部分欧几里得距离信息。最后，置乱过程可使用不同软件及装置硬件签名的散列值以为以下过程提供种子：(a)加盐过程，以使用添加给所有描述符的SHA512导出偏差向量更改PCA缩短特征(用于登记及验证模板两者，且在保存用于登记模板之前)，及(b)所得特征向量的座标的种子调制再排序(在保存用于登记模板之前)。

[0070] 注意，除了有损PCA投影之外，(a)及(b)两者均保留欧几里得距离，从而使得匹配能够在关联到用户的装置的置乱空间中进行。此是特别显著的属性，因为等距(距离保留)及可撤销替代空间中的匹配对于安全及私密生物特征图案匹配至关重要，且造成双重认证，因为前述生物特征认证的成功将需要所述装置及真实用户两者。不但匹配期间无须解扰描述符(且因此避免曝露风险)，而且独特的软件可撤销及装置特定置乱空间可横跨生物特征认证应用程序的每一次安装。

[0071] 密钥编码

[0072] 现在将描述用于密钥产生(即,将私密密钥计算为生物特征匹配的副产物)的扩增模板结构的一个实施方案。假设存在k次线性方程组,其系数被认为是私密数值$\vec{S}$,$\dim(\vec{S}) = k$)。在验证期间,k是真实用户的登记与验证模板之间的成功匹配过程期间找到的脉管兴趣点的最小数目,所述匹配过程以经验0%错误接受率(FAR)阈值操作(即,不承认使用最大可用生物特征目视读取数据集的任何冒充者的决定阈值)。线性方程组可用来编码密钥,因为求解所述密钥无需数据点的有序集合(鉴于眼睛静脉图案匹配的高敏感度及特殊性(起因于其错综复杂且高熵结构),所述密钥可直接编码到确切求解的线性方程组中)。

[0073] 因此,需要数据点集合D＝{d_i},n(D)≥k来唯一地求解线性方程组以检索可由成功的真实性验证实现的已编码私密数值向量$\vec{S}$,从而导致恢复求解组成密钥的k个未知数所需的k个方程(为了进一步加强密钥位序列流的标准长度及强度,可应用SHA512于此密钥的运算版本以具有模式不可预测的512位私密密钥序列)。注意,经恢复匹配点及因此方程式的次数无关紧要。密钥产生信息分散在经干扰片迷惑登记模板的扩增(具有用于函数拟合的描述符投影值)元素的子集内,此后称作T_{AK}且定义为:

[0074] $$T_{AK} = \{t_i\},\ t_i = \left[(x_i, y_i), \vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d, \vec{Y}_i^1, \vec{Y}_i^2, \ldots \vec{Y}_i^d\right],\ i=1、2、\ldots\ldots n(T_A)$$

[0075] 其中(x_i,y_i)是T_A中的兴趣及干扰片点i的位置。模板的扩增部分是$\vec{Y}_i^1, \vec{Y}_i^2, \ldots \vec{Y}_i^d$,其是维数类似于$\vec{V}_i^1, \vec{V}_i^2, \ldots \vec{V}_i^d$的向量集合,但是Y的每一元素是使用k路向量化函数(参见下文"向量化函数")且然后使用具有$\vec{S}$的内积运算的对应元素从V的投影,从而提供较早提及的方程组的右端(注意$\vec{V}$的每一元素编码不同的$\vec{S}$)。当由真实用户成功进行生物特征认证之后,随后检索私密向量$\vec{S}$(的集合)。前述过程是通过以下编码及解码步骤加以描述,所述编码及解码步骤是由标记及向量化函数实现以增强安全性及私密性,并同时维持数值稳定性。

[0076] 编码过程

[0077] 在一个实施方案中,密钥产生功能是基于成功的真实性接受(真实肯定验证)在登记模板与验证模板之间产生至少k个匹配点,即使被不可区分干扰片迷惑也是如此。因此,如果在此匹配过程之后建立具有k个未知数的k个方程的方程组(其中方程的k个数据点实际上只可通过成功的真实匹配而得知),那么只有发生真实匹配方可唯一地求解方程及因此所述密钥。

[0078] 注意k是图像质量及匹配器强度的函数,且可随着图像质量或匹配器强度的改善而增加,或通过用多个登记模板中的相同编码密钥匹配多个ROI/模板(来自登记及验证组)且在求解方程以恢复私密密钥之前采取已发现标记点的并集而增加。

[0079] 在一个实例中,鉴于以经验FAR＝0阈值对收集的数据集的观察,对于单一扫视、单一比较、2-ROI匹配来说,k＝40。匹配点是在通过其描述符的接近性与其对应验证对应物比较且使用具有仿射变换假设(或类似假设)的随机样本一致性(RANSAC)排斥异常值之后选择的模板条目。如果此类匹配模板条目的数目是k或更高(即,所产生或释放的机密在观察

界限内的阈值下对于每一解锁用户来说是唯一的)，那么不会发生错误接受。对于较为不敏感的应用程序，如果假设匹配器没有被破坏或盗用，那么可使用更小的k来减小密钥产生错误排斥率，假设鉴于匹配器正在排斥请求，密钥产生阶段处将不会进行错误接受事件(即，在其中匹配分数指示匹配，同时匹配点的数目稍微小于k的情况中，假设匹配分数具有高于匹配的多个点的敏感度及特殊性)。

[0080] 继续密钥产生，当创建经干扰片迷惑模板时，产生$T_A = T_{VPD} \cup T_{CHF}$($T_{VPD}$、$T_S$及$T_K$之间可存在少量重叠)。$T_K$的干扰片子集(由$f_K(T_{VPD})$标记)被提供给使用$T_K$的内容及线性方程组编码一或多个(随机)私密密钥$\vec{S}$的函数(例如，线性投影)。假设来自VPD子集的每一标记脉管元素存在(大约)一个标记点$t_i \in T_K$，i＝1、2、……、n(VPD)。因为对于所有不同的描述符集合(例如，SURF、LBP的直方图等等)，密钥编码过程可类似，所以可针对一个泛用类型的此类特征表明所述过程。

