[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
G06F 17/30 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710089466.3

[43] 公开日 2007 年 8 月 29 日

[11] 公开号 CN 101025778A

[22] 申请日 2001.7.23
[21] 申请号 200710089466.3
分案原申请号 01815535.9
[30] 优先权
[32] 2000. 7.25 [33] JP [31] 2000 - 223940
[32] 2000. 9.20 [33] JP [31] 2000 - 284811
[32] 2000.12.27 [33] JP [31] 2000 - 396990
[71] 申请人 有限会社信息安全
地址 日本大阪府
[72] 发明人 国米仁 桝野隆平 栗山雅行

[74] 专利代理机构 北京银龙知识产权代理有限公司
代理人 许 静

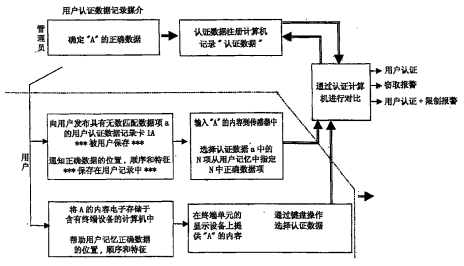
权利要求书 5 页 说明书 16 页 附图 16 页

[54] 发明名称

保密信息记录媒介、保护方法、保护存储方法及信息访问报警系统

[57] 摘要

一种加密密钥和系统的保密信息的保护，用于当访问加密信息时，通知窃取，限制或其他非常情况的发生。 保密信息包括大量的虚假数据和混在虚假数据中的单项或多项真实数据。 包括虚假数据和真实数据的保密数据是二维码数据，该码构成具有不同区域的组。 将分布混在虚假数据的真实数据的位置和次序报告给用户，用户加入预定的报警信号。 当用户输入密码告知其处于第三方控制之下时，系统可以检测出报警信号并且获知用户处于不正常状态，系统执行正常识别程序，采取保护措施。 虚假数据部分定义为限制报告数据并加入到真实数据中，只要包括了至少一项限定报告数据，就可以判断用户本身处于第三方控制之下，然后识别用户并且发出限定报告警告。



1．一种保密信息记录媒介，

其中单个真实数据项分布于无数虚假数据项中，并且虚假数据和真实数据由在具有不同区域的多组中的二维空间码数据组成，并且

其中确定分布于无数虚假数据项中的真实数据项的位置并将其提供给用户，

该记录媒介具有说明、图形等，其由无数虚假数据项和真实数据项组成，其中，分布于无数虚假数据项中的真实数据项的位置是按照急于有含义的信息的用户本身的记忆确定和选择时，说明，图形等作为辅助装置加入。

2．一种保密信息记录媒介，

其中单个真实数据项分布于无数虚假数据项中，并且虚假数据和真实数据由在具有不同区域的多组中的二维空间码数据组成，并且

其中确定分布于无数虚假数据项中的真实数据项的位置和／或存储顺序并将其提供给用户，

该记录媒介具有说明、图形等，其由无数虚假数据项和真实数据项组成，其中，分布于无数虚假数据项中的真实数据项的位置是按照基于有含义的信息的用户本身的记忆确定和选择时，说明，图形等作为辅助装置加入。

3．根据权利要求 1 或 2 的保密信息记录媒介，

其中单个真实数据项分布于无数虚假数据项中，并且虚假数据和真实数据由在具有不同区域的多组中的二维空间码数据组成，并且

其中确定分布于无数虚假数据项中的真实数据项的位置并将其提供给用户，

该记录媒介具有色彩，说明、照片，地形等，构成关于无数虚假数据项和真实数据项的背景，其中当分布于无数虚假数据项中的真实数据项的位置是按照基于有含义的信息的用户本身的记忆确定和选择时，该背景，如色彩，说明、照片，地形等作为辅助装置加入。

4. 根据权利要求 1 或 2 的保密信息记录媒介，该记录媒介具有色彩，说明、照片，地形等，构成关于无数虚假数据项和真实数据项的背景，

其中当分布于无数虚假数据项中的真实数据项的位置是按照基于有含义的信息的用户本身的记忆确定和选择时，该背景，如色彩，说明、照片，地形等作为辅助装置加入。

5. 一种保密信息保护方法，

其中被使用二维空间码进行加密形成带有加密密钥保密信息的单个真实数据项被插入在无数虚假数据项中，其中带有加密密钥的保密信息被用于进入限制和/或操作限制控制，并且

其中与无数虚假数据项相关的真实数据项的位置保存在基于有含义的信息的用户的记忆中用于记忆认证以防止任何未经授权的人对保密信息进行解密。

6. 一种保密信息保护方法，

其中被使用二维空间码进行加密形成带有加密密钥保密信息的多个真实数据项被插入在无数虚假数据项中，其中带有加密密钥的保密信息被用于进入限制和/或操作限制控制，并且

其中与无数虚假数据项相关的真实数据项的位置和存储顺序保存在基于有含义的信息的用户的记忆中用于记忆认证以防止任何未经授权的人对保密信息进行解密 。

7. 根据权利要求 5 或 6 的保密信息保护方法，其中所描述的错误和正确的数据被打印在一张纸卡上，因此能够被光学读卡机读取用于数据复制。

8. 一种保密信息保护方法，

其中指示用于加密的保密信息的解密密钥的真实数据项分布于无数用于混淆的虚假数据项中，并且分布于无数虚假数据项中的真实数据项的位置和读取顺序保存于基于有含义的信息的用户记忆中。

9. 一种保密信息保护方法，

其中正确信息被分割成多项并且分布于无数错误信息项中用于隐藏正确的信息，

其中提供用于指示正确信息项位置的无数真实数据项和用于指示错误信息项位置的无数虚假数据项，

并且其中分布于无数虚假数据项中的真实数据项的位置和存储顺序从基于有含义的信息的用户记忆中进行确定。

10．根据权利要求9的保密信息保护方法，

其中正确信息被分割成多项并且分布于无数错误信息项中用于隐藏正确的信息，

其中提供用于指示正确信息项位置的无数真实数据项和用于指示错误信息项位置的无数虚假数据项，并且

其中通过使用图片将分布于无数虚假数据项中的真实数据项的位置和存储顺序从基于有含义的信息的用户记忆中进行确定，其中图片包括色彩、说明、图形和图片规定部分的地形。

11．一种在访问保密信息时，用于报告窃取，限制等非常情况的系统，

其中通过选择与记录在记录媒介上的相匹配的数据项至一定数量从而包含单个的真实数据项和多个虚假数据项，以向用户提供认证数据记录媒介，该记录媒介中具有分布的单个的真实数据项和多个虚假数据项，该匹配数据由符号，标记，照片，二维数据码等组成，

其中在用户认证数据记录媒介上用加密密钥加密的记录保密信息中，无数个匹配数据项中的一个被确定为正确的数据并且剩余的匹配数据项被确定为虚假数据，

其中通过单个真实数据项指示的信息被确定为指示在用户认证数据记录媒介上用加密密钥加密的保密信息的认证数据，

其中在使用用户认证数据记录媒介进入认证数据过程中，从用户认证数据记录媒介中选择单个真实数据项，从而确定选择了正确认证数据并且对用户认证进行有效性检验，而且

其中在通过用户认证数据记录媒介进行输入操作的过程中，从用户认证数据记录媒介中选择单个真实数据项时，如果在输入数据中包含至少一个虚假数据项，就可以确定有人正试图通过窃取的方式进行未授权

访问，然后产生一个窃取报警且使该用户的认证无效 。

12．一种在访问保密信息时，用于报告窃取，限制等非常情况的系统，

其中通过选择与记录在记录媒介上的相匹配的数据项至一定数量从而包含多个的真实数据项和多个虚假数据项，以向用户提供认证数据记录媒介，该记录媒介中具有分布的多个的真实数据项和多个虚假数据项，该匹配数据由符号，标记，照片，二维数据码等组成；

其中在用户认证数据记录媒介上用加密密钥加密的记录保密信息中，无数个匹配数据项中的几个通过指定其位置或顺序和特征，被确定为正确的数据并且剩余的匹配数据项被确定为虚假数据，并且通过多个真实数据项指示的信息被确定为指示带有加密密钥的保密信息的用户认证数据记录媒介上的认证数据；

其中从用户认证数据记录媒介中以正确的顺序且在通过用户认证数据记录媒介进行输入操作的过程中选择多个真实数据项，因此可确定正确匹配数据被选定并且对用户认证进行校验；

其中在利用用户认证数据记录媒介的装置进行输入操作过程中，如果选择的多个虚假数据项的数字少于确定数，验证第二认证输入；

其中在通过用户认证数据记录媒介进行输入操作的过程中，从用户认证数据记录媒介中选择多个真实数据项时，如果在输入数据中包含的虚假数据项的数目等于或大于预先确定的值，就可以确定有人正试图通过窃取的方式进行未授权访问，然后产生一个窃取报警且使该用户的认证无效；并且

其中发现产生窃取报警的控制中心阻止对所述的用户认证数据记录媒介的随后使用。

13．一种在访问保密信息时，用于报告窃取，限制等非常情况的系统，

其中通过选择与记录在记录媒介上的相匹配的数据项至一定数量从而包含单个或多个的真实数据项和多个虚假数据项，以向用户提供认证数据记录媒介，该记录媒介中具有分布的多个的真实数据项和多个虚假

