(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 101047498 B
(45)授权公告日 2012.10.31

(21)申请号 200710091588.6
(22)申请日 2007.03.28
(30)优先权数据
2006-091807 2006.03.29 JP
2007-000671 2007.01.05 JP
(73)专利权人 株式会社日立制作所
地址 日本东京都
(72)发明人 高桥健太 比良田真史 日野英逸 三村昌弘
(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静
(51)Int.Cl.
H04L 9/10(2006.01)
G06K 9/00(2006.01)
(56)对比文件
US 2004/0015705 A1,2004.01.22, 全文.
US 6836554 B1,2004.12.28, 全文.
WO 2005/121924 A2,2005.12.22, 说明书第9页第9行－第10页第17行、图3,4.
审查员 郝政宇

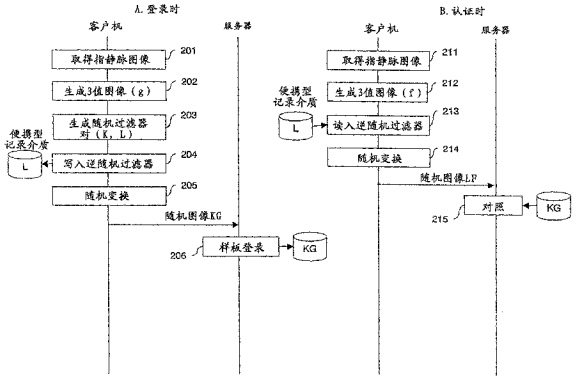
权利要求书 4 页 说明书 11 页 附图 12 页

(54)发明名称

生物体认证方法以及系统

(57)摘要

在采用个人生物体信息的登录图像和对照图像的相互相关性来认证本人的个人认证方法中，在生物体信息登录时，生成用于干扰图像的过滤器、以及逆过滤器，使该过滤器作用于由生物体信息生成的登录图像上，生成登录样板并登录在存储装置中。在个人认证时，使逆过滤器作用于由个人取得的生物体信息生成的对照图像上，根据逆过滤器作用后的对照图像与登录样板的相互相关性来判定个人。



CN 101047498 B

1. 一种生物体认证方法，其根据个人生物体信息的登录图像与对照图像的相互相关性来认证个人，其特征在于，

生成用于干扰该图像的过滤器、以及该过滤器的逆过滤器，使该过滤器作用于由该生物体信息生成的该登录图像上，生成登录样板并预先登录在存储装置中，

在认证时，使该逆过滤器作用于由个人取得的生物体信息生成的对照图像上，根据该逆过滤器作用后的对照图像与该登录样板的相互相关性来判定个人，

该登录图像以及逆过滤器作用前的该对照图像的亮度值是具有0、1、2这3种值的3值图像，

在登录时，在该登录图像上将亮度值为2的像素的亮度值变更为0，将亮度值具有0、1这2种值的2值图像作为登录2值图像来生成，使用于该干扰的过滤器分别作用于该登录图像与所述登录2值图像上，作成登录样板，

在认证时，在逆过滤器作用前的该对照图像上将亮度值为2的像素的亮度值变更为0，将亮度值具有0、1这2种值的2值图像作为对照2值图像来生成，使该逆过滤器分别作用于逆过滤器作用前的该对照图像与该对照2值图像上，

采用该登录样板的登录图像与对照图像的相互相关性、以及过滤器作用前的登录2值图像与逆过滤器作用前的对照2值图像的相互相关性来算出距离值，以判断是否是本人。

2. 根据权利要求1所述的生物体认证方法，其特征在于，

在生物体信息登录时，对该登录图像进行傅立叶变换，使用于进行上述干扰的过滤器在频率空间上作用，在认证时，对逆过滤器作用前的该对照图像进行傅立叶变换，使该逆过滤器在频率空间上作用。

3. 根据权利要求1所述的生物体认证方法，其特征在于，

在登录时，对该登录图像进行数学逻辑变换，使用于进行上述干扰的过滤器在数学逻辑变换后的空间上作用，在认证时，对逆过滤器作用前的该对照图像进行数学逻辑变换，使该逆过滤器在数学逻辑变换后的空间上作用。

4. 根据权利要求1所述的生物体认证方法，其特征在于，

用于进行所述干扰的过滤器以及该逆过滤器，设定为：使该过滤器作用后生成的登录样板、以及使该逆过滤器作用后生成的对照图像具有随机值。

5. 根据权利要求1所述的生物体认证方法，其特征在于，

生成的所述逆过滤器，在用户持有的记录介质或者该终端装置内的存储部中进行存储。

6. 根据权利要求1所述的生物体认证方法，其特征在于，

根据适用的对象变更该过滤器以及该逆过滤器的系数来进行使用。

7. 根据权利要求1所述的生物体认证方法，其特征在于，

在登录图像上选择一个位置以上的坐标，切出以该坐标的各自为中心的规定大小的局部图像，在对照图像上根据该坐标的周边图像与该局部图像的相互相关性或者距离来判定关于该局部图像的一致或者不一致，根据成为一致的局部图像数来判定本人。

8. 根据权利要求7所述的生物体认证方法，其特征在于，

在所述登录图像上选择的坐标是在该登录图像中具有特征的构造的点的坐标。

9. 根据权利要求7所述的生物体认证方法，其特征在于，

在所述登录图像上选择的坐标是在该登录图像中具有特征的构造的点的坐标以及随机选择的点的坐标。

10. 根据权利要求 8 所述的生物体认证方法，其特征在于，

所述生物体信息为指纹，具有所述特征的构造的点是指纹的端点或者分歧点，所述坐标以指纹的核心为原点进行计算。

11. 根据权利要求 1 所述的生物体认证方法，其特征在于，

所述生物体信息为指静脉。

12. 一种生物体认证系统，采用经由网络连接的终端装置和服务器，进行个人的生物体认证，其特征在于，

该终端装置，具有：

图像生成单元，其根据所提取的个人生物体信息生成登录图像或者对照图像；过滤器生成单元，其生成用于干扰该图像的过滤器以及逆过滤器；变换单元，其在该图像生成单元生成的该登录图像上，使通过该过滤器生成单元生成的过滤器作用，生成登录样板，或者在该图像上使该逆过滤器作用生成变换对照图像；和第一通信单元，其将至少含有该登录样板或者该变换对照图像的信息发送到该服务器中，

该服务器，

具有：第 2 通信单元，其接收由该终端装置发送的信息；登录单元，其将经由第 2 通信单元接收到的该登录样板存储在存储装置中；和对照单元，其对照在认证时经由该第 2 通信单元得到的该变换对照图像，计算该登录样板和该变换对照图像的相互相关性并判断相似性，

所述服务器根据该对照单元的判断结果来认证个人，

该登录图像以及逆过滤器作用前的该对照图像的亮度值是具有 0、1、2 这 3 种值的 3 值图像，

在登录时，在该登录图像上将亮度值为 2 的像素的亮度值变更为 0，将亮度值具有 0、1 这 2 种值的 2 值图像作为登录 2 值图像来生成，使用于该干扰的过滤器分别作用于该登录图像与所述登录 2 值图像上，作成登录样板，

在认证时，在逆过滤器作用前的该对照图像上将亮度值为 2 的像素的亮度值变更为 0，将亮度值具有 0、1 这 2 种值的 2 值图像作为对照 2 值图像来生成，使该逆过滤器分别作用于逆过滤器作用前的该对照图像与该对照 2 值图像上，

采用该登录样板的登录图像与对照图像的相互相关性、以及过滤器作用前的登录 2 值图像与逆过滤器作用前的对照 2 值图像的相互相关性来算出距离值，以判断是否是本人。

13. 根据权利要求 12 所述的生物体认证系统，其特征在于，

在更新登录样板时，该终端装置重新生成过滤器以及逆过滤器并进行保存，求出已有的过滤器与新过滤器的差分，将过滤器的差分向该服务器发送，该服务器使接收到的过滤器的差分作用于由第 2 通信单元接收到的、存储在存储装置中的该登录样板上，生成新的样板并登录到该存储装置中。

14. 根据权利要求 12 所述的生物体认证系统，其特征在于，

在登录所述登录样板时，该终端装置，对登录图像进行傅立叶变换，使用于进行所述干扰的过滤器在频率空间上作用，在认证时，对逆过滤器作用前的变换对照图像进行傅立叶

变换，使该逆过滤器在频率空间上作用。

15. 根据权利要求 12 所述的生物体认证系统，其特征在于，

用于进行所述干扰的过滤器以及逆过滤器，设定为：使该过滤器作用后生成的登录样板、以及使该逆过滤器作用后生成的变换对照图像具有随机值。

16. 根据权利要求 12 所述的生物体认证系统，其特征在于，

根据适用的系统变更该过滤器以及该逆过滤器的系数后进行使用。

17. 一种终端装置，其与根据个人生物体信息的登录图像和对照图像的相互相关性进行生物体认证的服务器连接来使用，其特征在于，

具有：生物体提取单元，其提取生物体信息；图像生成单元，其由提取的个人生物体信息生成用于登录或者对照的图像；过滤器生成单元，其生成用于干扰该图像的过滤器以及逆过滤器；变换单元，其在该图像生成单元生成的该图像上，使通过该过滤器生成单元生成的过滤器作用，生成登录样板，或者在该图像上使该逆过滤器作用生成对照图像；和通信单元，其将至少含有该登录样板或者该对照图像的信息发送到该服务器中，以供生物体认证，

该登录图像以及逆过滤器作用前的该对照图像的亮度值是具有 0、1、2 这 3 种值的 3 值图像，

在登录时，在该登录图像上将亮度值为 2 的像素的亮度值变更为 0，将亮度值具有 0、1 这 2 种值的 2 值图像作为登录 2 值图像来生成，使用于该干扰的过滤器分别作用于该登录图像与所述登录 2 值图像上，作成登录样板，

在认证时，在逆过滤器作用前的该对照图像上将亮度值为 2 的像素的亮度值变更为 0，将亮度值具有 0、1 这 2 种值的 2 值图像作为对照 2 值图像来生成，使该逆过滤器分别作用于逆过滤器作用前的该对照图像与该对照 2 值图像上，

采用该登录样板的登录图像与对照图像的相互相关性、以及过滤器作用前的登录 2 值图像与逆过滤器作用前的对照 2 值图像的相互相关性来算出距离值，以判断是否是本人。

18. 一个生物体设备，其与根据个人生物体信息的登录图像和对照图像的相互相关性进行生物体认证的其它装置连接来使用，其特征在于，

具有：传感器，其提取个人生物体信息；图像生成单元，其由提取的个人生物体信息生成用于登录或者对照的图像；过滤器生成单元，其生成用于干扰该图像的过滤器以及逆过滤器；和变换单元，其在该图像生成单元生成的该图像上，使通过该过滤器生成单元生成的过滤器作用，生成登录样板，或者在该图像上使该逆过滤器作用生成对照图像；将含有已生成的该登录样板或者该对照图像的信息向该其它装置发送，以供生物体认证，

该登录图像以及逆过滤器作用前的该对照图像的亮度值是具有 0、1、2 这 3 种值的 3 值图像，

在登录时，在该登录图像上将亮度值为 2 的像素的亮度值变更为 0，将亮度值具有 0、1 这 2 种值的 2 值图像作为登录 2 值图像来生成，使用于该干扰的过滤器分别作用于该登录图像与所述登录 2 值图像上，作成登录样板，

在认证时，在逆过滤器作用前的该对照图像上将亮度值为 2 的像素的亮度值变更为 0，将亮度值具有 0、1 这 2 种值的 2 值图像作为对照 2 值图像来生成，使该逆过滤器分别作用于逆过滤器作用前的该对照图像与该对照 2 值图像上，

采用该登录样板的登录图像与对照图像的相互相关性、以及过滤器作用前的登录 2 值

图像与逆过滤器作用前的对照 2 值图像的相互相关性来算出距离值，以判断是否是本人。

19. 根据权利要求 18 所述的生物体设备，其特征在于，

在登录所述登录样板时，对登录图像进行傅立叶变换，使用于所述干扰的过滤器在频率空间上作用，在认证时，对对照图像进行傅立叶变换，使该逆过滤器在频率空间上作用。

生物体认证方法以及系统

[0001] 要求优先权

[0002] 本申请主张申请于2006年3月29日编号为2006-091807的日本专利申请和2007年1月25日编号为2007-000671的日本申请的优先权，相关内容以编入本申请参考文献的内容中。