[0081] 假设$T_A = T_{VPD} \cup T_{CHF}$的简化但尚未扩增形式(使用单一类型的描述符且注入干扰片)T如下所示：

[0082] $$T = \{t_i\},\ t_i = [(x_i, y_i), \vec{V}_i]$$

[0083] 如果V_i的维数是D，那么可如下将由D×k个数字组成的任何密钥矩阵W(真实或不真实，其中每一行可被视为不同密钥向量$\vec{S}$)编码为私密密钥的矩阵$W_{D\times K} = [W_{jd}]$。T_A中的特征向量V_i的VPD子集的每一标量元素$v_{i,d}$(d＝1、2、……、D，i＝1、2、……、n(T))是使用不明显且不可逆的向量化函数向量化(分裂)为k个特定值。向量化(分裂器)函数因此执行下式：

[0084] $$\vec{X} = \vec{\varphi}(x)、\ \dim(x) = 1、\ \dim(\vec{X}) = k$$

[0085] 无向量化函数的简化版本(其中最大维数D的密钥向量直接编码为每一$\vec{V}_i$的线性组合，假设D≥k(且因此每一扩增$\vec{V}_i$具有一个Y_i，而不是D))也是可能的。然而，解码过程的k并列$\vec{V}_i$的矩阵不应为奇异的。

[0086] 最后，对应的$y_{i,d}$通过下式关联于且被添加到编码$\vec{W}_d$的输入$v_{i,d}$(私密密钥矩阵W的行d具有k的长度)：

[0087] $$y_{d,i} = f_{encode}(\vec{W}_d, v_{d,i}) = \vec{W}_d \cdot \varphi(v_{d,i})$$

[0088] 对所有D尺寸的描述符/密钥集合$\vec{V}_i$、$\vec{W}_d$及用于密钥产生的模板的所有n(T_K)个标记为f_K的元素重复前述序列以得到$\vec{Y}_i$扩增的T_K：$\{[(x_i, y_i), \vec{V}_i, \vec{Y}_i]\}$。接着(通过添加小噪声最低程度地)变更W以达到$W_c$，且对模板的没有标记为$f_K$的部分作出类似应用以得到完全$\{y_{i,d}\}$扩增的T，使得其分量(包含$y_{i,d}$)跨标记、未标记、干扰片及脉管元素完全混合在一起。可产生多个伪造W'，其各自应用于T_{AK}的子集(为了增加的安全性建议的具有n(T_{VPD})个元素的子集)。

[0089] 注意上述过程是不可逆的，即，给定了$y_{i,d}$，上述过程不能恢复到$v_{i,d}$及$\vec{W}_d$(首先，

$\vec{\varphi}(x)$及$y_{d,i}$的计算是多对一函数且不可逆，且进一步来说，在肯定的真实验证之前，并不知道T_{AK}的哪个子集含有用于求解其的经标记且因此W编码数据)。

[0090] 在一个观察实例中，在具有k＝40的阈值(单一扫视、单一比较、2个ROI)的数据集内，不能产生错误接受。即，在观察限制内，没有任何两个不同的用户产生相同密钥，且因此熵看起来相等于密钥长度。然而，此并未暗示对于用户的更大数据库，k＝40不能发生冲突(错误接受)，在所述情况下，可仅仅增加k(但鉴于更高阈值，代价是可能更高的错误排斥率)。至于经验错误接受率估算，使用地球的所有70亿人口，可以经验保证大约仅达36位的生物特征密钥空间的唯一性($\log_2(7\times10e9)=36.03$)。鉴于上文，在k的某个任意严格阈值下，$T_{AK}$的干扰片引发迷惑的程度将最终构成对密钥熵的限制。

[0091] 可以多种不同方式改变、替换或撤销编码密钥，从改变W或对应$\{Y_i\}$的内容到改变向量化函数。标记函数及干扰片内容也可加以改变以实现前述。此类方法中的一些方法在登记时是可适用的，而其它方法在任何时间均可应用。例如，在任何时间，可通过扰乱跨i的$y_{d,i}$的至少$n(T_K)-k+1$个元素(例如，通过将小噪声向量添加到$\{Y_i\}$的所有第d个元素)以私密、安全且方便的方式撤销或改变每一向量密钥$\vec{W}_d$。此改变解$\vec{W}_d$且不显示其新的或旧的内容，这可只有在发现通过真实用户的成功验证可作出的T_k的至少k个元素才可得知。在多个登记模板及ROI的情况中，可在每一模板中编码相同密钥W使得来自最佳/组合比较的释放密钥保持相同。注意因为标记的模板元素在此类登记中是不同的，所以对应的$\{V_i,Y_i\}$也将是不同的，且不存在起因于比较多个模板与相同编码W的攻击向量。

[0092] 验证及解码

[0093] 在一个实施方案中，生物特征验证开始于以与如上文关于登记过程描述的方式相同或实质上相同的方式进行的图像采集、分段及增强、兴趣点检测及特征提取以及描述符置乱。另一方面，添加及标记干扰片及密钥编码只应用于登记过程。

[0094] 匹配

[0095] 在匹配期间，可通过匹配登记模板与相同置乱空间中的验证模板来验证如由所存储的登记模板表示的所声称身份。如果成功，那么由于肯定的真实匹配，准确地发现来自登记模板的至少k个脉管兴趣点。此实现密钥解码过程，其是密钥编码的逆运算但是类似于密钥编码。解码使得具有k或更大的基数的已发现T_{AK}子集能够计算W。

[0096] 为了缓和跨模板攻击，当狡猾的攻击者盗用装置、其代码及逻辑且取得对多个登记模板的使用权并试图交叉匹配所述多个登记模板时，可通过跨不同模板在彼此的匹配距离(或当合成各自被添加到登记模板的干扰片描述符时，先前模板的任何显著部分)内具有干扰片内容而挫败攻击。

[0097] 简单地如下描述模板匹配算法的一个实施方案。(1)对多标度匹配过程形成图像金字塔。(2)使用脉管点检测器寻找兴趣点。(3)使用前述点周围的多半径LBP(局部二进制图案)、多半径CS-LBP(中心对称LBP)、SURF、H-LBP(LBP的直方图)及H-CS-LBP(CS-LBP的直方图)计算特征。结果被保存为朴素登记模板((x,y)脉管点座标的集合加上用于所述座标周围的图像片的描述符向量，如上所述)。(4)使用预计算的PCA负载缩短描述符且使描述符解除相关，且等距地置乱描述符(装置特定加盐及尺寸改组)。在此代理私密空间中执行匹配。(5)基于登记验证点对周围的所有描述符的欧几里得距离使用加权求和寻找登记模板