数据项，该匹配数据由符号，标记，照片，二维数据码等组成；

其中在用户认证数据记录媒介上用加密密钥加密的记录保密信息中，无数个匹配数据项中的单个或几个通过指定其位置或顺序特征，被确定为正确的数据并且剩余的匹配数据项被确定为虚假数据，并且通过单个或多个真实数据项指示的信息被确定为指示带有加密密钥的保密信息的用户认证数据记录媒介上的认证数据，并且部分虚假数据被确定为限制信息数据；

其中在利用用户认证数据记录媒介的装置进行输入操作过程中，如果选择的多个虚假数据项的数字少于确定数，验证第二认证输入；

通过用户认证数据记录媒介进行输入操作的过程中，在用户认证数据记录媒介上从匹配数据中选择单个或多个真实数据项和选择读取顺序并向其中添加限制通知数据，因此确定已选择了正确认证数据并且对用户认证进行校验；并且

其中除真实数据外还包含至少一个限制通知数据项，从而确定用户处于一个未经授权的人的控制之下并且控制中心使用产生的限制信息报警对用户认证进行检 。

保密信息记录媒介、保护方法、保护存储方法及信息访问报警系统

本申请是国际申请日为 2001 年 7 月 23 日、申请号为 018155359、发明名称为"保密信息记录媒介、保护方法、保护存储方法及信息访问报警系统"的分案申请。

技术领域

本发明涉及包括加密密钥的保密信息的安全。此外，本发明还涉及用于包括加密密钥（如用户验证密码的使用）的保密信息的保护系统（如紧急情况通知系统）。

尤其是，本发明涉及包括加密密钥的保密信息的安全［如用于用户验证的个人身份信息、用于指示特定授权用户进入信息控制领域或识别操作者的信息、顾客的个人识别信息、敏感的个人信息（资产、证券评估和存储数据如存储空间）、敏感的公司信息如销售活动资料（顾客数据和商品数据）以及研究活动资料（如数学表达式、化学分子式、及其它在研究结果列表中的数字数据和在研究报告中的细节）］

例如，本发明涉及在电子商务中的用于用户验证的加密密钥以及那些用于保护存储在个人计算机或移动电话中的以防丢失和被窃取的保密信息的技术和那些用作登录限制控制或操作限制控制的加密密钥，以防止未经授权用户访问服务器中的存储媒介。

此外，本发明并不局限于在线应用，如在电子商务中的用户验证，也正在寻求用于离线应用，如在记录媒介上进行的记录、通过传真或邮件进行的传输打印输出或图像输出，以及以可移动或可存储的形式如打印的物质或软盘进行的传输和存储，以及其它广泛的应用，如在计算机的记录媒介上进行存储。

背景技术

为了保护这些多种保密信息,通常使用多位数和／或字符的密码和／

或IC卡。作为对这种早先的密码方法的改进或取代，还存在用户验证装置，其用于通过指纹或其它物理特征来验证用户。而IC卡在被丢失或盗窃后，IC卡可以被拥有者或授权用户之外的其它人使用。

此外，作为早先的一种以防验证卡丢失或被窃取的安全措施，其中在验证卡上记录有带有加密密钥的保密信息，来自于未经授权用户的认证请求被拒绝从而排斥此用户的在线连接，导致交易失败。然而，不存在这样的系统，其能够主动地使用于未经认证而进行访问的电子密钥（验证卡）失效或当出现对限制区域或电子设备进行未经认证的访问时而发出通知。

因此，如果记录有带有加密密钥的保密信息的验证卡丢失、被复制、和／或被窃取，当该卡被未经授权的人恶意使用时，当未经授权的人恶意的使用欺骗性的用户认证请求时，或当一个认证用户在未经授权的人恶意的控制下做出用户认证请求时（验证数据输入），没有一个安全的方法加以阻止。

发明内容

本发明的第一和第二实施例的目的就是提供隐蔽和存储保密信息的装置以及保护保密信息的方法，其中这些装置和方法中具有用户认证的功能但不需要指纹识别或其它物理特征方面的用户认证装置。这些实施例的另一目的是提供隐蔽、记录和存储保密信息如公司信息和技术信息的装置。

本发明的第三个目的就是探测来自于授权用户在未经授权的人恶意的控制下做出的访问，从而对用户和系统二者作出保护和维护。

本发明的第四个到第七个目的是建立一个报警系统和用于通知在出现对限制区域或电子设备进行未授权访问的系统，当带有加密密钥的信息、包括如保密信息的记录媒介、或具有如这种记录媒介的电子和／或通讯设备被窃取或丢失、或通过无效认证卡或泄漏的认证数据进行欺诈性的使用时，作为采取的安全措施。

本发明第一方面提供使用于保密信息的保密信息记录媒介，其中真实数据中的单个或多个数据项分布于无数虚假数据项中，并且虚假数据

和真实数据在具有不同区域的多组中组成二维空间码数据，并且在其中，基于有含义的用户本身的记忆，确定，提供和选择分布于无数虚假数据项中的真实数据项的位置和／或存储顺序。

本发明第二方面提供保密信息保护存储方法，其中使用二维空间码对真实数据中的单个或多个数据项加密形成的保密信息分布于无数虚假数据项中，并且其中与无数虚假数据项相关的真实数据项的位置和／或存储顺序保存于用于记忆认证（大脑认证）的用户记忆中，以防止任何未经授权的人对保密信息进行解密。

本发明第三方面提供保密信息保护存储方法，其中指示用于加密的保密信息的解密密钥的真实数据项分布于无数用于混淆的虚假数据项中，并且分布于无数虚假数据项中的真实数据项的位置和读取顺序保存于用户记忆中。

本发明第四方面提供对正确信息和错误信息交叉分布的保密信息进行隐藏、记录和存储的保密信息保护存储方法，其中正确信息被分割成多项并且分布于无数错误信息项中用于隐藏正确的信息，其中提供用于指示正确信息项位置的无数真实数据项和用于指示错误信息项位置的无数虚假数据项，并且其中分布于无数虚假数据项中的真实数据项的位置和存储顺序从用户记忆中进行确定。

当分布于无数虚假数据项中的真实数据项的位置和顺序从用户记忆中进行确定后，通过在本发明第四方面使用的图片，该图片包括色彩、说明、图形和地形，从而得到本发明的第四方面特征。

本发明第五方面提供访问保密信息时的用于报告如窃取或限制等非常情况的系统，其中通过选择与记录在记录媒介上的相匹配的数据项至一定数量从而包含单个的真实数据项和多个虚假数据项，以向用户提供认证数据记录媒介，该记录媒介中具有的匹配数据分布有单个的真实数据项和多个虚假数据项，其中在用户认证数据记录媒介上用加密密钥加密的记录保密信息中，无数个匹配数据项中的一个被确定为正确的数据并且剩余的匹配数据项被确定为虚假数据，其中通过单个真实数据项指示的信息被确定为指示在用户认证数据记录媒介上用加密密钥加密的保

密信息的认证数据，其中在使用用户认证数据记录媒介进入认证数据过程中，从用户认证数据记录媒介中选择单个真实数据项，从而确定选择了正确认证数据并且对用户认证进行有效性检验，且其中在通过用户认证数据记录媒介进行输入操作的过程中，从用户认证数据记录媒介中选择单个真实数据项时，如果在输入数据中包含一个虚假数据，就可以确定有人正试图通过窃取的方式进行未授权访问，然后产生一个窃取报警且使该用户的认证无效。

本发明第六方面通过在用户认证数据记录媒介中加入多个真实数据项而得到。

具体地，无数匹配数据项中的少数通过指定它们的位置和顺序而被确定为正确的数据，剩余的匹配数据项被确定为虚假数据，并且通过多个真实数据项指示的信息被确定为用户认证数据记录媒介上的认证数据。因此，从用户认证数据记录媒介中以正确的顺序且在通过用户认证数据记录媒介进行输入操作的过程中选择多个真实数据项，因此可确定正确匹配数据被选定并且对用户认证进行校验。

本发明第十方面通过确定部分虚假数据作为限制通知数据并将其加入到真实数据中使真实数据包括至少一个限制通知数据项，从而确定用户处于一个未经授权的人的控制之下并且通过产生的限制通知报警对用户认证进行检验而得到。

具体地，在用户认证数据记录媒介上记录用加密密钥加密的保密信息时，用事先确定的读取顺序来确定无数匹配数据项中的一项或几项为真实数据，剩余的匹配数据项被确定为虚假数据，通过单个或多个真实数据项以正确的读取顺序指示的信息被确定为认证数据，该认证数据在用户认证数据记录媒介上用加密密钥加密的保密信息，并且部分虚假数据被确定为限制信息数据。通过用户认证数据记录媒介进行输入操作的过程中，从匹配数据中选择单个或多个真实数据项和读取顺序并向其中添加限制通知数据，因此确定已选择了正确认证数据并且对用户认证进行校验。然后，除真实数据外还包含至少一个限制通知数据项，从而确定用户处于一个未经授权的人的控制之下并且控制中心使用产生的限制