技术领域

[0003] 本发明涉及采用个人生物体信息认证本人的生物体认证方法以及系统。

背景技术

[0004] 采用了生物体信息个人认证系统，在初期登录时取得个人的生物体信息，提取被称为特征量的信息来进行登录。将此登录信息称为样板。在认证时再次从个人上取得生物体信息提取特征量，对照之前登录的样板，确认是否是本人。

[0005] 在经由网络来连接客户机与服务器的系统中，在服务器对处于客户机侧的用户进行生物体认证时，典型的方法是服务器保存样板。客户机在认证时取得用户的生物体信息，提取特征量向服务器发送，服务器将特征量与样板进行对照来确认是否是本人。

[0006] 可是，由于样板是可以确定个人的信息，所以作为个人信息需要严密的管理，需要很高的管理成本。例如进行严密地管理，很多人从个人隐私的观点出发，对登录样板存在心理上的反感。另外，因为每个个人具有的一种生物体信息的数量有限（例如指纹只有10个手指的），所以不能如密码或密钥那样容易地变更样板。假如由于泄漏样板而发生伪造的危险时，有变得不可以使用其生物体认证这样的问题。此外，在针对不同的系统登录相同生物体信息时，就会威胁到其它系统。

[0007] 作用关于上述问题的对策，在特开2001-7802号公报(US 20050229009、EP1063812)中公开了这样的方法：加密生物体信息后发送到认证服务器上。根据这样的方法，由于在认证时需要临时解密，所以难以防止由于高度攻击而引起的泄漏、以及由服务器管理者造成的有意泄漏，即使作为对个人隐私问题的对策也是不足的。

[0008] 因此，提出了这样的方法（称为可取消(cancelable)的生物体认证），在登录生物体信息时用一定的函数和客户机具有的秘密参数来变换特征量，以隐匿了原始的信息的状态作为样板保管在服务器上，在认证时用相同函数和参数来变换客户机新提取的生物体信息的特征量，并向服务器发送，服务器保持着变换后的状态对照接收到的特征量和样板。

[0009] 根据此方法，客户机秘密保存变换参数，由此服务器即使在认证时也不能知道原始的特征量，可以保护个人的隐私。另外，即使在样板已泄漏的情况下，通过变更变换参数来再次生成、登录样板，就可以保持安全性。此外在针对不同的系统采用相同的生物体信息时，通过登录用各个不同的参数来变换的样板，可以防止一个样板泄漏而使其它系统的安全性降低。

[0010] 可取消生物体认证的具体实现方法，依存于生物体信息的种类及对照算法。M.Savvides，B.V.K.Vijayakumar and P.K.Khosla，“Authentication-InvariantCa

ncelable Biometric Filters for Illumination-Tolerant Face Verification", BiometricTechnology for Human Identification, Proceedings of SPIE Vol.5404, P156-163 中,提出了采用面部图像的可取消生物体认证的实现方法。该方法将面部图像变换为频率空间,在登录时作成吸收照明变动等的过滤器 (filter) 作用来生成样板,在认证时针对输入的面部图像进行采用了样板的过滤处理,通过对输出图形的阈值判定来进行认证。

发明内容

[0011] 根据上述特开 2001-7802 号公报 (US 20050229009, EP 1063812),在利用了生物体信息的远程本人认证系统中,将输入的生物体信息在客户机侧加密后发送,在认证服务器上解密。由此,即使在经由网络的生物体认证系统中也可以安全地收发生物体信息。但是,由于在认证服务器内解密生物体信息,所以不能对服务器管理者隐匿个人生物体信息。因此,可能由于意外事故或服务器管理者的不良行为而导致明文的生物体信息泄漏。另外仍然留有不能降低对个人的涉及隐私的反感这样的课题。

[0012] 根据 M.Savvides,B.V.K.Vijayakumar and P.K.Khosla,"Authentication-InvariantCancelable Biometric Filters for Illumination-Tolerant Face Verification", BiometricTechnology for Human Identification, Proceedings of SPIE Vol.5404, P156-163,可以通过使随机过滤器作用到登录样板上,来实现可取消化,但是在针对将图像彼此间的相互相关性作为对照值这样的对照算法,适用此方法来进行可取消化时,产生了由于对照值有较大的区别,使对照精度下降这样的问题。

[0013] 另外,在登录图像与对照图像的亮度值为根据表示作为生物体的特征的程度具有 3 种值的 3 值图像时,即使针对将 3 值图像彼此间的距离值作为对照值这样的对照算法, 在 M.Savvides, B.V.K.Vijayakumar and P.K.Khosla,"Authentication-Invariant Cancelable Biometric Filters for Illumination-TolerantFace Verification", Biometric Technology for Human Identification, Proceedings ofSPIE Vol.5404, P156-163 提出的方法中,也不能实现可取消化。

[0014] 本发明的目的是提供一种生物体认证,其针对具有规定特性的对照算法,不用使对照精度下降就可以实现可取消化。

[0015] 本发明,在根据个人生物体信息的登录图像与对照图像的相互相关性来认证个人的方法中,在登录时,生成用于干扰图像的过滤器、以及逆过滤器,使该过滤器作用于由生物体信息生成的登录图像上,生成登录样板并预先登录在存储装置中,在认证时,使该逆过滤器作用于由个人取得的生物体信息生成的对照图像上,采用逆过滤器作用后的对照图像与登录样板的相互相关来判定个人。

[0016] 另外,本发明的生物体认证系统,最理想的是成为这样的结构 :在进行个人生物体认证的生物体认证系统中,具有 :图像生成部,其由提取的个人生物体信息生成用于登录或者对照的图像 ;过滤器生成部,其生成用于干扰该图像的过滤器以及逆过滤器 ;变换部,其在该图像生成部生成的该图像上,使通过该过滤器生成部生成的过滤器作用,生成登录样板,或者在该图像上使该逆过滤器作用生成对照图像 ;登录部,其将该登录样板存储在存储装置中 ;和对照部,其对照在认证时得到的该对照图像与存储在该存储装置中的该登录样

板，判断两者的相互相关性，该生物体认证系统，根据该对照部的判断结果来认证个人。

[0017] 根据最理想的例子，本发明的生物体认证系统，采用经由网络连接的终端装置和服务器，进行个人的生物体认证，其中，终端装置具有：图像生成部，其由提取的个人生物体信息生成用于登录或者对照的图像；过滤器生成部，其生成用于干扰该图像的过滤器以及逆过滤器；变换部，其在该图像生成部生成的该图像上，使通过该过滤器生成部生成的过滤器作用，生成登录样板，或者在该图像上使该逆过滤器作用生成对照图像；和第一通信部，其将至少含有登录样板或者对照图像的信息发送到服务器中。服务器具有：第 2 通信部，其接收由终端装置发送的信息；登录部，其将经由第 2 通信部接收到的登录样板存储在存储装置中；和对照部，其对照在认证时经由第 2 通信部得到的对照图像与存储在该存储装置中的登录样板，判断两者的相互相关性；根据该对照单元的判断结果进行个人生物体认证。

[0018] 另外，本发明最理想的是还构成为这样的生物体设备，它是与根据个人生物体信息的登录图像和对照图像的相互相关性进行生物体认证的其它装置连接来使用的生物体设备，具有：传感器，其提取个人生物体信息；图像生成部，其由提取的个人生物体信息生成用于登录或者对照的图像；过滤器生成部，其生成用于干扰图像的过滤器以及逆过滤器；和变换部，其在图像生成部生成的该图像上，使通过过滤器生成部生成的过滤器作用，生成登录样板，或者在图像上使该逆过滤器作用生成对照图像；该生物体设备，将含有已生成的登录样板或者对照图像的信息向其它装置发送，以供生物体认证。

[0019] 另外，本发明最理想的是构成为在终端装置以及服务器上可执行的程序，它是在具有经由网络连接的终端装置和服务器的生物体认证系统中执行来进行个人生物体认证的程序，在终端装置中，具有实现以下单元的功能：图像生成单元，其由提取的个人生物体信息生成用于登录或者对照的图像；过滤器生成单元，其生成用于干扰图像的过滤器以及逆过滤器；变换单元，其在由图像生成单元生成的图像上使通过过滤器生成单元生成的过滤器作用，生成登录样板，或者在图像上使逆过滤器作用生成对照图像；和将至少含有登录样板或者对照图像的信息发送到服务器中的单元；在服务器中具有实现以下单元的功能：登录单元，其将由终端装置发送而得到的登录样板存储在存储装置中；和对照单元，其对照在认证时由终端装置发送而得到的对照图像与存储在存储装置中的登录样板，判断两者的相互相关性；根据对照单元的判断结果进行认证。

[0020] 根据本发明，在基于图像彼此间相互相关性的对照算法中，可以实现可取消生物体认证，该可取消生物体认证，可以在使登录图像以及对照图像随机化而对服务器管理者保持隐匿图像的状态下进行认证。另外，在图像为 3 值图像的情况下且在将距离值作为对照值这样的对照算法中，可以实现可取消生物体认证。另外，可以生成用于更加难以由随机化的图像恢复原始图像的随机过滤器。

附图说明

[0021] 图 1 是表示一实施方式中的可取消指静脉系统的结构图。

[0022] 图 2 是表示一实施方式中的指静脉的登录处理以及认证处理的流程图。

[0023] 图 3 是表示一实施方式中的随机变换的处理流程图。

[0024] 图 4 是表示其它例的随机变换的处理流程图。

[0025] 图 5 是表示其它例的随机变换的处理流程图。

[0026] 图 6 是表示一实施方式中的对照处理的详细流程图。

[0027] 图 7 是用于说明一实施方式中的恢复困难性提高的理由的图。

[0028] 图 8 是表示一实施方式中的样板更新方法的处理流程图。

[0029] 图 9 是表示第二实施方式中的可取消指纹认证系统的结构图。

[0030] 图 10 是表示第二实施方式中的指纹登录处理的流程图。

[0031] 图 11 是表示第二实施方式中的指纹认证处理的流程图。

[0032] 图 12 是表示第二实施方式中的指纹登录・认证处理的详细流程图。

[0033] [符号说明]

[0034] 100 :客户机 ;101 :3 值图像生成部 ;102 :随机变换部 ;103 :随机过滤器生成部 ;104 :记录介质 I/F 部 ;105 :通信部 ;110 :指静脉传感器 ;120 :便携型记录介质 ;130 :服务器 ;131 :通信部 ;132 :登录部 ;133 :存储装置 ;134 :对照部。

具体实施方式

[0035] 以下,参照附图对本发明的实施方式进行说明。

[0036] [实施例 1]

[0037] 在本实施方式中,对可取消指静脉认证系统举例进行说明,该可取消指静脉认证系统,在对服务器保持隐匿指静脉图像的状态下,在服务器内进行指静脉对照。

[0038] 图 1 表示可取消指静脉认证的系统结构图。该可取消指静脉认证系统的结构为 :进行样板的保管和对照的服务器 130,与进行登录・认证时的指静脉图像取得、3 值图像生成、以及随机变换的客户机终端 (以及仅称客户机)100,经由因特网及内部网这样的网络连接。

[0039] 客户机 100 由用户自身或者可以信赖的第三者来进行管理,其具有进行指静脉图像化的指静脉传感器 110,并且使用用户携带的便携型记录介质 120。便携型记录介质 120 是用户持有且管理的、如 IC 卡或 USB 存储器的存储介质。当然,便携终端或软盘介质也可以利用。例如,从自己家进行网上银行业务时也可以成为这样的构成 :客户机 100 是用户管理的自家 PC,服务器 130 为银行管理的服务器机器。