点与验证模板点之间的最近相邻匹配。候选对被传递到以下异常值排斥步骤。(6)执行具有仿射/非反射相似度假设的RANSAC以在假设的几何变换假设下寻找异常值以及相关变换矩阵。(7)最后匹配分数被发现是排除异常值的登记-验证匹配对的x及y座标、已发现对的数目(k)及来自RANSAC的经恢复标度及旋转(或变换矩阵与合理值以外的单位的其它度量总结偏差)的非线性函数。

[0098] 密钥解码

[0099] 在一个实施方案中,首先匹配验证模板与扩增及迷惑登记模板以在成功的真实匹配之后寻找T_{VPD}的k个或更多个成员。当对每一生物特征交易使用多个ROI或登记/验证模板时,用于命中k个或更高的匹配点的第一次比较可用于计算已编码的W。还可采取通过此类多次比较发现的已标记的扩增登记元素的并集以实现更高的k。

[0100] 接着,使用标记函数f_k,识别来自T_K的k个或更多个点。通过设计,此类点是在W编码函数f_{encode}上。所得方程组的确切解只需要k个点,因此可使用来自成功验证过程的第一个k(或已恢复的T_K的任何其它k个成员)。对于前文提及的T_K的k个成员中的每一者,使用下文在"向量化函数"中描述的相同向量化(分裂器)函数将相应$v_{i,d}$向量化为k个分量。沿着其对应$Y_d=[y_{i,d}]$,k路向量化的$v_{i,d}$(i=1、2、……、k)具有足够多的信息来如下寻找其对应的编码密钥$\vec{W}_d(w_{i,d},\ i=1、2、\ldots\ldots、k)$:对于每一行d,$v_{i,d}$的k个样本(迭代遍历i=1、2、……、k)通过以上向量化函数φ分裂为k路,从而产生$[\varphi]_{k\times k}$。接着使用编码事实寻找密钥向量$\vec{W}_d$:

[0101] $$[\varphi]_{k\times k}\,[w_d]_{k\times 1}=Y_d$$

[0102] 且因此:

[0103] $$[w_d]_{k\times 1}=[\varphi]^{-1}_{k\times k}\,Y_d$$

[0104] 此外,注意,因为k个数据点用于方程式求解,所以顺序无关紧要,且具有k的基数的T_K的任何子集将已经足够。使用上述简化版本进行的解码遵循类似逻辑,但是没有向量化函数。

[0105] 现在将描述初始安全分析。下文假设其中模板被破译且生物特征认证码被解译的盗用装置。鉴于携带干扰片T_K(具有大约n(T_{VPD})个成员)的私密密钥与模板元素的剩余部分不可区分,抽检显示T_K的成员的几率是n(T_K)/n(T_A)。用于猜测所有所需k个点的暴力攻击考虑此类猜测的独立且相似分布的本质以求解方程组,假设被盗且未加密的登记模板及过程逻辑加上是否成功的衡量的可用性接着是大约$\left(\frac{n(T_K)}{n(T_A)}\right)^k$,因为:

[0106]

$$P(guess_1\in T_K, guess_2\in T_K, \ldots guess_k\in T_K)=\prod_{i=1}^{k}\frac{n(T_K)-i}{n(T_A)-i}<\left(\frac{n(T_K)}{n(T_A)}\right)^k$$

[0107] 因此,有效熵可被计算为:

[0108] $$Entropy = -k\log_2\left(\frac{n(T_K)}{n(T_A)}\right)$$

[0109] 作为实例，由于k＝40个最小真实匹配点且典型的干扰片数目与总模板点比率是1/5(每个脉管兴趣点大约4个干扰片点)，熵大于92个位。

[0110] 注意，方程组的容量(即，密钥W的大小)是D×k×L个位，其中L是用来编码W的数字方程组的长度(以位为单位)。例如，只使用SURF-128特征(SURF的128维版本)且使用无符号64位整数格式来表示W(放弃LSB之后的63个有效位缓和四舍五入错误)，密钥容量(长度)是128×36×63＝290,304位，或大约35KB。然而，如早期计算，此并非方程组的熵。为了加强密钥序列流的标准长度及强度，SHA512可应用于每一已编码的密钥W_D。因此，无关于W_D的大小，均存在模式不可预测的512位私密密钥序列。

[0111] 样本干扰片产生及标记函数实施方案

[0112] 标记且使用干扰片解除后续功能与(已经置乱且迷惑的)真实模板点及横跨脉管系统的描述符的耦合，从而提供增加安全性、私密性及可撤销性。下文提供关于干扰片、其产生及标记的各个实施方案的更多特定细节。

[0113] 干扰片的空间放置

[0114] 可以若干方式实现空间均匀或不可区分脉管兴趣点的“干扰片注入”以保护所存储的模板(通常是登记模板，因为验证模板是在匹配期间瞬间产生)。在一个实例中，确定真实(非干扰片)兴趣点之间的最小(排斥异常值)空间距离。插入干扰片点直到任何两个点(干扰片及/或脉管兴趣点)之间的距离是大约相同最小距离为止。密集注入干扰片的模板将在多个方面提供更强的安全性。缺点是经干扰片迷惑模板的更大大小，这也可减缓匹配器。

[0115] 另一不太极端的实施方案是两步干扰片插入。更具体地说，鉴于在登记模板的空间跨距上的典型图块化，所述两步干扰片插入开始于对此步骤使用最小距离要求(例如，三个像素)来放置干扰片的第一部分(使每个区域颗粒(干扰片及非干扰片)的总模板点的平均值大约相等所需)，称作粗略干扰片插入。所述过程继续插入干扰片的剩余部分直到通过放宽最小距离阈值(例如，放宽到一个像素)实现所需干扰片与非干扰片比率(通常3x到7x)(精细干扰片插入步骤)。

[0116] 用于干扰片放置的另一方法包含使用现有模板以脉管图块对非(或几乎非)脉管图块复制脉管点的空间图案(在一些情况中，极少自然地发生几何失真)，并同时在空白位置/附近插入干扰片，观察图块边界处的注入干扰片的模板的x、y座标的空间分布的连续性，以及每次图块的总体均匀空间密度。