信息报警对用户认证进行检验。

附图说明

图 1 为一说明性图，表示了记录和存储卡的第一实施例，该卡包括由二维空间码数据组成的保密信息。

图 2 为一说明性图，表示了该卡的第二实施例。

图 3 为一说明性图，表示了该卡的第三实施例。

图 4 为一说明性图，表示了该卡的第四实施例。

图 5 为二维空间码的解释性图，其分别包括图 5a 中的小正方形、图 5b 中的大正方形以及图 5c 中的矩形。

图 6 为表示记录和存储卡的第五实施例的解释性图，其中记录和存储卡中包括由二维空间码数据组成的保密信息。

图 7 为在卡 1 上进行记录和读取操作的示意图。

图 8 表示与图 7 中相同操作的方框图。

图 9 为加密信息的解释性图。

图 10 为地址卡的解释性图。

图 11 为包括说明的地址卡的解释性图。

图 12 为用户数据记录卡的解释性图。

图 13 为用于使用不同形状的匹配数据的实施例的用户认证数据记录卡的解释性图。

图 14 为用于表示实施例的用户认证数据记录卡的解释性图，其中在实施例中记录了二维空间码数据。

图 15 为用于表示实施例的用户认证数据记录卡的解释性图，其中在实施例中标记和符号被用作匹配数据。

图 16 为在第二实施例中的读取匹配数据方法的解释性图，并且表示了控制计算机的功能。

图 17 为根据从第八实施例到第十实施例的紧急条件通知系统的系统操作的解释性图。

图 18 为用于表示与图 21 中的所示的相同系统操作的流程图。

图 19 为使用与图 19 相似的方式表示第十实施例的解释性图。

图 20 为用于表示第七实施例的流程图。

具体实施方式

根据本发明，持有包括由单个或多个真实数据项分布于无数虚假数据项中的保密二维空间码数据的记录和存储卡的用户从用户自己的存储体中确定和选择在无数虚假数据项中的真实数据项的位置和读取顺序。

在从用户自己的存储体中确定和选择在无数虚假数据项中的真实数据项的位置和读取顺序的过程中，用户将参考由无数虚假数据项和真实数据项组成的解释或图例作为辅助的方法。

在从用户自己的存储体中确定和选择在无数虚假数据项中的真实数据项的位置和读取顺序的过程中，用户也参考存在于无数虚假数据项和真实数据项的背景中的解释或图例。

从用户存储认证（大脑认证）中确定关于无数虚假数据项的单个或多个真实数据项的位置和存储顺序，来选择分布于无数虚假数据项中的单个或多个真实数据项，因此带有加密密钥的保密信息被解密用于复制。

在将加密的保密信息进行解密的过程中，从来自于用户自身记忆的无数虚假数据项中，用户确定和选择指示解密密钥的真实数据项的位置和读取顺序。

从用户记忆中确定用于分布在无数虚假数据项中的正确信息的真实数据项的位置和顺序，并且根据本发明第八方面的实施例，通过使用包括色彩、说明、图形和地形的图片作为辅助装置，来完成从用户记忆中进行确认的过程。

以下将参考附图对本发明进行详细的描述。

如图 1 到 3，参考数字 1 为包括保密信息的记录和存储卡，在该卡中单个或多个真实数据项 A 分布于无数虚假数据项 B 中并且虚假数据 B 和真实数据 A 通过使用二维空间码进行加密。

单个或多个真实数据项 A 和无数虚假数据项 B 分布在不同大小的组中。所有的虚假数据 B 和真实数据 A 不能通过视觉进行识别。二维空间码的记录数据项可以相互不同或一些记录的数据项可以位于包括无数相同数据项的组中。

此外，虚假数据项 B 和真实数据项 A 可以具有相同的形状（例如，正方形）或不同的形状如正方形、长方形和圆，并且这些不同的形状可以允许用户更容易地将真实数据项 A 的位置保存于用户记忆中。出于此目的，假设任何在大小和形状上的区别都与数据是否为正确或错误无关，因此数据不能够根据大小和形状上的区别进行验证。

标号 1 表示单个真实数据项 A 和无数其它的数据项具有相同的形状（例如正方形）但是为两个不同的大小，即较大正方形和较小正方形。

参考图 1，假设第一个单元记录 10 和第二个单元记录 12 共同代表一个公寓楼，第二个单元记录 12 代表楼梯和 / 或电梯，并且第一个单元记录 10 代表公寓楼中的住所。

为了定位加密密钥，假设在第二层楼的楼梯右侧的第二个住所为真实数据项 A 并且所有其它的为虚假数据项 B。

图 2 表示由正方形和长方形代表的多个真实数据项 A 和其它数据项作为三种单元记录类型，即第一个单元记录 10、第二个单元记录 12 和第三个单元记录 13。

用较小正方形表示的第一个单元记录 10 代表住所，用较大正方形表示的第一个单元记录 12 代表与图 1 中类似的楼梯和 / 或电梯，并且用长方形表示的第三个单元记录 13 代表避难层，使用于帮助用户对真实数据项 A 所处的位置进行记忆。

如图 3 所示，“机器人”代表由无数虚假数据项和真实数据项形成的图例。

为了从用户记忆中确定和选择分布在无数虚假数据项中的真实数据项的位置和顺序，假设在“机器人左眼上”的长方形代表第一个真实数据项 A1，“在机器人肚子中间”的较大正方形代表第二个真实数据项 A2，在“机器人的左腿”的脚趾处的较小正方形代表第三个真实数据项 A3。

这种作为机器人的“眼睛”、“肚皮”和“腿”的辅助方法能够被用来帮助对真实数据项的位置和从无数虚假数据项中选择它们的顺序进行确定。

如图 4 所示，地形代表由无数虚假数据项和真实数据项组成的背景。

图中，地形放置于由无数虚假数据项和分散于其中的真实数据项的组合形成的图上。值得注意的是在透明板上印制有地形的地形图被放置于具有无数虚假数据项和分散于其中的真实数据项的组合的数据板上，以覆盖或叠加在地形上。

为了从用户记忆中确定和选择分布在无数虚假数据项中的真实数据项，假设在“山上的三棵松树”的最左一颗中的长方形代表第一个真实数据项 A01，“河中的船只上”货物中的较大正方形代表第二个真实数据项 A02，在“桥附近的三块石头”中的离桥最近处的较小长方形代表第三个真实数据项 A03。

这种作为“山上的三棵松树”、“河中的船只”和“桥附近的石头”的辅助方法能够被用来帮助对真实数据项的位置和从无数虚假数据项中选择它们的顺序进行确定。

以下，将参考图 5 对通过使用二维空间码获得的数据进行说明。

二维空间码包括网格状排列的（矩阵）正方形或长方形，集中排列的圆和多层条形码，并且其优点在于因为它的二维空间排列，与数据单元的一维条形码相比，信息量能够连续地增长；在于通过对数据单元作改变从而改变要显示的数据，使得无数不同的数据项看起来非常接近；在于无数具有不同大小和形状的数据项可以被认为是相同的数据。本发明的第一个实施例使用了这些优点。

在图 5 中，二维空间码包括网格状排列的（矩阵）正方形或长方形，即图 5a 中的小正方形，图 5b 中的大正方形和图 5c 中的长方形，并且各个二维空间码的记录相在三个图中指示相同的数值或标记。此外，引用数字 14 指定一个较宽的数据范围，数字 15 指定二维空间码数据。

在上面所描述的实施例中，色彩能够有助于从记录媒介或打印的介质上记录的数据中确定真实数据项的位置以及从无数虚假数据项中对它们进行选择的顺序。

下面，对第二实施例进行描述。

根据本发明第三方面的实施例，通过对带有加密密钥的保密信息使用二维空间码加密得到的部分真实数据项被分散于无数虚假数据项中，

并且真实数据项的位置相对于无数虚假数据项的位置保存于用户的记忆中以用于记忆认证（大脑认证），从而防止任何未经授权的人对保密信息进行解密。

第二到第四实施例可以通过使用一个记录和存储卡，该记录和存储卡用于带有加密密钥的保密信息，其根据第一实施例使用二维空间码加密得到；以及通过使用另外的记录和存储卡，该记录和存储卡用于带有加密密钥的保密信息，其根据如图 6 所示的二维空间码加密得到。

在图 6 所示的卡中，用于每个数据项的二维空间数据在形状上相同，即相同尺寸的正方形。加入一系列的字母字符用于帮助用户记忆真实数据项的位置和读取顺序。值得注意的是字母字符（例如，B2、B1、F1、F2、F3.....）可被添加到图 1 和图 2 所示的卡中，用于帮助记忆真实数据项的位置和读取顺序。

参考图 7 和图 8，下面将对卡 1 的记录和读取操作进行描述。

假设在卡 1 上印有的 20 个编码中，16 个编码是伪码。一个密码被分割成四部分，从左端开始被分别放置在上面的第二个位置，下面的第五个位置，下面的第六个位置以及上面的第九个位置（参见图 6）。假设这四个部分以“E-9-2-F”的顺序被读取。

一个知道该顺序的授权的用户使用手持的或笔型的扫描器 2 如图 7 所示顺序地读取下面的第五个位置＃1，上面的第九个位置＃2，上面的第二个位置＃3 和下面的第六个位置#4，在此过程中忽略其它的位置。被访问的系统通过上千的数字和／或字符接收到上百个复原后的密码对该授权的用户进行验证。

参照图 7 和图 8，引用数字 3 表示终端设备，4 表示键盘，5 表示通讯网络如因特网，6 表示中央控制计算机和 7 表示数据。

下面，对第三实施例和第四个实施例进行描述。

图 9 中的加密信息 20 被分割为三个正确信息项 P1、P2、P3，其被分布于错误信息项 Q1、Q2，...中以掩盖正确信息。因此，错误信息 Q 和正确信息 P 不能够从它们的外观上进行区分。