[0040] 客户机终端 100 的结构为具有以下各部 :3 值图像生成部 101,其从指静脉图像中提取指静脉图形,进行 3 值化 ;随机过滤器生成部 103,其在登录时生成在各像素中具有随机值的随机过滤器对 ;随机变换部 102,其采用该随机过滤器来变换 3 值图像以生成随机图像 ;记录介质 I/F 部 104,其与便携型记录介质 120 间进行通信 ;和通信部 105,其经由网络进行通信。上述 3 值图像生成部 101、随机过滤器生成部 103 以及随机变换部 102 的处理,可以通过客户机 100 的处理器执行程序来实现。此外例如,可以通过特开 2004-178606 公报所公开的方法来实现 3 值图像的生成。

[0041] 服务器 130 的结构为具有以下各部 :通信部 131,其经由网络进行通信 ;登录部 132,其将随机图像作为样板来登录 ;存储装置 133,其存储样板 ;和对照部 134,其将在认证时新接收的随机图像与样板对照并计算失配率。通过服务器 130 执行程序来实现登录部 132 以及对照部 134 中的处理。

[0042] 在此,所谓失配率是表示作为对象的随机图像与样板不相似至何种程度的指标,可以说失配率越小越相似。此外,失配率计算可以使用例如在 NaotoMiura, Akio Nagasaka,

Takafumi Miyatake,“Feature extraction of finger-veinpatterns based on repeated line tracking and its application to personalidentification”,Machine Vision and Applications(2004)Vol.15,P.194-203 中所公开的方法来实现。

[0043] 图 2 表示指静脉的登录处理以及认证处理动作的流程。首先,对登录处理动作进行说明。在客户机 100 中,指静脉传感器 110 取得用户的指静脉图像 (S201)。然后,客户机 100 从指静脉图像中提取指静脉图形,并 3 值化,生成 3 值图像 (S202)。

[0044] 这里,3 值图像的生成,例如可以通过特开 2004-178606 公报中所述的方法来实现。根据该方法,当将在登录时生成的 3 值图像 g 的纵幅设为 He、横幅设为 We,将在认证时生成的 3 值图像 f 的纵幅设为 Hv、横幅设为 Wv 时,则有 He ＜ Hv,We ＜ Wv。可是在本实施方式中,通过以下方法将登录时 3 值图像 g 的尺寸扩张为认证时 3 值图像 f 的尺寸。首先,使 g 中心与 f 中心重合,接着,将在 g 外侧 f 内侧的区域 (即,超出了 g 的区域) 的像素亮度值设为 1。由此,g 的尺寸可以扩张为纵幅 Hv、横幅 Wv。

[0045] 接着,客户机 100 生成随机过滤器对 (K, L)(S203)。这里,将 K 称为随机过滤器,将 L 称为逆随机过滤器。客户机 100 将逆随机过滤器 L 写入便携型存储装置 120,还将逆随机过滤器 L 从客户机内的存储装置中消去 (S204)。该逆随机过滤器 L 被保管在便携型存储介质 120 内,并对服务器 130 进行隐匿。

[0046] 客户机 100 向随机变换部 102 输入上述随机过滤器 K 以及上述 3 值图像,将输出的随机图像 KG 向服务器 130 发送 (S205)。对于随机变换的详细说明在后面进行叙述。服务器 130 接收该随机图像 KG,并将这个作为样板登录到存储装置 133 中 (S206)。

[0047] 以下,对认证时的处理动作进行说明。客户机 100 经由指静脉传感器 110 取得用户的指静脉图像 (S211)。客户机 100 由指静脉图像生成 3 值图像 (212)。这里,例如通过在特开 2004-178606 公报中记载的方法来生成 3 值图像。3 值图像 f 的尺寸为纵幅 Hv、横幅 Wv。

[0048] 接着,客户机 100 从便携型存储介质 120 读入所述逆随机过滤器 L(S213)。并且,客户机 100 向随机变换部 102 输入所述逆随机过滤器 L 以及其 3 值图像 f,将输出的随机图像 LF 向服务器 130 发送 (S214)。此外,对于随机变换的详细说明在后面进行叙述。

[0049] 服务器 130 接收随机图像 LF,并将这个与所述样板 KG 对照,判断是否是本人的指静脉 (S215)。此外,认证处理结束后,客户机 100 从内部存储装置中消去所述逆随机过滤器 L。

[0050] 如以上所述,服务器 130 将变换后的随机图像 KG 作为样板来保管,还在认证时接收变换后的随机图像 LF。对服务器 130 隐匿随机过滤器 K 以及逆随机过滤器 L,由此服务器 130 无法知晓原始的指静脉图像 g 以及 f。因此,对服务器 130,用户的匿名性提高,这样可以保护个人隐私。另外,假设从服务器 130 泄漏了样板 KG,因为不清楚原始的 3 值图像 g 所以也不能伪造指静脉。另外,变更随机过滤器 K 以及逆随机过滤器 L 以更新样板,由此可以在利用相同手指的同时使旧样板无效。由此可以实现更高的安全性,且削减服务器的样板管理成本。此外在本实施方式中,逆随机过滤器 L 保管在用户持有的记录介质中,不过也可以保管在客户机 100 内,还可以由用户输入的密码动态生成等。

[0051] 接着,参照图 3 对生成上述的随机过滤器对的动作进行说明。这里,在对于随机变换中的基底变换进行了傅立叶变换时,就其在随机过滤器生成部 103 中的随机过滤器对

(K,L) 生成方法进行叙述。在该方法中首先设定随机过滤器 K(u,v)。将 (u,v) 作为在基底变换后空间内的坐标,按每一 (u, v) 产生随机数,并将该随机数作为 K(u, v) 的值 (S301)。接着,设定逆随机过滤器 L(u,v)。L(u,v),将与每一 (u,v) 对应的 K(u,v) 的倒数 (或者,为关于乘法的逆元) 作为值来进行设定 (S302)。另外如后所述,在随机变换中进行 2 值图像生成,而且用于干扰该 2 值图像的随机过滤器对 K′ (u, v) 和 L′ (u, v),采用与上述相同的流程来另行生成。

[0052] 如果采用这样生成的随机过滤器对 K(u,v),则干扰作为样板应该登录在服务器上的图像 K(u,v)·G(u,v)、K′ (u,v)·G′ (u,v),假设即使从服务器泄漏了 K(u,v)·G(u,v)、K′ (u,v)·G′ (u,v),但如果不知道随机过滤器 K(u,v)、K′ (u,v),则恢复 G(u,v)、G′ (u, v) 是困难的。另外,对于在认证时发送到服务器的图像,可以通过采用逆过滤器 L(u,v) 和 L′ (u,v) 生成 L(u,v)·F(u,v)、L′ (u,v)·F′ (u,v),来进行干扰。由此可以成为指静脉对照的可取消化。

[0053] 此外,作为其它例,可以通过下面这样的方法来实现随机过滤器生成部 103 中的随机过滤器对 (K,L) 生成。在该方法中,将 K(u,v)、L(u,v) 设定为 :随机变换部 102 的输出的随机图像 K(u,v)·G(u,v)、L(u,v)·F(u,v) 成为同样的随机数。

[0054] 以下,采用图 4 对此例进行说明。客户机首先按每一 (u, v) 产生同样的随机数 (S401)。接着,接收图像 G(u,v),将随机数 R(u,v) 除以 G(u,v),将这个值作为随机过滤器 K(u,v) (S402)。接着,计算 K(u,v) 的倒数,将这个倒数作为逆随机过滤器 L(u,v) (S403)。如果采用这样生成的随机过滤器 K(u, v),则作为样板应该登录在服务器上的随机图像 K(u,v)·G(u,v) 与 R(u,v) 相等,成为同样的随机数。假设即使从服务器泄漏了 K(u,v)·G(u,v),因为这是同样的随机数,所以如果不知道随机过滤器 K(u,v),则不能判断为是指静脉图像,恢复 G(u, v) 也是困难的。如果利用这样的方法来生成随机过滤器对,则可以使保存在服务器的随机图像 K(u,v)·G(u,v) 的恢复更加困难。另外,关于应该针对 2 值图像 K′ (u,v)·G′ (u,v) 来作用的过滤器 K′ (u,v)·L′ (u,v),也可以采用与上述相同的流程来设定。

[0055] 以下,参照图 5 对随机变换的处理动作进行说明。客户机 100 向随机变换部 102 输入 3 值图像 (g 或者 f)。随机变换部 102 首先计算 3 值图像的静脉像素数 (S501)。在登录时,在 3 值图像 g(x,y) 上求亮度值为 2 的像素总和。将这个设为 Sg。在认证时,在 3 值图像 f(x,y) 上求亮度值为 2 的像素总和。将这个设为 Sf。

[0056] 接着,随机变换部 102,由 3 值图像生成 2 值图像 (S502)。在该 2 值图像生成中,在 3 值图像 (g(x, y) 或者 f(x, y)) 各像素的亮度值是 0 以及 1 时为保持原状的值,当是 2 时将该值置换为 0。这里将生成的 2 值图像称为 g′ (x,y) 以及 f′ (x,y)。

[0057] 接着,随机变换部 102,对 3 值图像 (g(x,y) 或者 f(x,y)) 以及 2 值图像 g′ (x,y) 或者 f′ (x, y) 进行基底变换 (S503)。这里,作为基底变换以傅立叶变换为例子。通过傅立叶变换,图像 g(x,y) 被变换为傅立叶图像 G(u,v)。G(u,v) 的值在将 x 方向的频率设为 u,y 方向的频率设为 v 时,表示 g(x,y) 的空间频率成分。以后,将 g(x,y) 的傅立叶图像称为 G(u,v),将 f(x,y) 的傅立叶图像称为 F(u,v),将 g′ (x,y) 的傅立叶图像称为 G′ (u,v),将 f′ (x, y) 的傅立叶图像称为 F′ (u, v)。此外,作为基底变换可以采用傅立叶变换以外的数学逻辑变换。

[0058] 接着，随机变换部 102 采用随机过滤器对所述傅立叶图像进行随机过滤器运算 (S504)。在登录时采用随机过滤器 K，对 G 以及 G′ 进行运算，在认证时采用逆随机过滤器 L 对 F 以及 F′ 进行运算。这里，K 以及 L 是如傅立叶图像这样的过滤器，按每个 x 方向的频率 u 以及 y 方向的频率 v 的组合具有值，可表示为 K(u,v)、L(u,v)。K(u,v)、L(u,v) 的值是随机的，且具有 K(u,v)·L(u,v) ＝ 1 这样的关系。作为随机过滤器运算的内容，在登录时计算 K(u,v)·G(u,v) 以及 K(u,v)·G′ (u,v)，在认证时计算 L(u,v)·F(u,v) 以及 L(u,v)·F′ (u,v)。以后，将这些计算结果称为随机图像。这样在不知道 K(u,v)、L(u,v) 时，因为不能由这些随机图像来恢复原始的图像 G(u,v) 及 F(u,v)，所以可以使指静脉 3 值图像对于服务器 130 隐匿。

[0059] 接着，参照图 6 对服务器 130 的对照部 134 的处理动作进行说明。服务器 130 向对照部 134 输入随机图像 L(u,v)·F(u,v)、L(u,v)·F′ (u,v) 以及样板 K(u,v)·G(u,v)、K(u,v)·G′ (u,v)。对照部 134，首先计算 L(u,v)·F(u,v) 与 K(u,v)·G(u,v) 的积，L(u,v)·F′ (u,v) 与 K(u,v)·G′ (u,v) 的积 (S601)。将计算结果分别称为 W(u,v)、W′ (u,v)。

[0060] 接着，对照部 134，对 W(u,v)、W′ (u,v) 进行逆基底变换 (S602)。这里，作为逆基底变换，以与傅立叶变换对应的逆傅立叶变换为例。作为 W(u,v) 的逆傅立叶变换的结果的 w(p,q)，表示针对 f(x,y) 将 g(x,y) 平行移动了 (p,q) 时的相互相关的值。另外，W′ (u,v) 的逆傅立叶变换 W′ (p,q)，同样表示针对 f′ (x,y) 将 g′ (x,y) 平行移动了 (p,q) 时的相互相关的值。此外，如果作为基底变换采用傅立叶变换以外的数学逻辑变换等，则最好采用对应的逆变换。