[0117] 又另一方法包含在最接近点过于靠近时使用L方程组(树状结构的林德迈耶(Lindenmayer)语法)遵循相同脉管树状结构。接着根据L方程组产生的空间图案将干扰片添加到较少的脉管图块直到达到跨模板的均匀图块密度并同时观察到图块边界处的连续性为止。

[0118] 干扰片描述符内容

[0119] 在一个实施方案中，模板中的描述符特征向量(如果被视为信号)是非各态过程。注入干扰片的登记模板中的每一特征元素的统计性质(此外关于空间及特征空间中所述特征元素前后的事物)对于干扰片对非干扰片描述符来说应相同。描述符间距离的分布以及

其在干扰片及非干扰片内及跨干扰片及非干扰片的平均值及协方差矩阵也应类似。前述可通过使描述符(干扰片及非干扰片)呈现零平均值且不相关的PCA投影来实现。在前述边界内,可选取更接近脉管点的位置的干扰片描述符使得其不太可能彼此匹配,使得匹配准确度并不充足(并同时保持在VPD描述符分布特性内)。除了从现有真实点描述符产生干扰片描述符内容(例如,应用小的循环移位加上小噪声于VPD相关特征向量)之外,PCA投影及置乱函数将进一步使干扰片与真实描述符之间的任何差变平坦。注意,置乱伪装且以装置特定方式重新排序座标,从而维持欧几里得距离用于只在给出独特软件及硬件环境内的置乱空间中的匹配目的,实现单一生物特征眼睛扫描交易期间的双重认证。PCA步骤的特征向量投影之后的可选特征向量标准化产生白化的存储模板,其接近识别跨所有其特征的协方差矩阵以用于进一步保护。

[0120] 标记

[0121] 标记函数可以许多不同方式(例如通过使用散列函数)实施。例如,假设兴趣点及其对应特征向量的x、y座标:(1)添加x、y座标使得局部特征向量V的前面8个元素对应于相应兴趣点。(2)用SHA512散列化所得值。将所得位串分组为64个字节。(3)为了导出标记(输出)的座标,通过将所有奇数字节位置视为一个序列(Seq1,32个字节)且将所有偶数位置视为第二序列(Seq2,32个字节)从前述字节串提取两个序列集合。(4)Seq1中的所有字节经位XOR以得到标记为x座标的单一字节。类似地,Seq2中的所有字节经位XOR以得到标记为y座标的单一字节。(5)如果前述提及位置处存在干扰片点,那么其将被“标记”。如果否且最近的干扰片是在r个像素(例如一个像素)的半径处,那么选择移动到所计算位置且被标记。如果没有发生以上情况中的任一者,那么此位置处产生被标记的干扰片点。如果x、y范围超出0到255之外,那么可实施Seq1及Seq2的不同重散列。

[0122] 另一方法是对标记位置使用数学函数。假设级联应用三步骤过程(下文的T1、T2及T3)。如下变换输入模板点的(x,y)座标:

[0123] T1:

[0124] $x_{new} = x \sin(y)$

[0125] $y_{new} = x \cos(x)$

[0126] T2:

[0127] $$x_{new} = \begin{cases} -x & \text{如果 } x < 1 \\ x - x_{max} & \text{如果 } x > x_{max} \\ 1 & \text{如果 } x = 0 \\ x & \text{否则} \end{cases}$$

[0128] $$y_{new} = \begin{cases} -y & \text{如果 } y < 1 \\ y - y_{max} & \text{如果 } y > y_{max} \\ 1 & \text{如果 } y = 0 \\ y & \text{否则} \end{cases}$$

[0129] x_{max}及y_{max}是注入干扰片的模板中的空间座标的最大值。

[0130] T3:

[0131] $$x_{new} = \begin{cases} x_{max} - x & \text{如果} x \text{是奇数} \\ x & \text{否则} \end{cases}$$

[0132] $$y_{new} = \begin{cases} y_{max} - y & \text{如果} y \text{是奇数} \\ y & \text{否则} \end{cases}$$

[0133] 注意标记函数可经级联或重新参数化以改变跨生物特征认证应用程序的不同安装的行为。干扰片放置可被限于ROI遮罩(更具体来说,填充ROI遮罩的并集,以隐藏个别眼睑轮廓)

[0134] 干扰片位置及内容合成的实例算法

[0135] 干扰片位置及内容合成的算法的一个实施方案如下所示。考虑沿着其相应描述符(当前是H LBP、H CS LBP及SURF)存在N个原始(VPD)点,从大小R×C像素的图像产生模板(其中R是行数且C是列数)。在一个实施方案中,用于计算干扰片及标记的步骤如下所示:

[0136] 1.将干扰片定义为脉管兴趣点“比率”参数(例如,近似3.5到4.5)

[0137] 2.对用于密钥产生的每一原始点插入标记点(密钥标记):

[0138] a.使用接受原始点的位置及描述符信息作为其输入的第一标记函数在R×C窗口内产生标记点。

[0139] b.检查标记位置是否是原始点的位置:

[0140] i.如果是,那么不采取任何动作。

[0141] ii.如果否但是一个像素半径内存在干扰片点,那么将干扰片移动到标记位置。

[0142] iii.否则如果为否:

[0143] 1.在所述位置处产生从第一标记函数产生的干扰片点。

[0144] 2.使用最接近原始点为上述点产生描述符。

[0145] 描述符(FineChaffDescriptor)

[0146] 3.对用于服务器握手的每一原始点插入标记点(ServerTag)。

[0147] a.使用具有原始点的位置及描述符信息的第二标记函数在R×C窗口内产生标记点。

[0148] b.检查标记位置是否是原始点或KeyTag:

[0149] i.如果是,那么不采取任何动作。

[0150] ii.如果否但是一个像素半径内存在干扰片点,那么将干扰片移动到标记位置。

[0151] iii.否则如果为否:

[0152] 1.创建从第二标记函数产生的干扰片点。

[0153] 2.使用最接近原始点为上述点产生描述符。

[0154] 描述符(FineChaffDescriptor)

[0155] 4.将R×C分为相等大小的k个图块(例如,对于4×5图块,k=20,且R=80,C=100,+/-20)。应注意,前述值是用于实例目的,且预期其它可能值。某些值可例如基于图像传感器(所得图像分辨率)而改变。