正确信息项 P1、P2、P3 被指定为 5、A 和 イ（一种片假名字符）作

为地址信息相P（真实数据）并且其它的错误信息项Q1、Q2，...被指定为除5以外的数字、除A以外的字母字符以及除イ以外的片假名字符作为地址信息相Q（虚假数据）。

参照图10，真实数据项P和虚假数据项Q都被放在地址卡21A、21B和21C上。

然后用户通过记忆认证（大脑认证）从虚假数据项中选择真实数据项5、A和イ。

为了有助于读取顺序的安全选择，这些数据项可被标为红色、黄色和蓝色。

如果使用二维空间码，如图1到图4和图6所示的实施例可以被使用。此外，如图11所示，也可以使用除字母字符以外的标记和符号。

值得注意的是第三和第四实施例并不局限于光学的/打印的二维空间码，也适用于非光学的/非打印的索引数据块和光学/非光学的符号。这些实施例所使用的算法不仅可用于打印作为二维空间码的部分数据项，也适用于打印作为符号和数据块的部分数据项或没有被打印但作为存储媒介上的索引和记录的部分数据项。

上述的从第一到第四实施例有助于用于用户认证的认证数据的输入操作以及从无数虚假数据项中选择真实数据项的操作，因此更容易地保存在人地记忆中。此外，因为虚假数据项地数目与字母字符的数目相同，这些实施例可以更安全地防止任何未经授权地人对认证符号进行解密。存储合作信息和/或个人信息的记录媒介可以更安全地被隐藏。此外，用于用户认证的加密密钥和保密信息如合作信息和/或个人信息可以以更为安全地方式进行处理，以用于在线应用和离线应用以及在计算机自身的记录媒体上进行记录和存储。因为数据项地数目与多个数字的字母字符串的数目相同，这些实施例可以更安全地防止任何未经授权地人对认证符号进行解密。记录媒体存储合作信息和/或个人信息可以更安全地被隐藏。

现在，下面对第五到第七实施例进行描述。

图15显示了将用户认证数据记录卡A1作为本发明的用户认证数据

记录媒介并且无数匹配数据项如日本汉字字符串、字母字符串、图像和/或声音数据是二维空间码，且其通过记录方法被记录在数据记录卡上，其中记录方法能够通过光学和/或磁性来读取数据。

图 16 显示了在不同形状下的 a1、a2、a3 的匹配数据。

图 17 显示了通过计算机控制的打印机或磁性记录的匹配数据并且如图所示的二维空间码能够使得记录与数据形状不相关的相同的数据。此外，二维空间码能够使得区别可视的记录数据项变得困难，因为它们是用基本相同的形状被打印出来。

值得注意的是本发明并不局限于如上所述的二维空间码和一维空间码，包含说明的符号以及漫画、字母字符串、日本汉字字符串、单词和短语可被用作匹配数据。因此，匹配数据可以包含字符串和图像和/或声音数据，它们可以被计算机进行加工以用于匹配操作。

用户认证数据记录卡 A1 的记录媒介可以为光学可读打印卡的或磁性记录区域的一部分，其中形成的磁性记录区域位于如信用卡等类似的卡上的一个部分。

图 18 显示了包括作为匹配数据 a4、a5 和 a6 的标记和符号的用户认证数据记录媒介（用户认证数据记录卡 A）的实施例。在向每个用户发布如上所描述的用户认证数据记录媒介之前，从无数的匹配数据项中确定单个或多个真实数据项 P 以及所有剩余的匹配数据项被确定为多个虚假数据项 Q，然后由单个或多个真实数据项和多个虚假数据项组成的匹配数据被记录在用户认证数据记录媒介上。值得注意的是当使用多个真实数据项 P 时，对真实数据项 P 的读取顺序也被确定。例如，如图 12 所示，真实数据项被确定为 P1＝E，P2＝9，P3＝2 和 P4＝F 来用于作为匹配卡的用户认证数据记录媒介 1（用户认证数据记录卡 A1）。

在用户认证数据记录媒介 1（用户认证数据记录卡 A1）上的真实数据项的位置和多个真实数据项的读取顺序被确定并被记录在 CPU 和中央控制计算机的记录单元上，从而可以使得计算机在持卡人出示的用户认证数据记录媒介 1（用户认证数据记录卡 A1）上记录的认证数据进行匹配操作。

下面，将对在用户认证数据记录媒介 1（用户认证数据记录卡 A1）上输入认证数据的过程进行描述。

参考图 19，在如图 15 所示的用户认证数据记录媒介 1（用户认证数据记录卡 A1）上的认证数据通过笔形的扫描器 2 输入到终端单元 3 中，然后被直接或通过通讯线（因特网）发送到与终端单元连接的 CPU 上。

对于每个认证的用户，在 20 个匹配数据项中 4 个预先确定的数据项以一定的顺序输入。具体地，下面的第五项＃1，上面的第九项＃2，上面的第二项＃3 和下面的第六项＃4 以这个顺序被读出。这些数据项为包括如图 15 所示的文字与数字的字符“E－9－2－F”。手持扫描仪 2 在用户认证数据记录卡上读取所有的数据项并且通过如键盘 4 的选择性输入方法选择认证数据项并将其通过终端单元 3 发送到 CPU 和中心控制计算机 6 中。

除了以上所描述的记录单元，CPU 或中心控制计算机 6 包括真实数据辨别器、虚假数据辨别器、限制通知数据辨别器、真实数据计数器、虚假数据计数器、用户认证信号产生器、窃取报警（未授权的访问报警）产生器和限制通知信息产生器。

由 CPU 或控制计算机 6 进行发射如上所述的认证数据的操作将在参考图 20 中的操作流解释图和图 8 中的流程图下面对其进行描述。

当 4 个特殊的数据项以特定的顺序（例如，如图 15 中的用户认证数据记录媒介 1 被用来以“E－9－2－F”的顺序输入四个真实数据项 P1＝E，P2＝9，P3＝2 和 P4＝F）输入时，进行的过程如图 21 中左边的流程图。即，步骤 S1、S2、S3 和 S4 以这样的顺序进行来成功地完成用户认证操作。

如果任何真实数据项以不正确地顺序输入（输入任何错误的数据项或输入在用户认证数据中不存在的数据项（噪音数据）），将被认为是授权错误从而引起步骤 S1、S2、S3 和 S4 出现分支，导致用户认证失败。然后，如果错误计数超过预先确定的值，例如，在步骤 S5 上超过 3 次，认证访问即被终止。如果错误计数少于预先确定的值，例如，为 2 次或更少，还允许进行再一次的认证访问。

如果输入了错误的数据项，进行如图中的中心流程所示的过程并且进行步骤 S6、S7、S8 和 S9 这样的顺序过程，以 CPU 或控制计算机 6 的记录方法存储虚假数据项，计算输入的虚假数据项。

如果错误计数为 2 次或更多，在任何步骤 S10、S11 和 S12 中将出现分支以发现“未经授权的访问”。

如果在 4 次输入操作中虚假数据计数为 1 次，将被认为是“误操作”从而可以再次输入匹配数据。

作为如上所述的将预先确定的真实数据项分散在虚假数据项中的方法的一种替代方法，带有无数匹配数据项的用户认证记录媒介，其中不管这些数据项是真的还是假的（即，没有预先确定的真数据项和虚假数据项），可以交给用户让用户从中选择部分作为真数据项而剩下的作为虚假数据项。即，用户被给予临时的权限来选择真数据项和虚假数据项以及限制通知数据项。

如果无数虚假数据项中的一项被作为“报警数据”项并且步骤 S1、S2、S3 和 S4 以这样的顺序进行来成功地完成用户认证操作后输入报警数据项（即，在 4 个真实数据项输入以后），产生用户认证和限制通知信息并且在步骤 S13 中发送任何探测到的“限制通知数据”项。

在图 22 和 23 所示的实施例中，记录在用户认证数据记录媒介 1（用户认证数据记录卡 A1）上的所有数据项可通过读卡器进行读取，然后通过选择输入方法如键盘选择的认证数据项被通过终端单元 3 发送到 CPU 和中心控制计算机 6 中。作为如下所述的可选择的另一种方法，包括在电子设备终端单元中的计算机可以被用来电子地记录用户认证数据记录媒介的内容（用户认证数据记录卡 A）以及在线或离线地将内容记录在控制中心（认证数据注册计算机），因此根据用户发送的记录的作为认证数据输入的匹配数据串可以被在线或离线地输入控制中心（认证计算机）以用于匹配认证数据。值得一提的是文字与数字的字符、二进制比较、图像比较和其它的数据比较技术也可以被用来进行匹配。

参考图 25，在控制中心（认证数据注册计算机）中的 CPU 和中心控制计算机 6A 除了用于第一实施例的图 5 中所示的功能方法[真实数据辨

别器、虚假数据辨别器、限制通知数据辨别器、真实数据计数器、虚假数据计数器、用户认证信号产生器、窃取报警（未授权的访问报警）产生器和限制通知信息产生器]外还具有输入数据存储器。

由 CPU 和中心控制计算机 6A 进行的发射如上所述的认证数据将参考如 10 的流程图在下面进行描述。

当 4 个特殊的数据项以特定的顺序（例如，如图 12 中的用户认证数据记录媒介 1 被用来以“E－9－2－F”的顺序输入四个真实数据项 P1＝E，P2＝9，P3＝2 和 P4＝F）输入时，并且在记录单元中的认证数据与在输入数据存储器中的认证数据匹配时，可以确定输入了正确的认证数据并成功完成了用户认证操作。如果在记录单元中的认证数据与输入数据存储器（输入任何错误的数据项或输入在用户认证数据中不存在的数据项（噪音数据））中的认证数据不匹配时，将被认为是授权错误从而导致用户认证失败。