[0061] 接着，对照部 134 根据 w(p,q)、w′ (p,q)、Sg、Sf 来计算失配率 Rm(p,q) (S603)。失配率 Rm(p,q)，将 Sf+Sg-[w(p,q)-w′ (p,q)]/2 除以 Sf+Sg。计算将 (p,q) 作为变量时的失配率 Rm(p,q) 的最小值，并与设定的阈值比较，在比阈值小时判定为本人，在比阈值大时判定为他人 (S604)。

[0062] 这里，无需由随机图像 K(u,v)·G(u,v)、K(u,v)·G′ (u,v)、L(u,v)·F(u,v)、L(u,v)·F′ (u,v) 恢复 3 值或者 2 值图像、来进行对照，这点是应该注意的。即，可以保持着对于服务器 130 隐匿了指静脉的 3 值图像或者 2 值图像的状态，进行认证处理。由此，可以实现样板（这里是指静脉的 3 值图像或者 2 值图像）保护型的指静脉认证。此外，在本实施方式中，对服务器 130 公开 Sf 以及 Sg，但是由这些来恢复原始的 3 值图像是困难的，所以在隐匿上不构成问题。

[0063] 此外，在本实施方式中，根据以下这样的方法，也可以使原始的 3 值图像的恢复困难性提高。这个可以通过将数学逻辑变换使用到在随机变换部 102 中的基底变换 (S303) 来实现。首先对 2 维时的数学逻辑变换进行概略说明。给出 2 维数据列 d(x,y)，将 x、y 的范围设为 0 ≤ x ≤ N-1、0 ≤ y ≤ N-1。作为某整数 M，存在满足下式的 1 的原始 N 次方根 α。

[0064] [公式 1]

[0065] $\alpha^N = 1 \pmod{M}$

[0066] 对于 d(x) 的数学逻辑变换，以将整数 M 作为模的运算为基础通过以下公式来定义。

[0067] [公式 2]

[0068] $$D(u, v) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} d(x, y)\alpha^{ux+vy} \qquad (0 \le u, v \le N-1)$$

[0069] 逆变换用下式来定义。

[0070] [公式 3]

[0071] $$d(x, y) = N^{-1} \cdot N^{-1} \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} D(u, v)\alpha^{-(ux+vy)} \qquad (0 \le x, y \le N-1)$$

[0072] 在本实施方式中，对上述的3值图像(g(x,y)或者f(x,y))以及2值图像(g′ (x,y)或者f′ (x,y))进行2维数学逻辑变换，生成变换后图像Gn(u,v)、G′ n(u,v)、Fn(u,v)、F′ n(u,v)。在登录时，使在上述的随机变换中采用的随机过滤器K(u,v)作用于Gn(u,v)和G′ n(u,v)，而此时将整数M作为模进行乘法运算。另外，与上述的逆随机过滤器L(u,v)对应的，是采用将K(u,v)的整数M作为模时的逆元Ln(u,v)。即，K(u,v)·Ln(u,v) = 1(mod M)成立。在认证时使该Ln(u,v)作用于Fn(u,v)、F′ n(u,v)。

[0073] 接着，参照图7，对恢复困难性提高的理由进行说明。这里，以K(u,v)·Gn(u,v)举例。攻击者，在K(u,v)·Gn(u,v)已知的情况下，以知道K(u,v)以及Gn(u,v)为目的。将整数M作为模求K(u,v)·Gn(u,v)，而且在通过作为单纯的整数的运算来求出的K(u,v)·Gn(u,v)比M还大时，如在图7的实数直线上所示，将这个视为与用M除以后的余数相同。因此，在此例中，K(u,v)·Gn(u,v)为比K(u,v)、Gn(u,v)各自的值小的值。其结果是，作为攻击者应该求出的K(u,v)、Gn(u,v)的候补，得到比K(u,v)·Gn(u,v)小的K(u,v)、Gn(u,v)。

[0074] 另一方面，在采用上述傅立叶变换时，得不到这样的候补。因此，对于攻击者来说，由于可能值的组合增大，所以循环攻击所需的计算量增大，由此，在事实上，恢复困难性提高。

[0075] 为了回避从服务器130泄漏样板后被重复攻击等风险，最理想的是定期的、或者在发觉样板泄漏时，更新在服务器130上登录的、可取消化的样板。此时，也以不进行指静脉自体的再登录、来降低对用户的负担为目的。以下，对于样板更新方法的例子进行叙述。另外，该例子以在随机变换的基底变换中采用傅立叶变换为前提进行说明，不过数学逻辑变换等其它的基底变换也可以适用。

[0076] 图8表示样板更新方法的处理动作。客户机100新生成随机过滤器对(S801)。这里，将原有的随机过滤器对设为(K_1、L_1)，将新的随机过滤器对设为(K_2、L_2)。随机过滤器对的生成方法可以按照之前所述的例子。

[0077] 接着，客户机100将新的逆随机过滤器L2写入便携型记录介质中，并覆盖原有的逆随机过滤器L1(S802)。接着，客户机100计算K_2/K_1，并将这个作为随机过滤器差分ΔK(S803)。接着，服务器130从客户机100接收随机过滤器差分ΔK，并作用于原有的样板K_1G(S804)。即，计算ΔK(u,v)·K_1(u,v)G(u,v)。因为ΔK(u,v) = K_2(u,v)/K_1(u,v)，所以此值等于K_2(u,v)G(u,v)。接着，服务器130将K_2(u,v)G(u,v)作为样板来登录，并更新样板(S805)。

[0078] 通过以上的处理，在没有将新旧随机过滤器K_1、K_2向服务器130泄漏的情况下，无需再次登录指静脉自体，就能进行样板更新。由此既降低用户的指静脉再登录的负担，又更新可取消化的样板，这样可以回避重复攻击等风险。

[0079] 涉及上述实施方式的、将生物体信息登录到服务器上进行对照的生物体认证系统，也可以适用于其它例，而并非仅限定在上述例中。例如，可适用于公司内网络中的信息访问控制、或网上银行业务系统、ATM（银行自动提取装置）中的本人确认、或向面向会员Web站点的注册、或进入到保护区时的入场时的个人认证等。

[0080] 此时，假设同一个人为了利用多个系统而在各个系统上登录生物体信息这样的情况，在此情况下最理想的是与作为对象的系统相对应，变更上述过滤器以及逆过滤器的系数来适用。通过这样预先变更系数，可以针对来自某系统的生物体信息的泄漏，保护在其它系统中的相同生物体信息的利用。

[0081] [实施例2]

[0082] 接着，参照图9至12，对第二实施方式进行说明。本实施方式是这样的可取消指纹认证系统：在对服务器保持着隐匿指纹图像的状态下，在服务器内进行指纹对照。

[0083] 图9表示可取消指纹认证的系统结构。该可取消指纹认证系统的结构为：进行样板的保管和对照的服务器930，经由因特网及内部网这样的网络，与进行登录·认证时的指纹图像取得、2值图像生成、中心·特征点提取、图像切出、以及随机变换的客户机终端（以及仅称客户机）900连接。

[0084] 客户机900由用户自身或者可以信赖的第三者来进行管理，其具有进行指纹图像化的指纹传感器910，并且使用用户携带的便携型记录介质920。便携型记录介质920与上述第一实施例相同，是由用户持有且管理的、如IC卡或USB存储器的存储介质。例如，从自己家进行网上银行业务时也可以成为这样的构成，客户机900是用户管理的自家PC，服务器930为银行管理的服务器机器。

[0085] 客户机900的结构为具有以下各部：2值图像生成部901，其使指纹图像2值化；核心·特征点提取部902，其从2值图像上检测核心（指纹旋涡的中心）和特征点（指纹隆线的端点以及分歧点）的位置；伪特征点生成部903，其随机生成与本来的特征点坐标不同的伪特征点坐标；随机过滤器生成部904，其针对各特征点（原来特征点与伪特征点）生成随机过滤器对；图像切出部906，其以各特征点为中心切出小片(chip)图像或者周边图像；随机变换部907，其针对各小片图像或者周边图像分别采用随机过滤器变换2值图像来生成随机图像；记录介质I/F部905，其在与便携型记录介质920之间进行通信；和通信部908，其经由网络进行通信。上述2值图像生成部901、核心·特征点提取部902、伪特征点生成部903、随机过滤器生成部904、图像切出部906、随机变换部907的处理，可以通过客户机900的处理器执行程序来实现。此外，2值图像生成、核心·特征点提取、图像切出，例如也可以通过特开2001-344213号公报(US 20020150283，EP 1313026)所公开的方法来实现。

[0086] 服务器930的结构为具有以下各部：通信部931，其经由网络进行通信；登录部932，其将随机图像作为样板来登录；存储装置933，其存储样板；和对照部934，其将在认证时新接收的随机图像与样板对照并计算类似度。登录部932以及对照部934中的处理，通过服务器930执行程序来实现。

[0087] 在此，所谓类似度是分别比较了在登录时切出的多个小片图像和在对照时切出的多个周边图像时的、一致的图像数目。类似度越大，表示登录指纹和对照指纹越相似。小片图像与周边图像的一致/不一致，以在重合了图像时一致的像素数为基础进行判断。但是，在登录时与对照时，存在由于失真或旋转等影响造成特征点位置偏移的情况，所以周边图

像的尺寸比小片图像的尺寸取得大，一边使小片图像在周边图像上平行移动，一边探索一致像素数为最大的位置，以该最大值为基础判断一致 / 不一致。更详细的内容可以通过特开 2001-344213 号公报 (US 20020150283，EP 1313026) 的记载来理解。

[0088] 以下，采用图 10 以及图 12 对本实施方式中的指纹登录处理动作进行说明。首先，客户机 900 取得用户的指纹图像 (S1001)。接着，使取得的指纹图像 2 值化，生成登录用 2 值图像 1200(S1002)。这里，各像素值为 -1(白) 或者 1(黑)。接着，从登录用 2 值图像中提取核心以及特征点的位置，将核心位置作为原点 (0,0) 计算各特征点的坐标 (S1003)。此外，除了抽出的特征点之外，作为伪特征点生成多个随机的坐标 (S1004)。以下，将本来的特征点和伪特征点综合起来，称为特征点。接着，以各特征点坐标 (Xi,Yi)(i ＝ 1,...,n) 为中心从登录用 2 值图像中切出规定尺寸 (w×w 像素) 的小片图像 1201(gi)(S1005)。

[0089] 接着，针对各特征点，生成随机过滤器对 (Ki,Li)(S1006)。这里将 Ki 称为随机过滤器，Li 称为逆随机过滤器。随机过滤器 Ki 的尺寸为 W×W 像素 (W ≥ w)，与所述第一实施例相同，随机生成各像素值。另外，将 Ki 的各像素值取逆后的值作为逆随机过滤器 Li。接着，将特征点坐标和逆随机过滤器的组 1204(Xi,Yi,Li)(i ＝ 1,...,n) 写入便携型记录介质 920(S1007)。

[0090] 接着，采用随机过滤器 Ki 变换各小片图像 1201(gi)，生成随机图像。具体来说，用 0(灰色) 来填充小片图像 1201(gi) 的四周，扩张为 W×W 像素，将这个进行基底变换 (数学逻辑变换或者傅立叶变换)。将基底变换后的图像 1202(W×W 像素) 设为 Gi。按各像素对 Gi 乘以随机过滤器 Ki，来生成随机图像 1205(Gi •Ki)。对各小片图像 gi(i ＝ 1,...,n) 来进行这个处理。将生成后的随机图像 Ki •Gi(i ＝ 1,...,n) 发送到服务器 930 上 (S1008)。服务器 930 接收随机图像 Ki • Gi，并将这个作为样板来登录 (S1009)。