[0156] 5.计算每一图块中的点数(原始+KeyTags+ServerTags)且寻找最大值(MaxPoints)。

[0157] 6.计算所需点且改变每个图块的类型:

[0158] a.如果图块中的点数小于MaxPoints/2:那么进行CoarseChaff直到MaxPoints/2后续跟着FineChaff直到总点数等于MaxPoints+/-5%。(如此实例算法中使用,+/-X%可能是指-X到+X的范围内的随机数)。

[0159] b.如果图块中的点数大于MaxPoints/2:那么进行FineChaff直到总点数等于MaxPoints+/-5%。

[0160] 7.对于步骤6中产生的干扰片的随机20%(对于更高干扰片计数,其可增加),产生ChaffTagChaff。

[0161] a.使用具有原始点的位置及描述符信息的第三标记函数在R×C窗口内产生标记点。

[0162] b.检查标记位置是否是原始点或KeyTag或ServerTag或干扰片:

[0163] i.如果是,那么不采取任何动作。

[0164] ii.如果否但是一个像素半径内存在干扰片点,那么将干扰片移动到标记位置。

[0165] iii.否则如果为否:

[0166] 1.创建从第三标记函数产生的点。

[0167] 2.使用最接近原始点描述符(FineChaffDescriptor)为上述点产生描述符。

[0168] 8.如果(KeyTag+ServerTag+CoarseChaff+FineChaff+ChaffTagChaff)的数目/原始点小于比率:产生FineChaff。

[0169] CoarseChaff

[0170] 1.在图块内产生远离所有点至少三个像素的随机干扰片点。

[0171] 2.CoarseChaffDescriptor:采取最接近原始描述符(OrigDesc)。

[0172] 3.对于SURF描述符:

[0173] a.NewSURFdescriptor=CircularShift(OrigDesc,+/-30%长度)+(0.01%高斯噪声)。

[0174] b.如果(OrigDesc,NewSURFdescriptor)的标准化SSD<0.1,那么进行到3.a。

[0175] 4.对于HLBP描述符:

[0176] a.NewHLBPdescriptor=CircularShift(OrigDesc,+/-30%长度)+(20%高斯噪声)。

[0177] b.如果(OrigDesc,NewHLBPdescriptor)的标准化SSD<0.1,那么进行到4.a。

[0178] 5.对于HDLBP描述符:

[0179] a.NewHCSLBPdescriptor=CircularShift(OrigDesc,+/-30%长度)+(20%高斯噪声)。

[0180] b.如果(OrigDesc,NewHCSLBPdescriptor)的标准化SSD<0.1,那么进行到5.a。

[0181] FineChaff

[0182] 1.在图块内产生远离所有点至少1个像素的随机干扰片点。

[0183] 2.FineChaffDescriptor:采取最接近原始描述符(OrigDesc)。

[0184] 3.对于SURF描述符:

[0185] 3.1.NewSURFdescriptor=CircularShift(OrigDesc,+/-30%长度)+(0.01%高斯噪声)。

[0186] 3.2.如果(OrigDesc,NewSURFdescriptor)的标准化SSD<0.2,那么进行到3.1。

[0187] 4.对于HLBP描述符：

[0188] 4.1.NewHLBPdescriptor＝CircularShift(OrigDesc,+/-30％长度)+(20％高斯噪声)。

[0189] 4.2.如果(OrigDesc,NewHLBPdescriptor)的标准化SSD<0.225,那么进行到4.1。

[0190] 5.对于HDLBP描述符：

[0191] 5.1.NewHCSLBPdescriptor＝CircularShift(OrigDesc,+/-30％长度)+(20％高斯噪声)。

[0192] 5.2.如果(OrigDesc,NewHCSLBPdescriptor)的标准化SSD<0.225,那么进行到5.1。

[0193] 向量化函数

[0194] 用于以k种方式分离例如$v_{i,d}$的标量的简单又安全且有效方式是提供标量(或其函数)给例如SHA512的散列函数,且使用所产生的位串的群组作为所需数字系列。使用向量化函数的原因如下所示:(1)无关于描述符内容,横跨线性方程组的数值稳定性(例如,其可极为接近零,尤其是在特征向量的若干位置的给出数值确度的约束内);(2)多个或较大密钥内容的较大容量,因为每一向量元素可横跨其自身的线性混合方差线;及(3)为了增加安全性,方差系数需要由模板元素在运行时间计算,而非仅仅从其存储值回调。

[0195] 向量化函数的另一实例如下所示。造成解码过程的稳定非奇异解的其它确定性且安全的向量化函数也是可接受的。

[0196] 用$v_{i,d}$的函数种入伪随机数产生器(PRNG)且产生k个伪随机数的序列。例如,使用由$f_{md_num_gen}$标示的加密安全PRNG算法且用下式种入所述算法

[0197] $$f_{seed}(k, v_{i,d}) = \lfloor 2^{31} |\cos(k v_{i,d})| \rfloor$$

[0198] 此过程中可使用一个以上$v_{i,d}$,例如组合$v_{i,d}+v_{i,d+1}$(或更有效地,以减小W容量为代价降低D)为一个,以增加数值稳定性及不可逆性。

[0199] 接着,采取所得前面的k个伪随机数rnd_seqi(i＝1、2、……、k)作为向量化输出。因此,向量化函数是:

[0200] $$\overrightarrow{rand\_seq}_{i,d} = f_{md\_num\_gen}\left(f_{seed}(k, v_{i,d})\right)$$

[0201] 视情况,为了增加安全性及动态范围控制,可通过非平凡不可逆函数$\varphi(x)$传递上述$v_{i,d}$横跨向量。一个实例如下所示。应用rnd_seq_i＝(rnd_seq$_i$-0.5)x 8(以线性地投影随机序列为[-4,4]以用以下$\varphi(\bullet)$产生更加不可预测的波动)。φ的一个实例(下文描绘)是:

[0202] $$\varphi(x) = \tanh(x-10)\sin\left((x-10)e^{-\frac{x-10}{2}}\right)$$

[0203] 最后,输入$v_{i,d}$及其相关联/编码的$\vec{W}_d$的对应$y_{i,d}$(私密密钥矩阵W的行d)是由下式给出:

[0204] $$y_{d,i} = f_{encode}(\vec{W}_d, v_{d,i}) = \sum_{j=1} w_{d,j}\varphi(rnd\_seq_d(j))$$

[0205] 如提及,使用早期提及的基于SHA的向量化拒绝对此类类型的向量化的需要。

[0206] 信任服务器功能

[0207] 在一个实施方案中，信任服务器是可结合本地密钥方法使用的可选添加安全层。信任服务器的另一增加优势是替代远程验证及模板/使用权可撤销性。例如，如果服务器没有识别由装置发送的令牌(验证时的生物特征眼睛扫描的唯一但可重新公开副产品)，那么其可发送信号到例如所涉及的网上银行服务或使用生物特征认证的其它服务，但是不会履行特定请求的交易。本实施方案的细节对于上述干扰片标记及模板匹配过程大部分是相似的。

[0208] 假设S_{CHF}，$T_S:\{\vec{V}_i^1,\vec{V}_i^2,\ldots\vec{V}_i^d\}(i=1、2、\ldots\ldots、n(T_S))\rightarrow S_{CHF}=H(\{\vec{V}_i^1,\vec{V}_i^2,\ldots\vec{V}_i^d\})=\{h_i\}$ (i＝1、2、……、n(T_S))的描述符部分的散列H(.)被指定为主干扰片记录且在登记时存储在信任服务器上(例如，在多登记系统中，每次登记具有一个主干扰片记录)。在生物特征验证时，如果需要信任服务器确证，那么可发生以下“握手”过程：模板元素T_{VER}的匹配子集被提供给f_S(类似于f_K但是支持信任服务器功能的第二干扰片标记函数)，产生S_{VER}＝H(T_{VER})，其在验证时发送到信任服务器。根据匹配器的性质，对于成功的真实匹配可知：

[0209] (a) $T_{VER}\subset T_{VPD}$，及

[0210] (b) n(T_{VER})≥k

[0211] 即，成功匹配寻找至少k个真实脉管兴趣点中，且失败(例如，虚假)匹配并未如此。因此，其遵循服务器端必须满足以下条件以验证装置端匹配的完整性：

[0212] $S_{VER}\subset S_{CHF}$及n(S_{VER})≥k

[0213] 注意，还可例如通过对S_{VER}进行n次的SHA512嵌套重复传输S_{VER}的时变散列，其中n是通用时戳的函数(例如，模数)。信任服务器将在任何比较之前对其S_{VER}执行相同时变散列。

[0214] 信任服务器的其它可能功能包含撤销对远程服务的使用权(例如，在被盗装置的情况中)，因为新装置上的新登记将创建不同的S_{VER}及S_{CHF}。注意，服务器干扰片与密钥产生干扰片并不相似，且因此此分离提供部分独立性且因此增加相对于若干假想攻击向量的安全性。否则，私密密钥对服务器干扰片的验证精确度及确证安全性可被认为相同。

[0215] 初始安全分析如下。以下案例假设其中模板被解密、生物特征认证码被解译且因此装置服务器握手逻辑加上模板结构被攻击者所知的被盗用装置。鉴于干扰片及真实脉管兴趣点的不可区分性，首次抽检模板的概率至多是$\frac{n(T_S)}{n(T_A)}$，即，由f_S标记的干扰片(大约与n(VPD)相同)除以模板元素的总数的比率，因为：

[0216] $$P(guess_1\in T_S,guess_2\in T_S,\ldots guess_k\in T_S)=\prod_{i=1}^{k}\frac{n(T_S)-i}{n(T_A)-i}<\left(\frac{n(T_S)}{n(T_A)}\right)^k$$

[0217] 假设此类猜测是独立的且被相似地分布。

[0218] 攻击者能够通过猜测收集所有所需最少k个T_S成员的机会极低。对每一脉管兴趣点使用大约一个标记干扰片的典型值且对每一脉管兴趣点使用总共四个插入干扰片，且对于单一2-ROI扫描来说k＝40，首次尝试便成功的机会是：

[0219] $$\left(\frac{n(T_S)}{n(T_A)}\right)^k = 0.2^{40} = 1.1 \times 10^{-28}$$

[0220] 如果信任服务器限制失败尝试的次数，那么此攻击成功的总体机会仍然极小。此外，如果攻击者危及信任服务器及用户的装置且破译所有所需内容，那么他或她不能通过从用户装置模板减去服务器主干扰片记录来存取用户模板的脉管兴趣点部分，因为T_S只是T_{CHF}的子集。

[0221] 本文中采用的术语及表达用作描述的术语及表达且无限制，且在使用此类术语及表达时并无排除所示且所描述的特征或其部分的任何等效物的意图。此外，在描述本发明中的某些实施方案之后，所属领域一般技术人员将明白，在不脱离本发明的精神及范围的情况下，可使用并有本文中揭示的概念的其它实施方案。各个实施方案的特征及功能可以各种组合及排列而布置，且全部被视为属于所揭示发明的范围内。因此，所描述实施方案在所有方面均被视为说明性且并无限制性。本文中描述的配置、材料及尺寸也希望是说明性且绝无限制的。类似地，虽然已提供物理解释用于解释性目的，但是并无受限于任何特定理论或机制或限制根据任何特定理论或机制的权利要求书的意图。