然后，如果错误计数少于预先确定的值，例如为 1 次或更少，允许进行另外一次认证访问。

如果错误计数等于或超过预先确定的值，例如，为 2 次或更多，即认为是“未经授权的访问”从而产生窃取报警。

如果无数虚假数据项中的具体一项被作为“报警数据”项并且在成功地完成用户认证操作后输入报警数据项（即，在 4 个真实数据项输入以后），产生用户认证和限制通知信息并且发送任何探测到的“限制通知数据”项。

如果用户认证数据记录媒介的内容被记录在移动电话或便携式终端设备中的计算机的记录单元上，在便携式电子设备中的记录方法可以使得控制中心通过记录相似的信息来发布用户认证数据记录媒介到用户认证数据记录卡中，即根据便携式电子设备中的记录方法，无数匹配数据项 a 从其中确定真实数据项 P，并且根据便携式电子设备和控制中心中的计算机中的记录方法，为根据便携式电子设备的持有者确定和记录认证数据。

在用户认证操作过程中，无数匹配数据项 a 被提供在便携式电子设

备的显示设备上，从而可以使得用户从用户记忆中指定真实数据项 P 的位置用于将其发送到控制中心（认证数据注册计算机）。如果任何虚假数据项 Q 被发送，会被通知或报警便携式电子设备（例如移动电话或新型的认证设备）可能丢失或被窃取。如果发现任何“限制通知数据”，将会产生和发送用户认证和限制通知信息。

为指定真实数据项 P 的位置，可以使用键盘（包括 10 个键的键盘或拨号器）、触摸屏或其它的计算机输入装置。对于一个应用来讲，其中用户认证操作必须在没有任何与控制中心通讯的条件下离线进行，一个单独的设备可能包括认证数据注册中心中的计算机以及图 19 所示的认证计算机所能完成的所有功能。例如，新型的控制器可以打开门上的锁而使某人仅仅通过用户认证而不需与外部计算机进行任何通讯而进入房间。然而，这样的控制器可以被设置通过在线通讯的通讯方法以产生和发射盗窃报警或限制通知信息来实现安全。

具体地，在需要用户限制通知信息的条件下，除允许进行房间和操作电子设备以外的安全通讯对于援救用户和电子设备及电子设备所控制的房间的安全来讲是有效的。

本发明第五方面使用单独的真实数据项 P。一发现错误的数据项 Q，就通知或报警出现了丢失或盗窃。

本发明第六方面使用多个真实数据项 P 并且在探测到多个错误的数据项 Q 就产生报警，因此应当减少由于输入错误而产生的错误报警。

除了本发明第七方面的特征外，发明能够根据探测到的任何“限制通知数据”产生和发射限制通知信息。因此，当实现第五个和第六个实施例时，如图 23 所示的根据探测到的任何“限制通知数据”产生和发射限制通知信息的附加特征可以被忽略。

本发明第五方面到第七方面能够使用用户认证数据记录媒介 1，其中媒介 1 上记录有无数相似的匹配数据项，并且这些实施例也能够从用户的记忆中在无数相似的匹配的数据项中选择正确的数据项从而可以安全地防止任何未经授权的人根据认证数据进行用户认证请求。如果要发送的认证数据包括虚假数据项，盗窃报警的产生能够增强防止通过 丢失或

窃取的用户认证数据记录媒介进行的未经授权的访问。

此外，如果该用户处于怀有恶意的未经授权的人的控制之下，这些发明可以有效地保护和防止来自于用户的对用户和系统的访问。

工业应用

本发明提供隐藏、记录和存储保密信息如公司信息和技术信息的方法。本发明也确立了一个报警系统，当带有加密密钥的保密信息、含有这种保密信息的记录媒介或具有这种记录媒介的电子和/或通讯设备被窃取或丢失，或通过欺诈性地使用泄漏的认证数据，该报警系统可作为一种安全措施。本发明进一步建立了一个当对限定区域或电子设备进行未经授权访问时会发出通知的系统。此外，本发明能够探测来自于处于怀有恶意的未经授权的人的控制之下的授权用户的访问，并且能够对用户和系统进行保护和保存。因此，本发明在使用保密信息记录媒介的工业领域非常有用，其中在保密信息记录媒介上记录有带有加密密钥的保密信息。