[0091] 以下，采用图 11 以及图 12 对本实施方式中的指纹认证处理动作进行说明。首先，客户机 900 取得用户的指纹图像 (S1101)。接着，使取得的指纹图像 2 值化，生成对照用 2 值图像 1210(S1102)。这里，各像素值为 -1(白) 或者 1(黑)。接着，由便携型记录介质 920 读入特征点坐标和逆随机过滤器的组 1204(Xi,Yi,Li)(i ＝ 1,...,n)(S1103)。接着，从对照用 2 值图像中切出以各特征点坐标 (Xi,Yi) 为中心的周边图像 1211(fi)(S1104)。周边图像的尺寸为 W×W 像素。接着，按各像素使基底变换 (数学逻辑变换或者傅立叶变换) 了周边图像 fi 的图像 1212(Fi) 和逆随机过滤器 Li 相乘，由此生成随机图像 1214(Fi • Li)。对各周边图像 fi(i ＝ 1,...,n) 进行该处理。将生成后的随机图像 Fi •Li(i ＝ 1,...,n) 发送到服务器 930 上 (S1105)。

[0092] 服务器 930 接收随机图像 Fi • Li，与样板中的各随机图像 Gi • Ki 对照，判定小片图像 1201(gi) 和周边图像 1211(fi) 一致 / 不一致。具体来说，按每一像素使随机图像彼此间相乘。因为 Li 各像素值是 Ki 各像素值的倒数，所以通过相乘相互抵消，成为 (Fi • Li) • (Gi • Ki) ＝ Fi • Gi。对这个进行逆基底变换 (逆数学逻辑变换或者逆傅立叶变换)，得到 fi 与 gi 的相关图像 1215。相关图像上坐标 (ΔX，ΔY) 中的像素值，表示使小片图像 gi 在周边图像 fi 上平行移动 (ΔX，ΔY) 后相互重合时的相关值。因为 2 值图像的各像素值是 -1(白) 和 1(黑)，所以得到 :

[0093] 相关值＝ (白黑一致时的像素数)-(白黑不一致时的像素数) ＝ 2×(白黑一致时的像素数)-W×W。

[0094] 因此，通过将相关图像上像素值（相关值）的最大值与规定的阈值比较，可以判定2值图像 fi 与 gi 一致／不一致。这样按各小片图像、周边图像的对判断一致／不一致，计数一致的图像的数目来作为类似度 (S1106)。最后，将类似度与规定的认证阈值比较，如果在认证阈值以上则判定指纹一致，如果未达到认证阈值则判定为不一致 (S1107)。

[0095] 如以上所述，根据本实施方式的指纹认证，将指纹的小片图像以及周边图像通过随机过滤器以及逆随机过滤器干扰之后向服务器发送，所以尽管服务器不能知道原始的图像，但仍可以进行相关值的计算。由此，用户可以对服务器在保持着隐匿指纹的状态下接受指纹认证。此外，还考虑了如第一实施方式那样变换、对照全体指纹图像的方法，但是由于指纹与指静脉不同容易产生失真，所以在基于全体图像相关的对照中不能得到足够的认证精度。与此相对，通过局部地观察图像来判断一致／不一致，可以降低失真的影响。尤其因为指纹的特征点（端点或者分歧点）周边具有特殊的构造，所以适合于指纹的识别。

[0096] 在本实施方式中，需要预先记录特征点坐标。特征点坐标其自身是识别指纹有力的信息，可以说是一种指纹信息。因此，在从客户机泄漏了特征点坐标时，有可能成为用来伪造指纹的线索。因此在本实施方式中，可以通过追加伪特征点，来排除这样的危险性。因为伪特征点的小片图像不仅本人指纹就连他人指纹一致的概率也较高，所以与仅使用本来的小片图像的情况相比，对本人／他人一致的小片数（类似度）都增加，只要使认证阈值适当增加这个量，就不会出现精度下降。

[0097] 此外，本发明还可以以各种变形来实施，而并不仅限定在上述实施方式中。例如，在图 1 例中，构成这样的结构 :进行由指静脉传感器 110 提取个人生物体信息、在客户机 100 内生成登录图像以及对照图像等处理。可是，根据其它变形例，还可以通过将图 1 所示的客户机 100 内的各功能 101 ～ 105 与指静脉传感器 110 一体安装，来构成生物体设备。利用此构成的生物体设备，携带生物体设备，可以在任意的时间、场所提取个人生物体信息利用在个人认证中。此外不言而喻，本发明还可适用于基于手相及其它生物体信息的认证，而并不仅限定在上述实施例中所述的基于指静脉及指纹的认证。

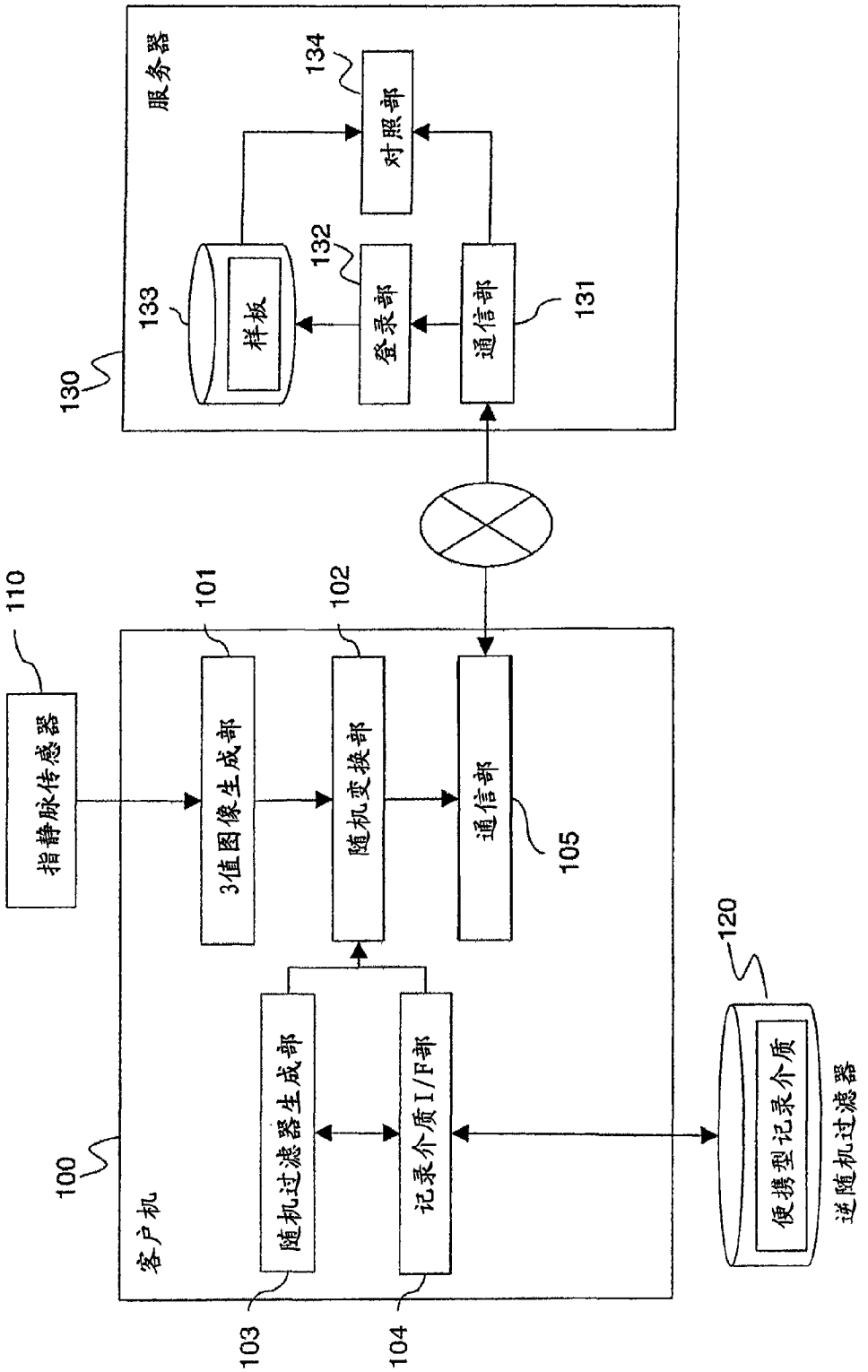

服务器
130
133
样板
132
登录部
131
通信部
134
对照部
客户机
100
指静脉传感器
110
3值图像生成部
101
随机变换部
102
通信部
105
随机过滤器生成部
103
记录介质I/F部
104
便携型记录介质
120
逆随机过滤器

图 1

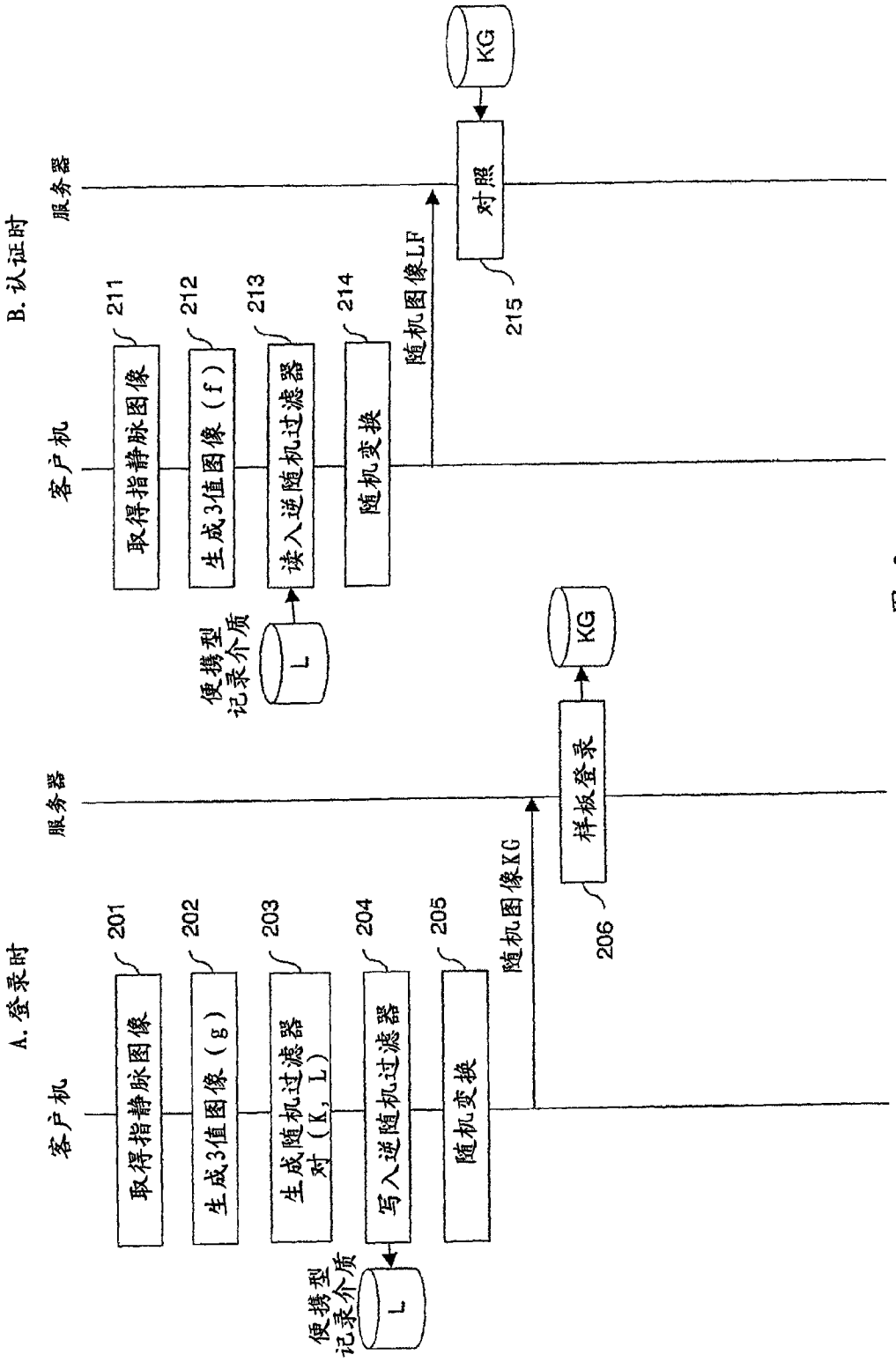

A. 登录时
客户机
服务器
取得指静脉图像
201
生成3值图像（g）
202
生成随机过滤器对（K，L）
203
写入逆随机过滤器
204
随机变换
205
便携型记录介质
L
随机图像KG
样板登录
206
KG
B. 认证时
客户机
服务器
取得指静脉图像
211
生成3值图像（f）
212
读入逆随机过滤器
213
随机变换
214
便携型记录介质
L
随机图像LF
对照
215
KG