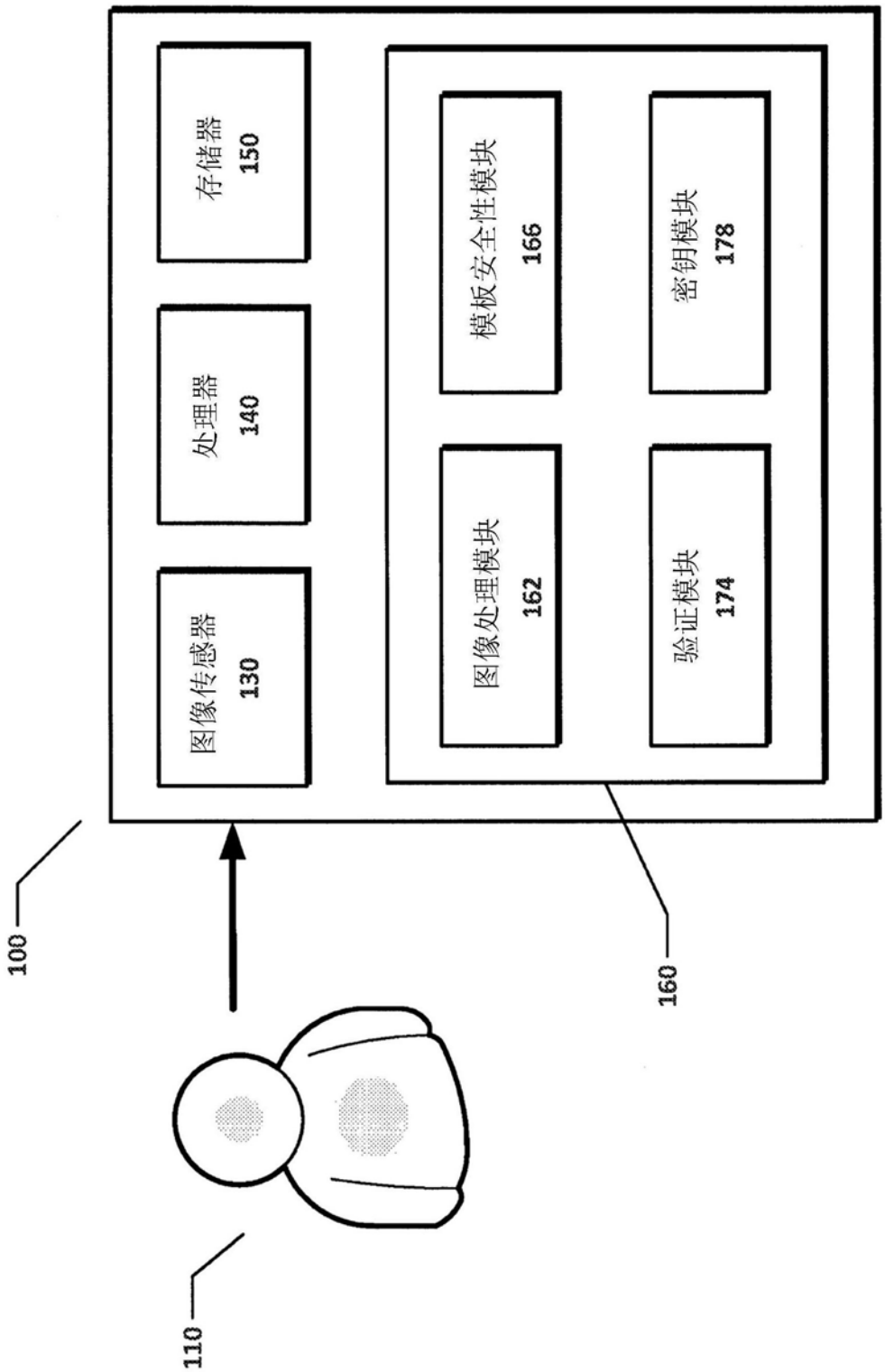
存储器
150
处理器
140
图像传感器
130
模板安全性模块
166
密钥模块
178
图像处理模块
162
验证模块
174
100
160
110

图1

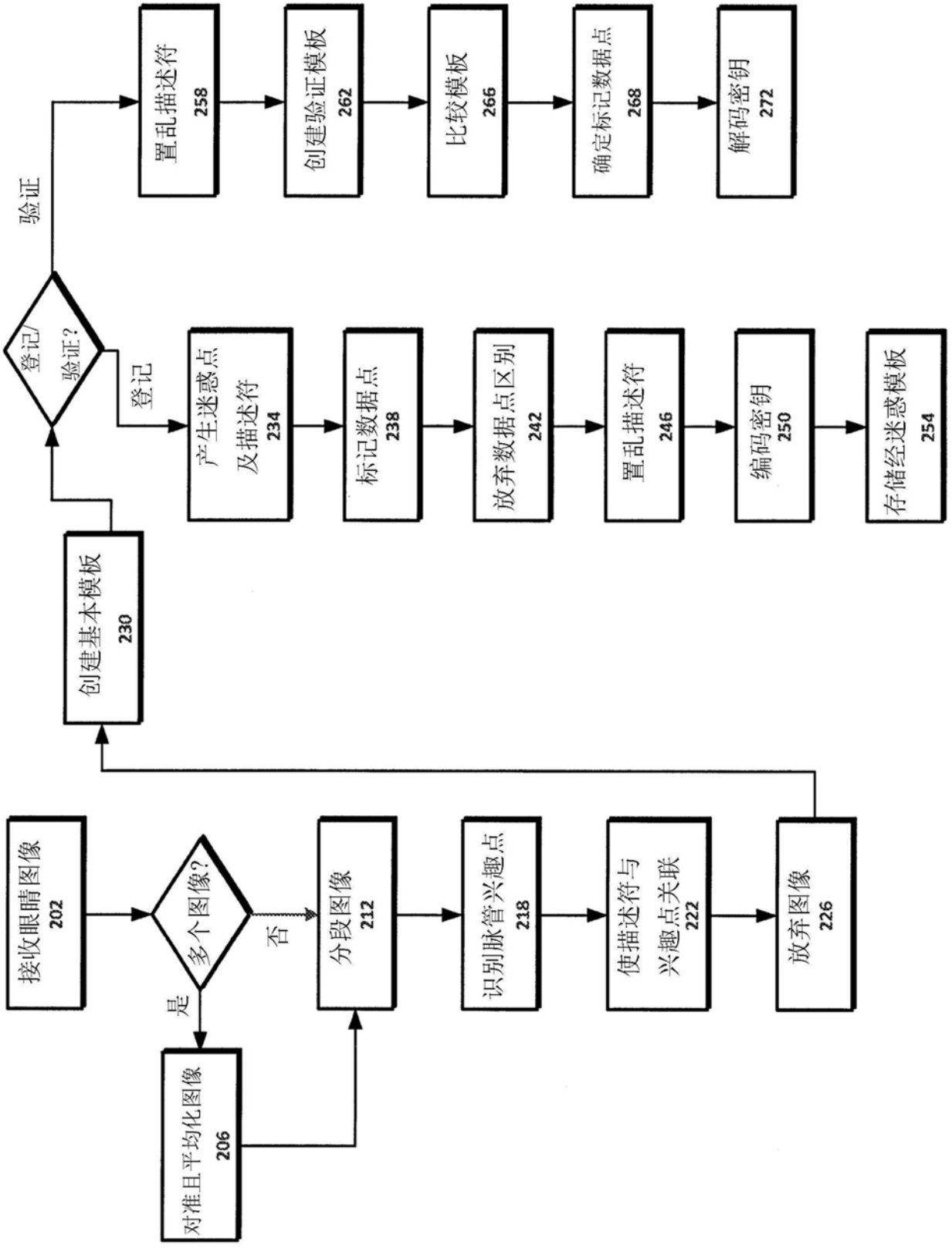
接收眼睛图像
202
多个图像?
是
否
对准且平均化图像
206
分段图像
212
识别脉管兴趣点
218
使描述符与
兴趣点关联
222
放弃图像
226
创建基本模板
230
登记/
验证?
登记
产生迷惑点
及描述符
234
标记数据点
238
放弃数据点区别
242
置乱描述符
246
编码密钥
250
存储经迷惑模板
254
验证
置乱描述符
258
创建验证模板
262
比较模板
266
确定标记数据点
268
解码密钥
272