图 1

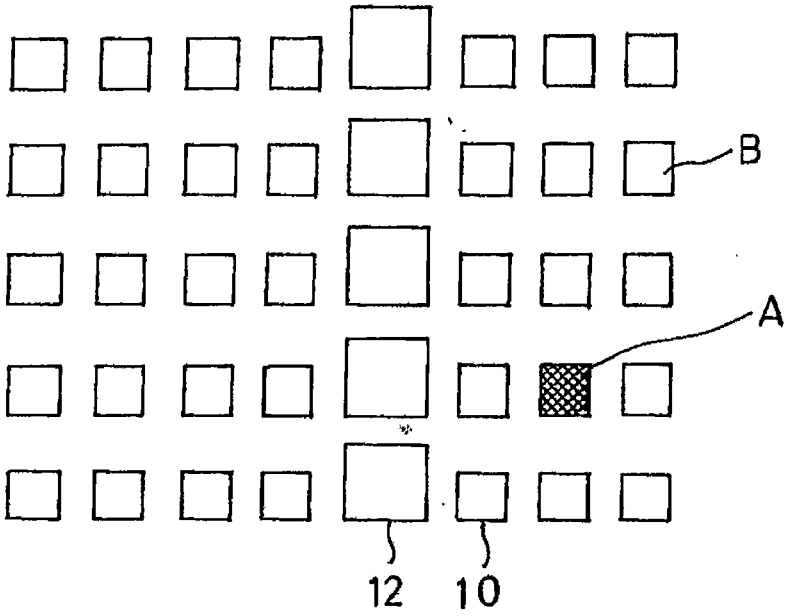


图 2

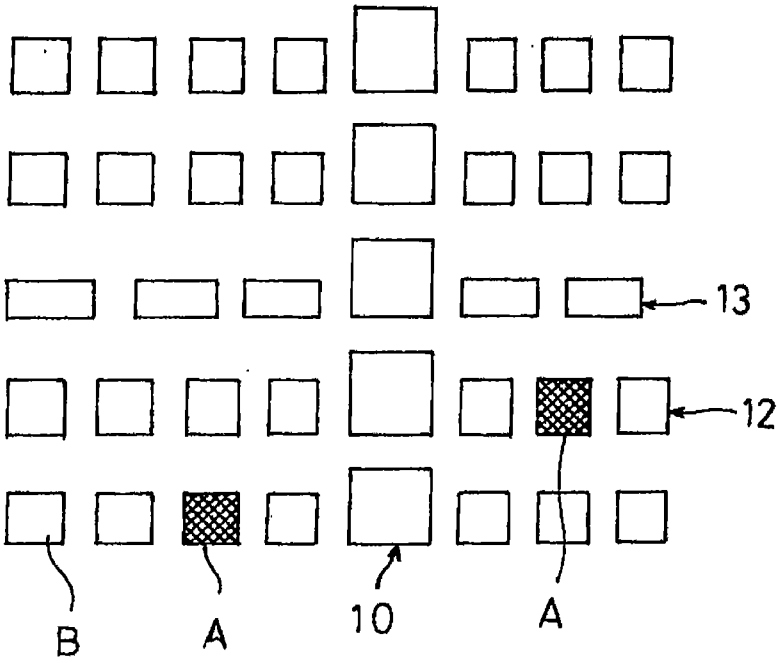


图 3

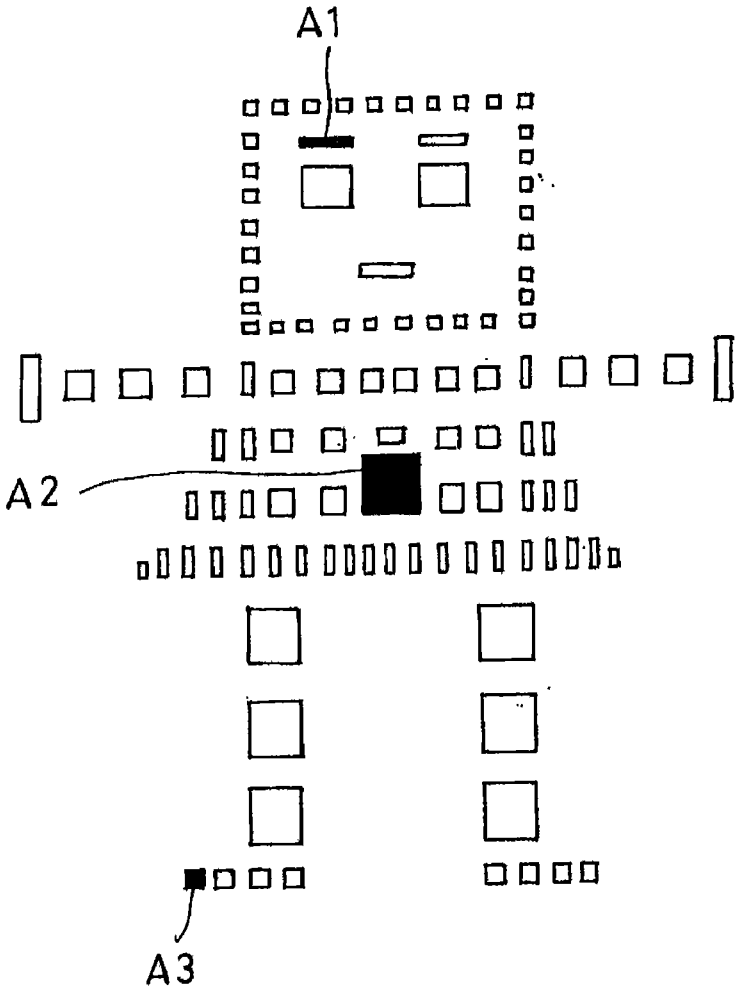


图 4

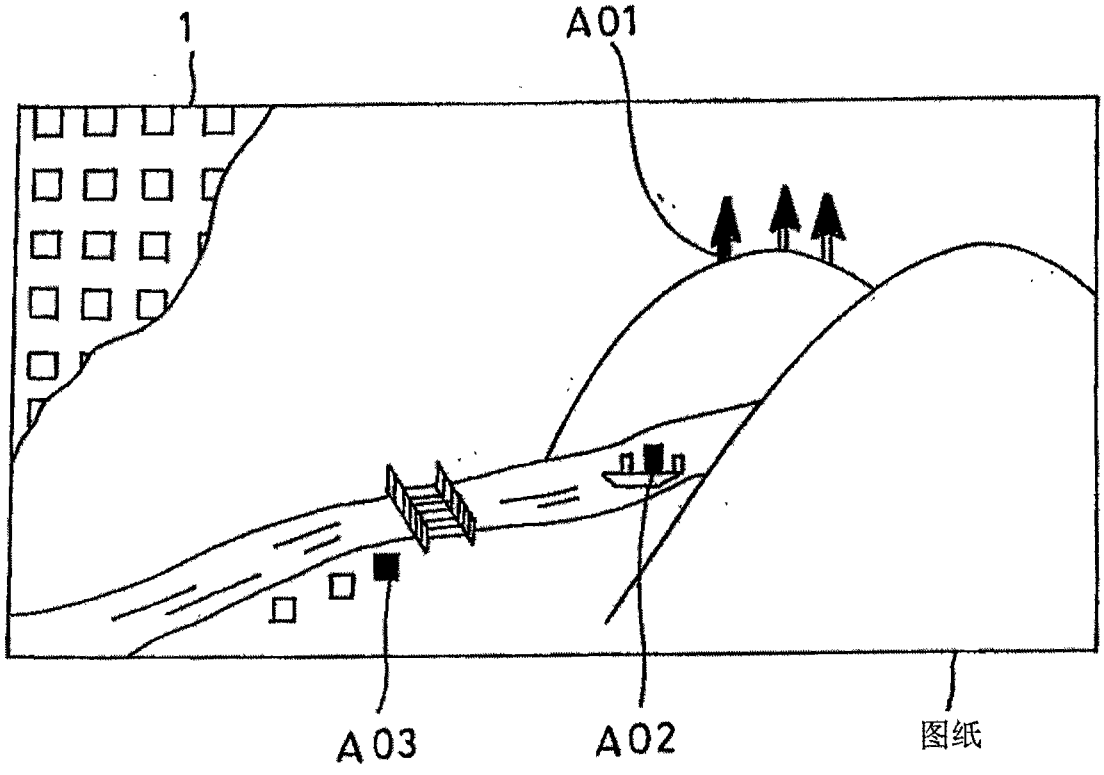


图 5

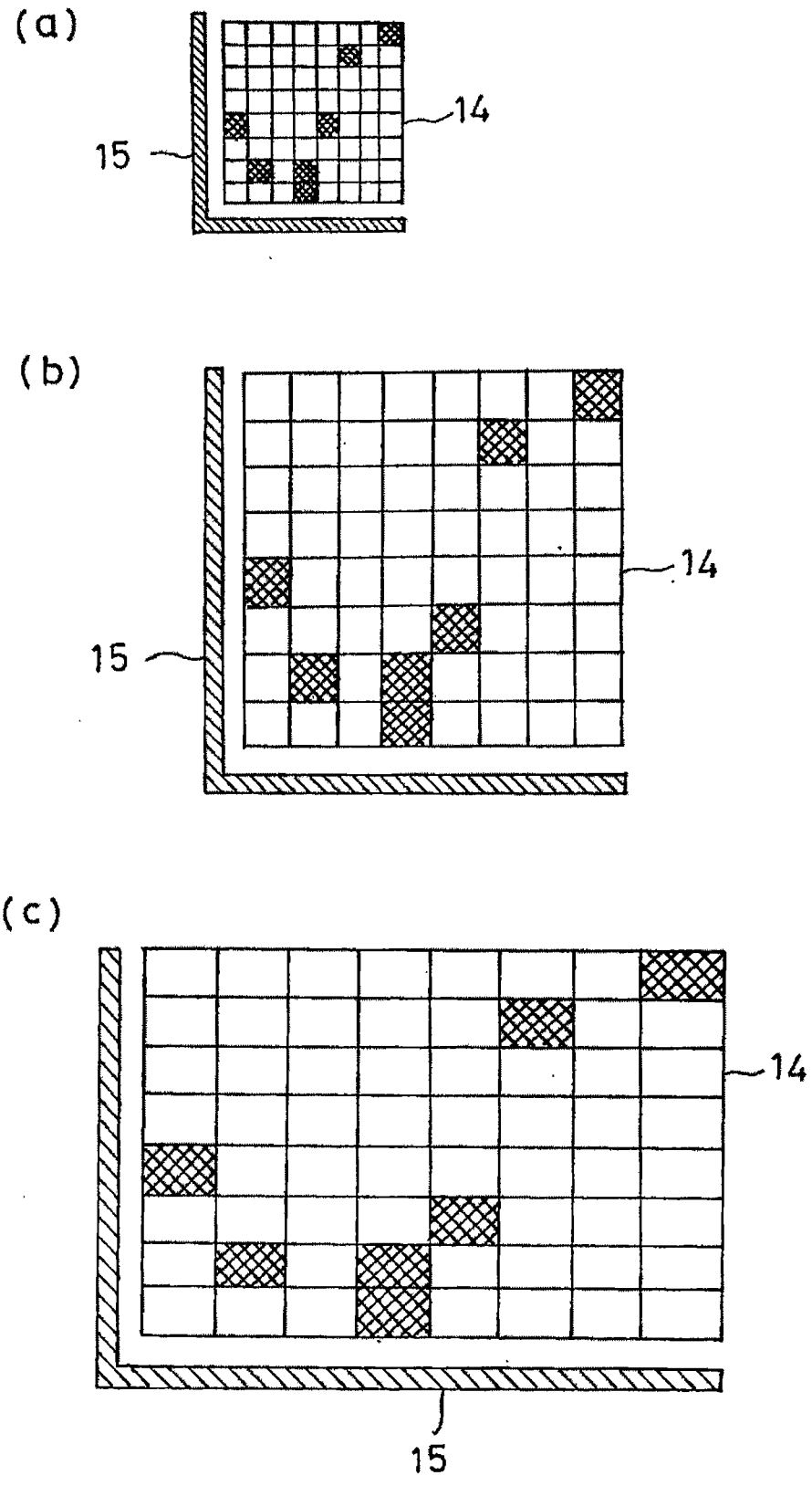


图 6

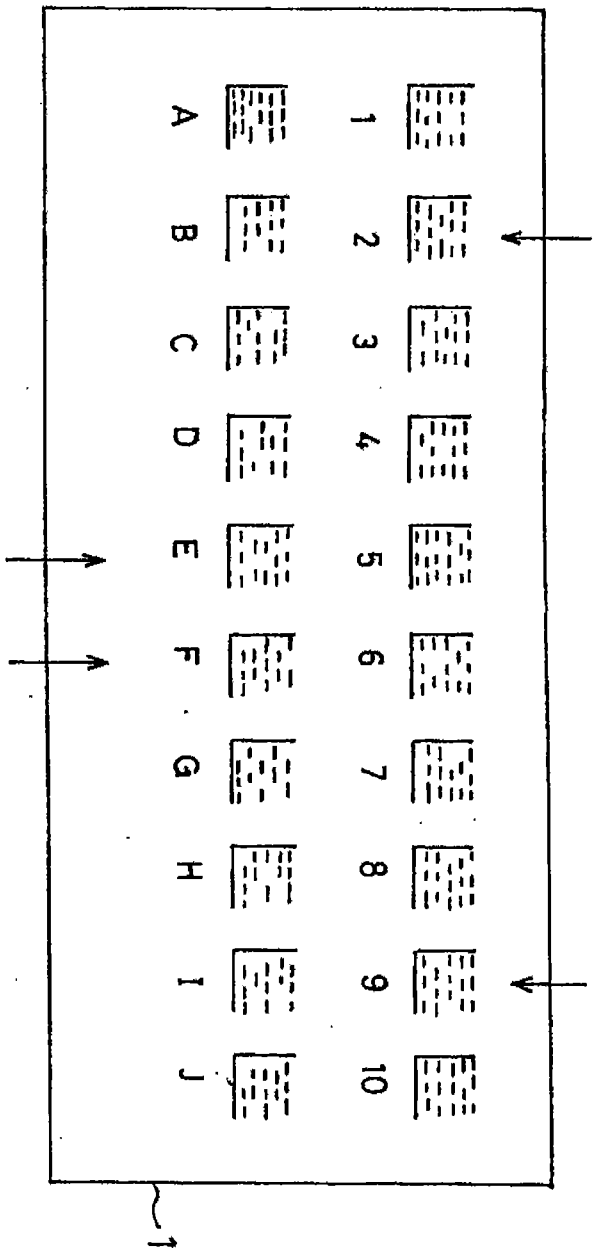


图 7

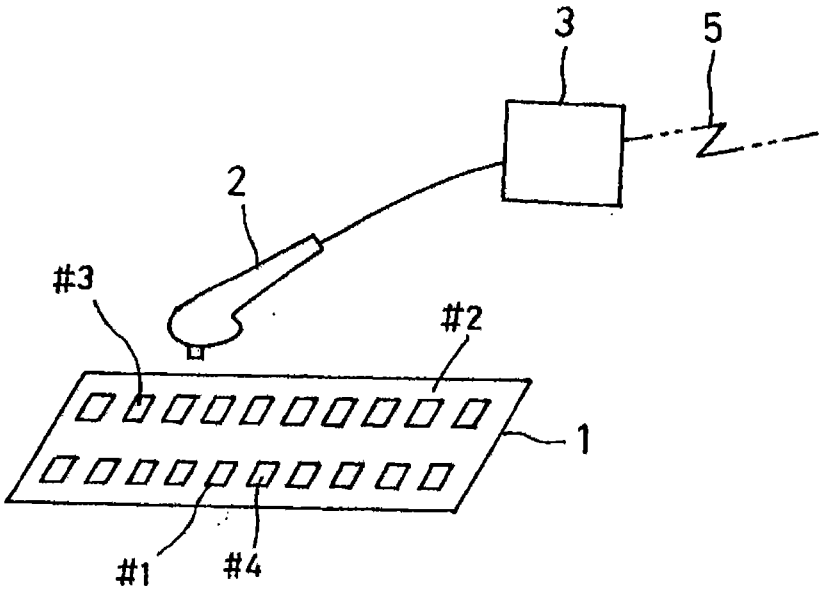


图 8