图 2

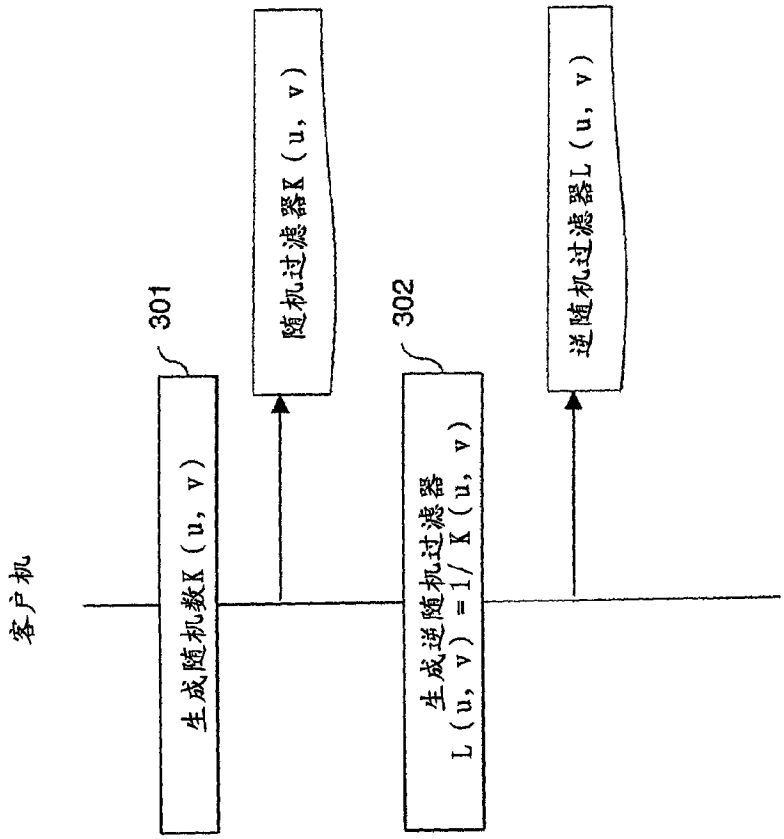


图 3

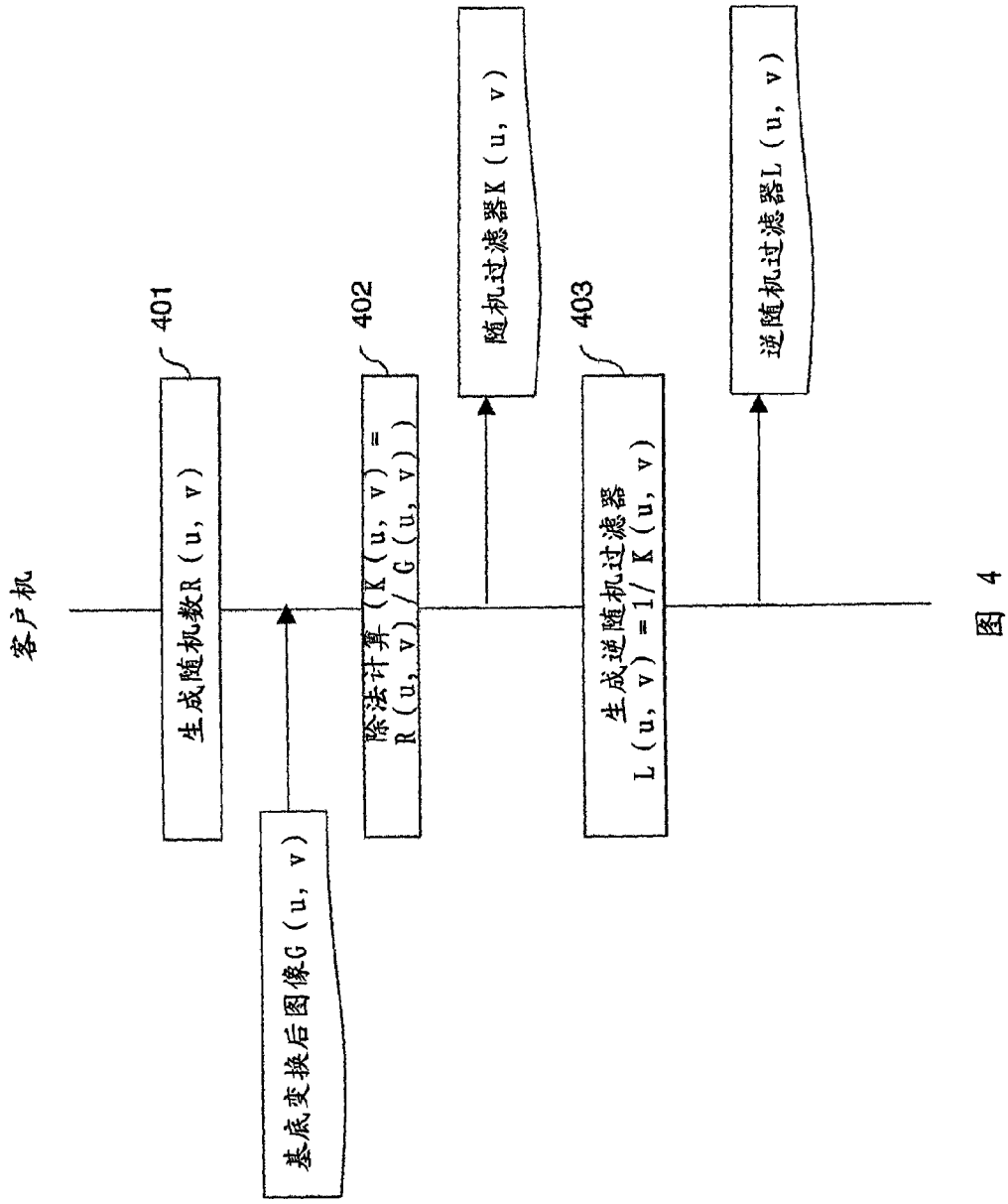

客户机
401
生成随机数R（u，v）
402
除法计算（K（u，v）=
R（u，v）/ G（u，v））
403
生成逆随机过滤器
L（u，v）=1/ K（u，v）
基底变换后图像G（u，v）
随机过滤器K（u，v）
逆随机过滤器L（u，v）