图2

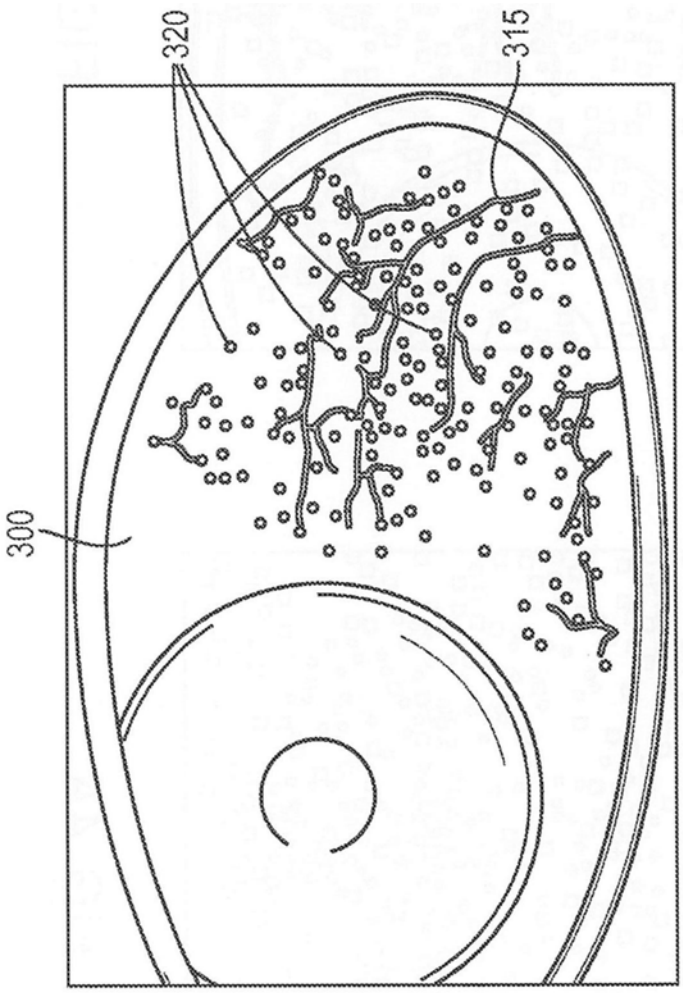

图3

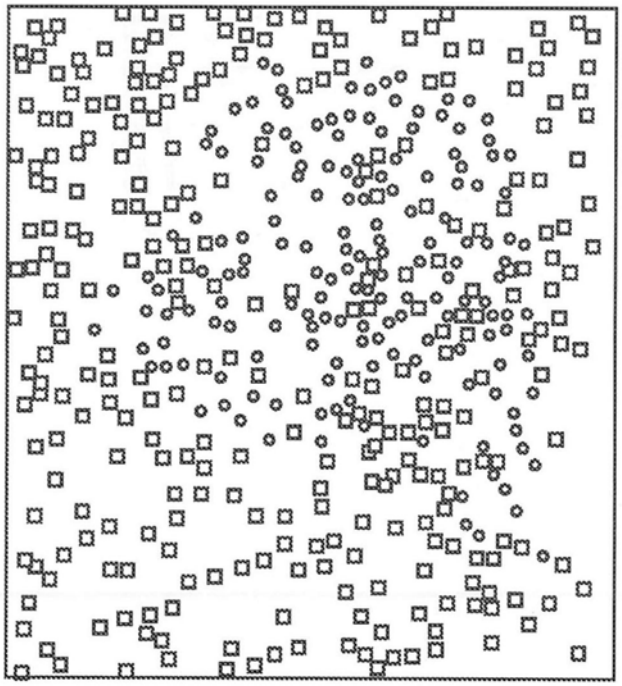

图4A

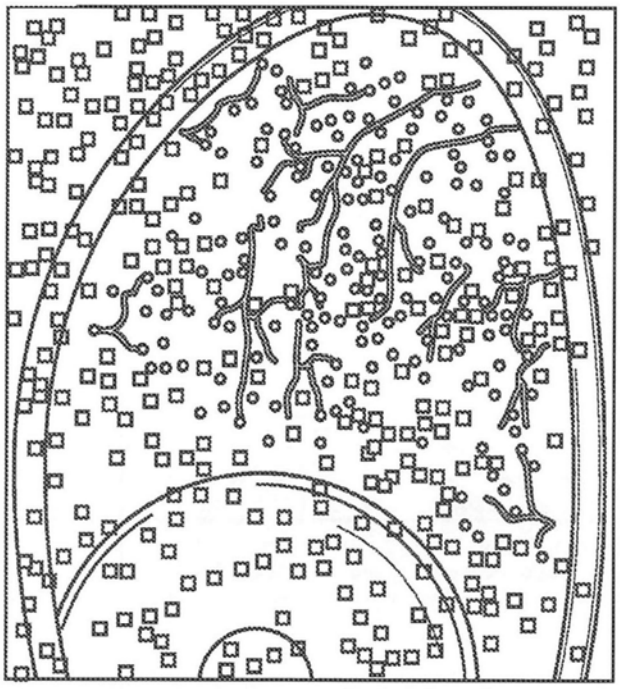

图4B

图5