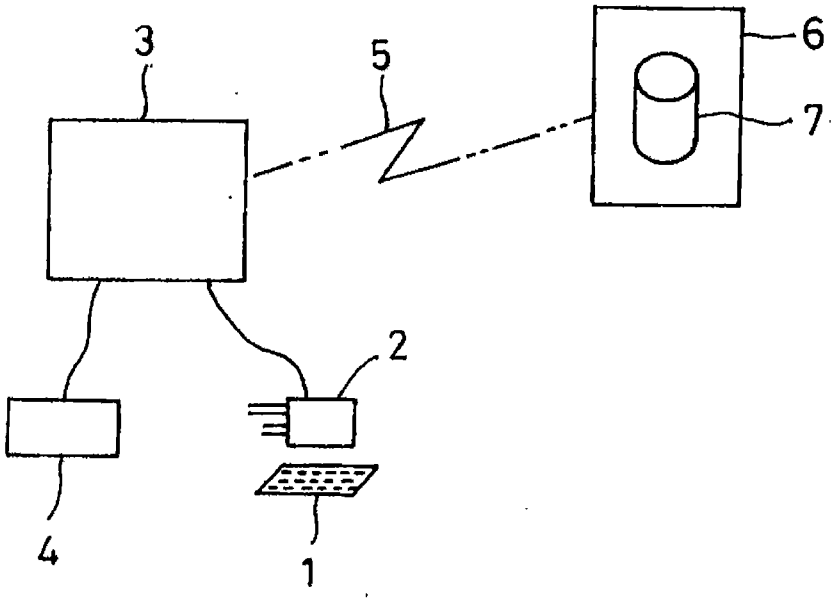


图 9

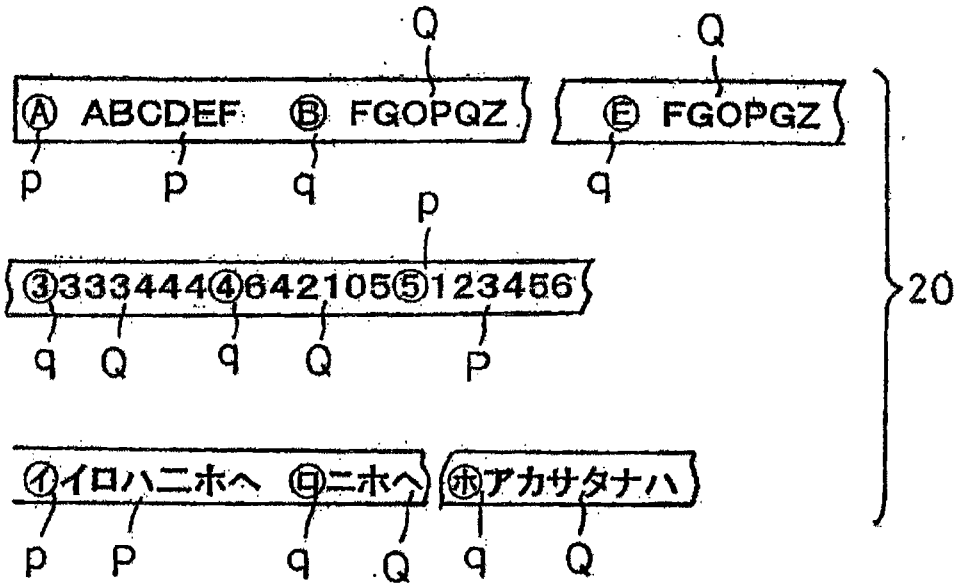

Q
Q
Ⓐ ABCDEF
Ⓑ FGOPQZ
Ⓔ FGOPGZ
p
p
q
q
p
③333444④642105⑤123456
q
Q
q
Q
P
20
㋑イロハニホヘ
㋺ニホヘ
㋩アカサタナハ
p
P
q
Q
q
Q

图 10

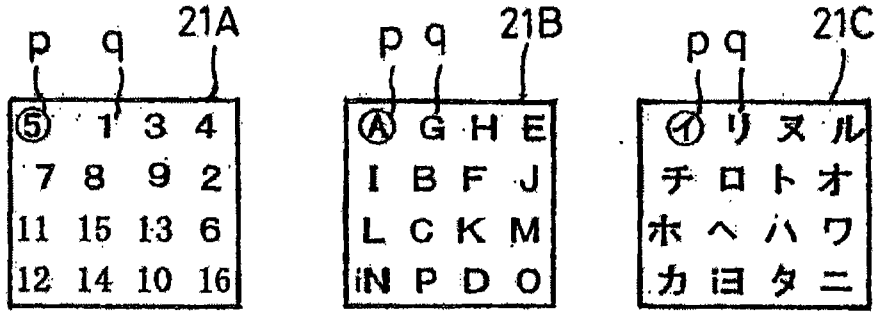

p
q
21A
⑤ 1 3 4
7 8 9 2
11 15 13 6
12 14 10 16
p
q
21B
Ⓐ G H E
I B F J
L C K M
N P D O
p
q
21C
㋑ リ ヌ ル
チ ロ ト オ
ホ ヘ ハ ワ
カ ヨ タ ニ