图 4

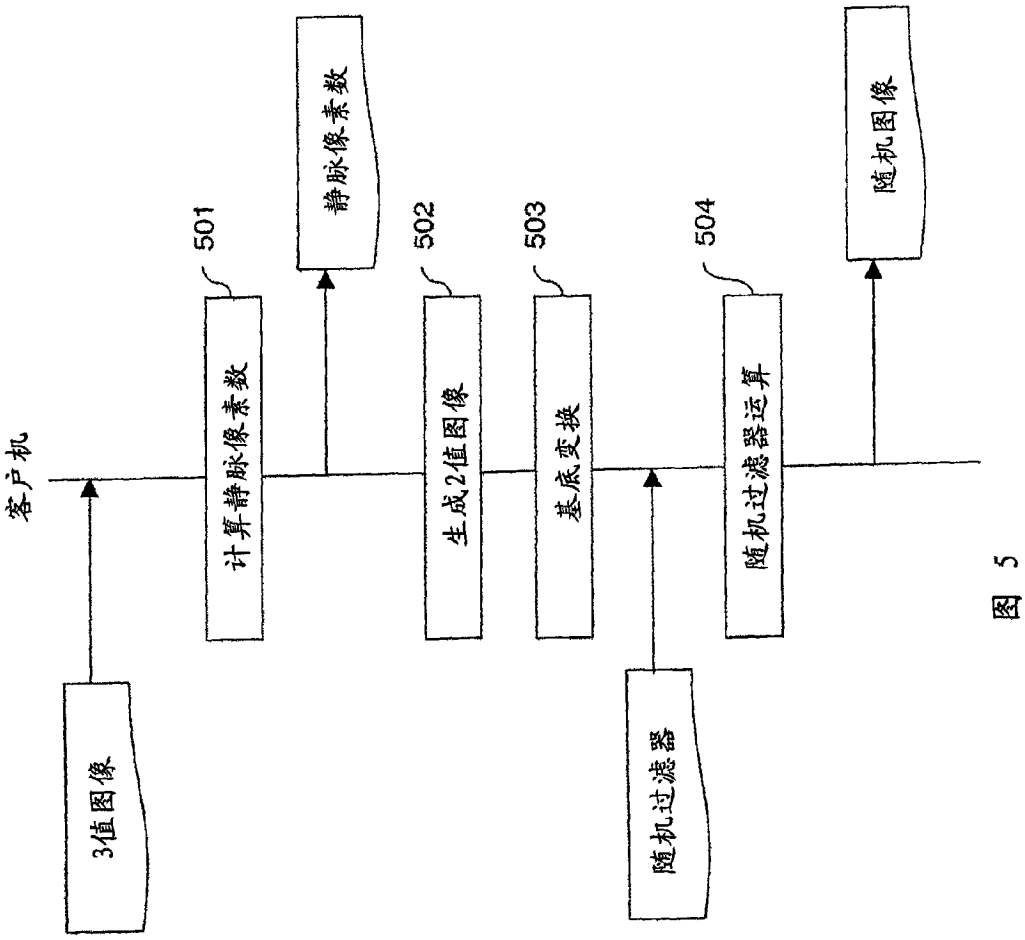

客户机
3值图像
501
计算静脉像素数
静脉像素数
502
生成2值图像
503
基底变换
随机过滤器
504
随机过滤器运算
随机图像

图 5

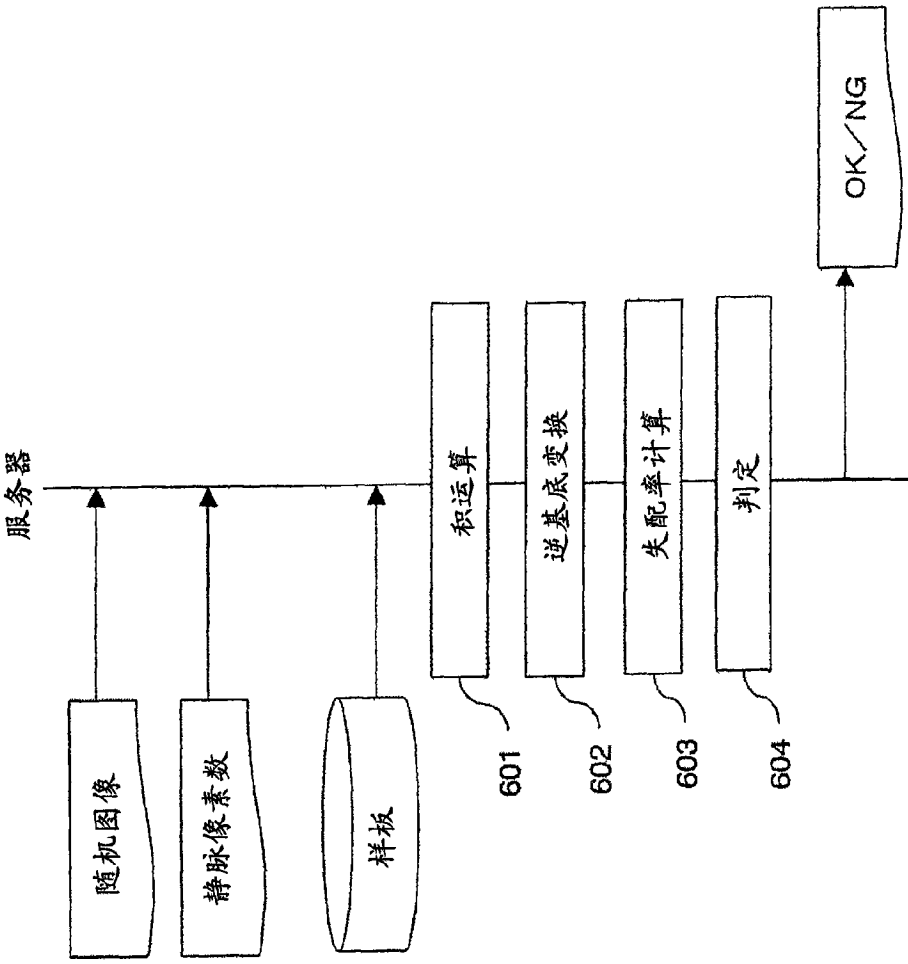


图 6

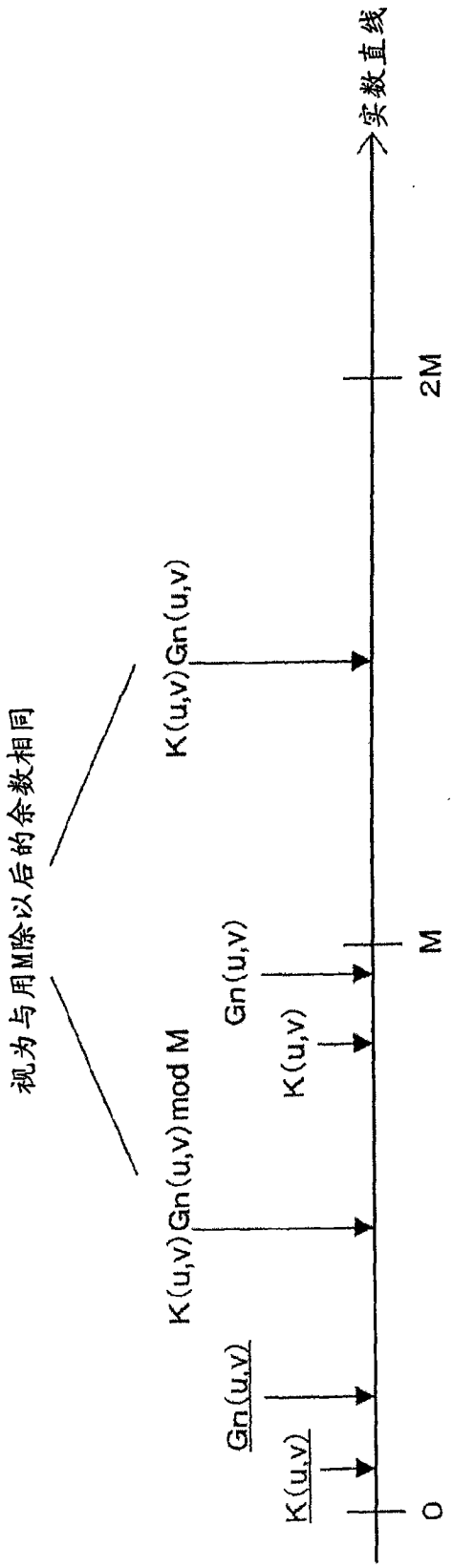

实数直线
0
M
2M
K(u,v)
Gn(u,v)
K(u,v)
Gn(u,v)
视为与用M除以后的余数相同
K(u,v)
Gn(u,v) mod M
K(u,v)
Gn(u,v)

图 7

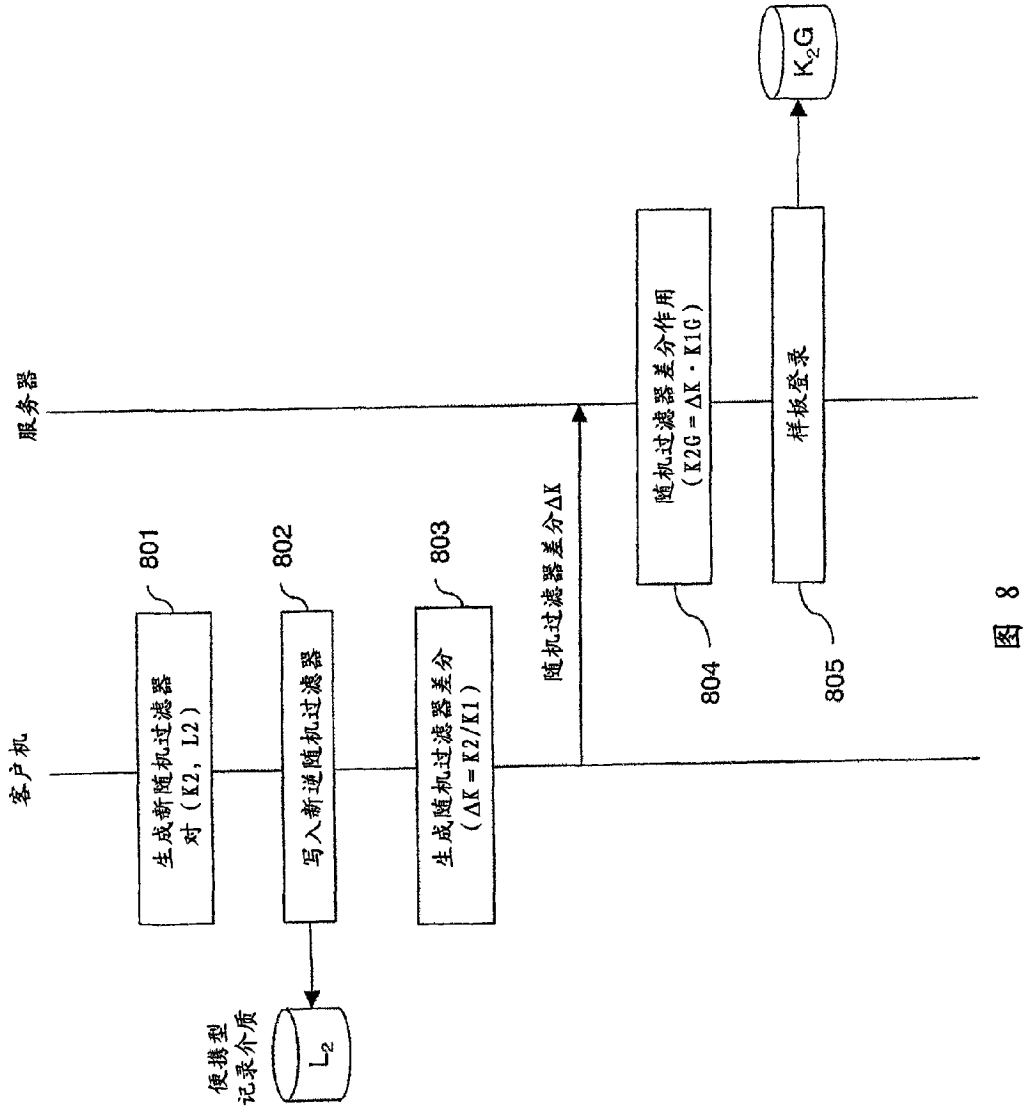

服务器
客户机
801
802
803
804
805
生成新随机过滤器对（K2，L2）
写入新随机过滤器
生成随机过滤器差分（ΔK = K2/K1）
随机过滤器差分ΔK
随机过滤器差分作用（K2G = ΔK · K1G）
样板登录
K_2G
L_2
便携型记录介质

图 8

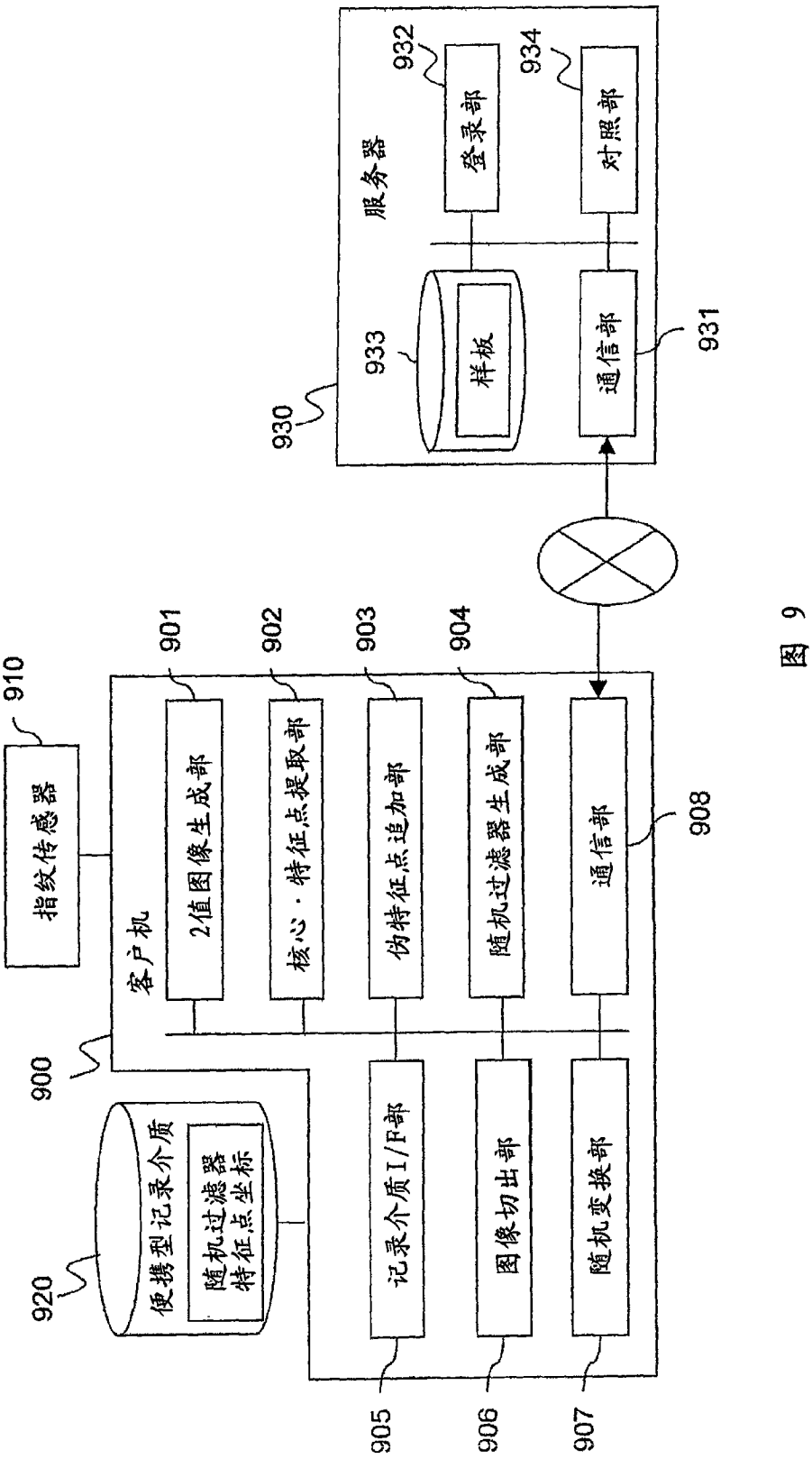

930
服务器
933
样板
932
登录部
934
对照部
931
通信部
910
指纹传感器
900
客户机
901
2值图像生成部
902
核心·特征点提取部
903
伪特征点追加部
904
随机过滤器生成部
908
通信部
920
便携型记录介质
随机过滤器
特征点坐标
905
记录介质I/F部
906
图像切出部
907
随机变换部

图 9

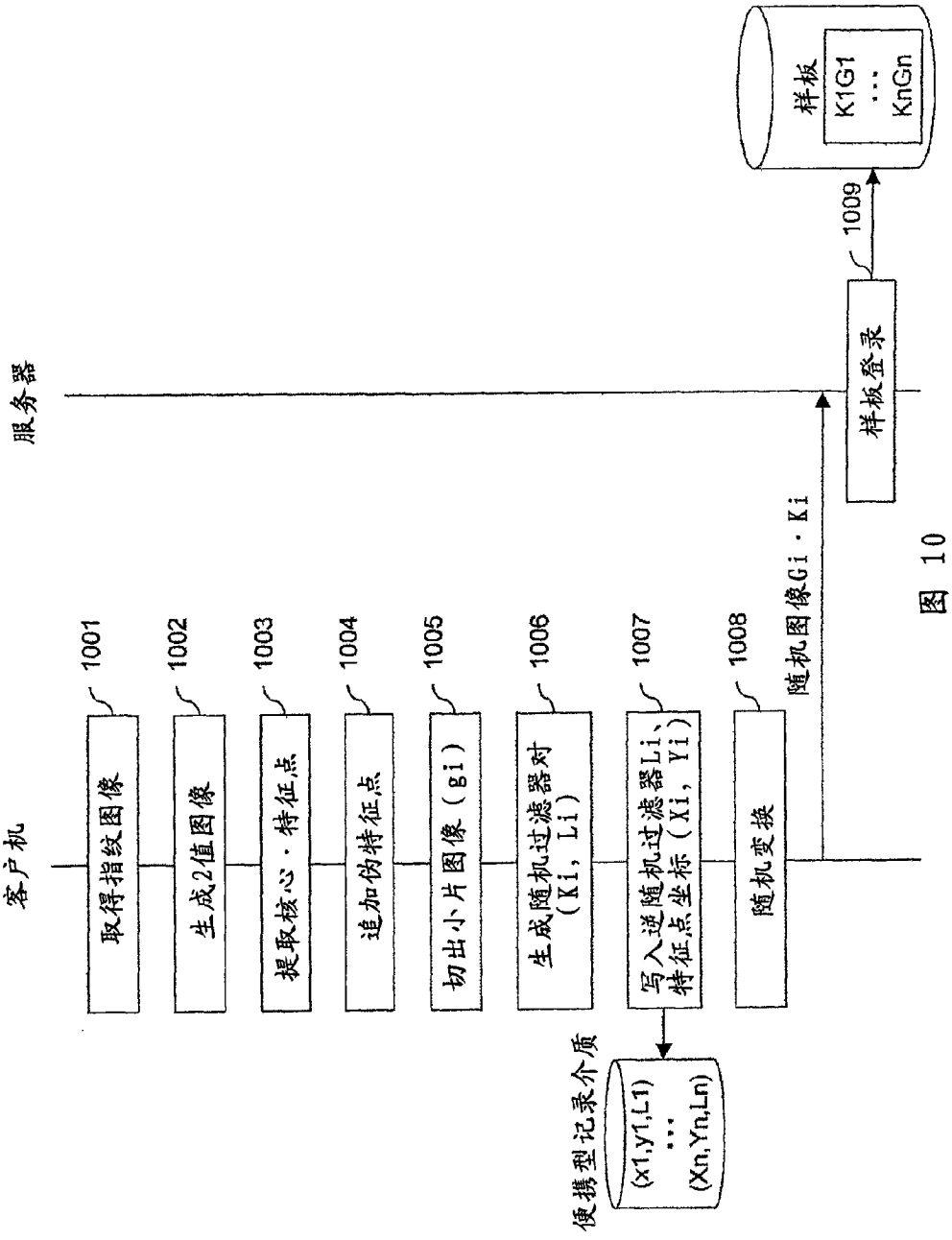

客户机
服务器
取得指纹图像
1001
生成2值图像
1002
提取核心·特征点
1003
追加伪特征点
1004
切出小片图像（gi）
1005
生成随机过滤器对（Ki，Li）
1006
写入逆随机过滤器Li、特征点坐标（Xi，Yi）
1007
随机变换
1008
随机图像Gi·Ki
样板登录
1009
样板
K1G1
…
KnGn
便携型记录介质
(x1,y1,L1)
…
(Xn,Yn,Ln)

图 10

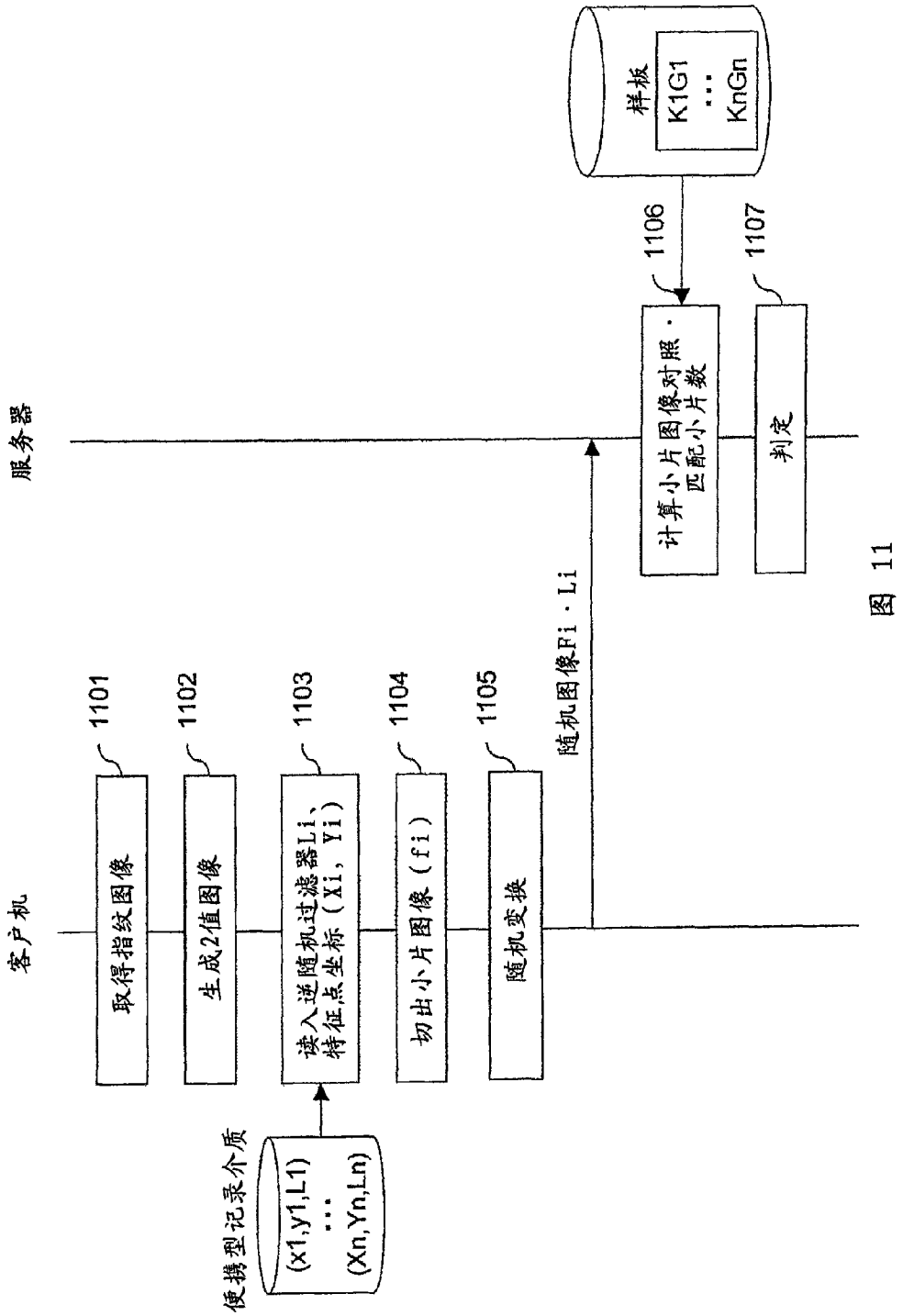

客户机
服务器
便携型记录介质
(x1,y1,L1)
...
(Xn,Yn,Ln)
取得指纹图像
1101
生成2值图像
1102
读入逆随机过滤器Li、特征点坐标（Xi，Yi）
1103
切出小片图像（fi）
1104
随机变换
1105
随机图像Fi · Li
样板
K1G1
...
KnGn
1106
计算小片图像对照 · 匹配小片数
1107
判定

图 11

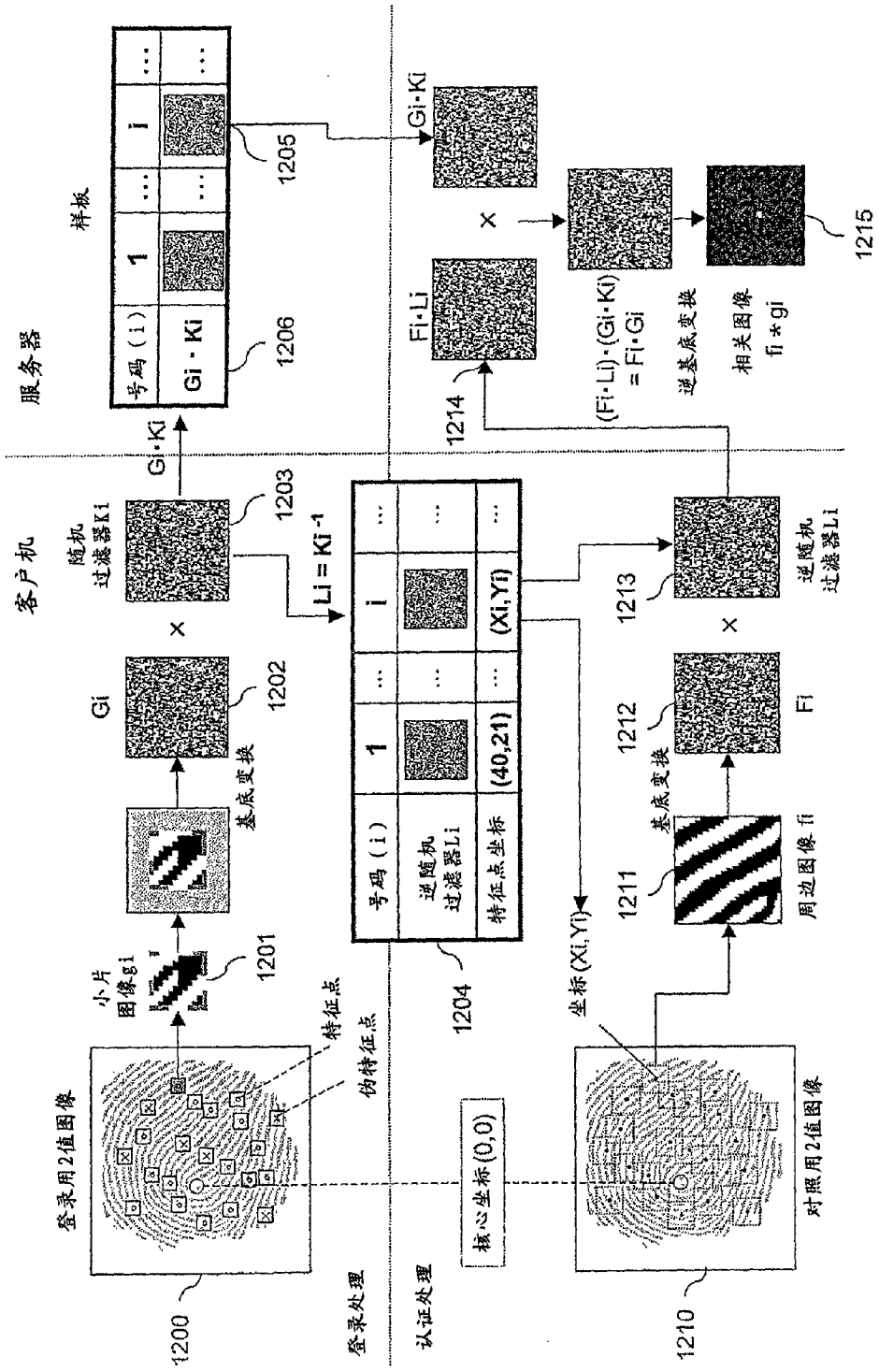

登录用2值图像
小片图像gi
特征点
伪特征点
基底变换
Gi
随机过滤器Ki
Gi·Ki
服务器
样板
号码(i)
Gi·Ki
1
i
1205
1206
客户机
Li = Ki⁻¹
1203
1202
1201
1200
登录处理
认证处理
核心坐标(0,0)
号码(i)
逆随机过滤器Li
特征点坐标
(40,21)
(Xi,Yi)
1204
坐标(Xi,Yi)
1211
基底变换
1212
Fi
周边图像 fi
对照用2值图像
1210
逆随机过滤器Li
1213
Fi·Li
1214
(Fi·Li)·(Gi·Ki)
= Fi·Gi
逆基底变换
相关图像
fi * gi
1215

图 12