图 11

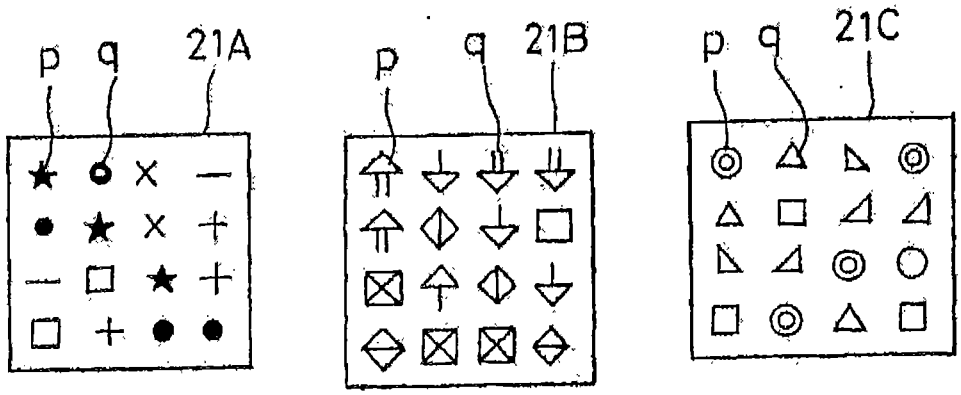

p
q
21A
p
q
21B
p
q
21C

图12

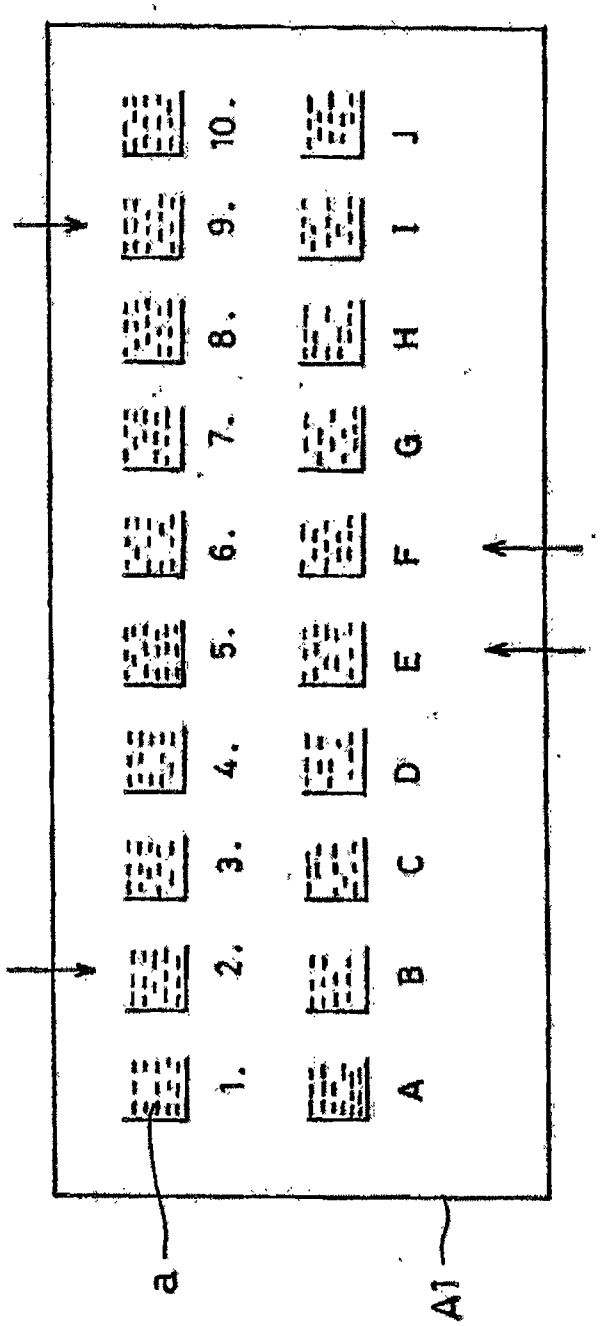


图 13

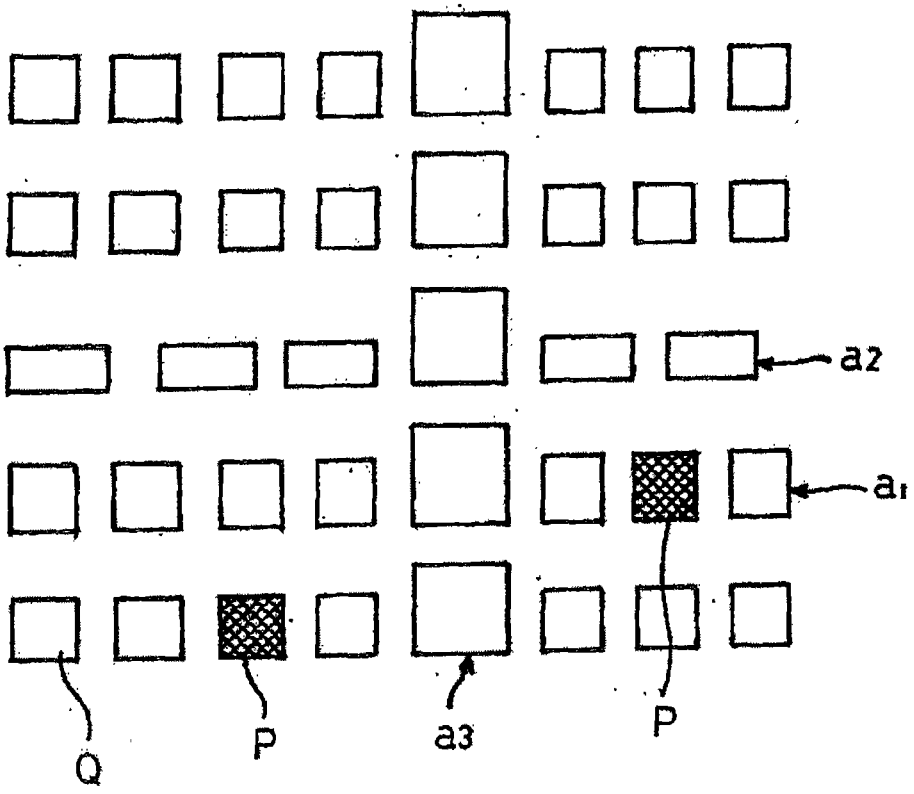


图 14

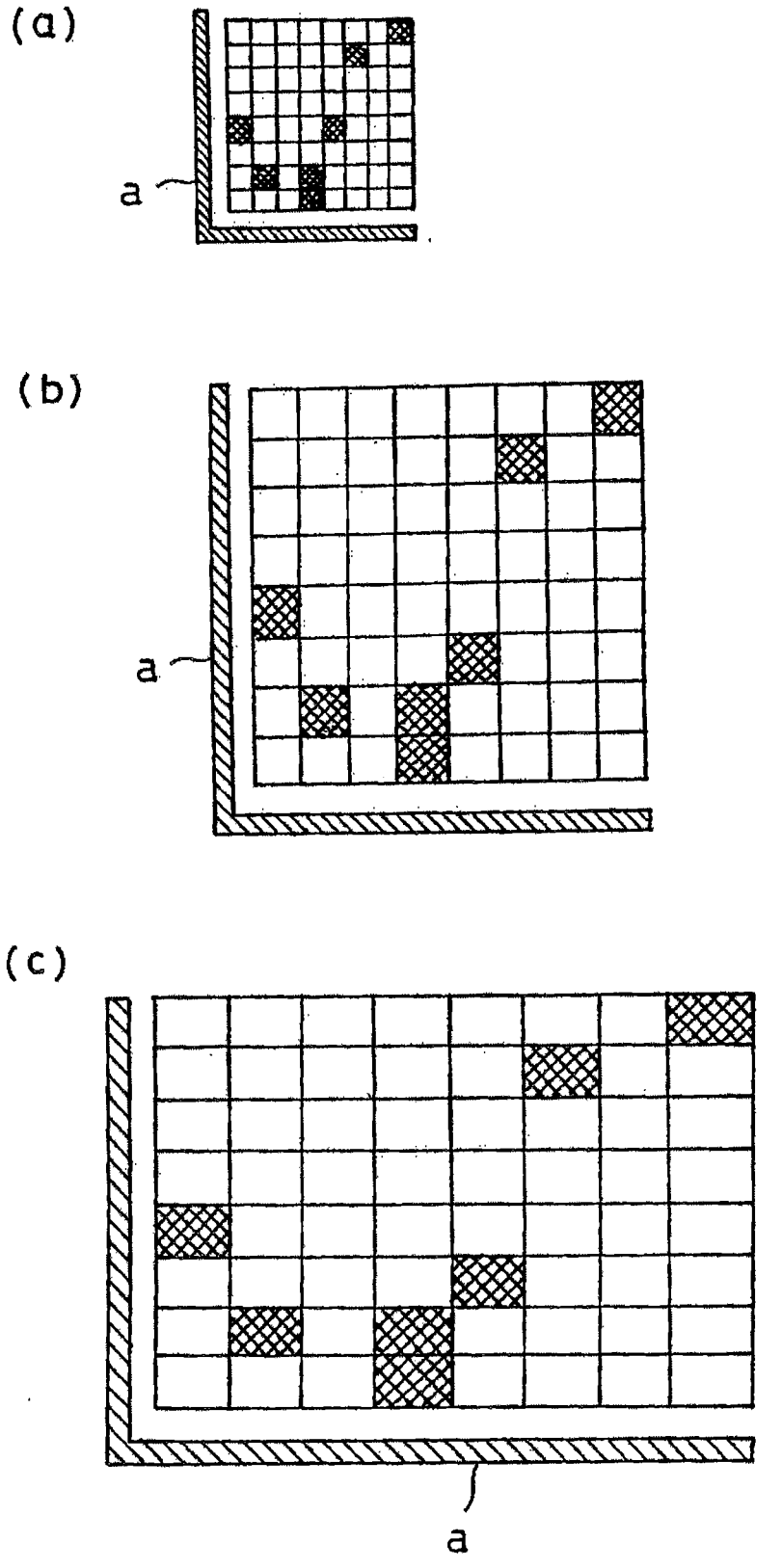
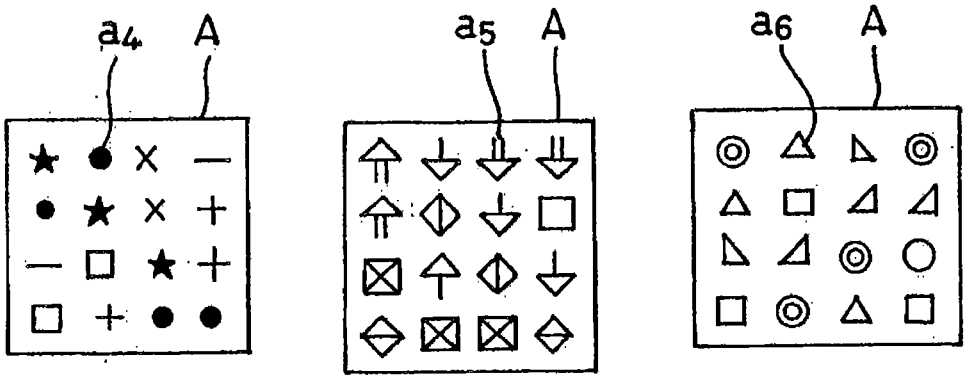


图 15



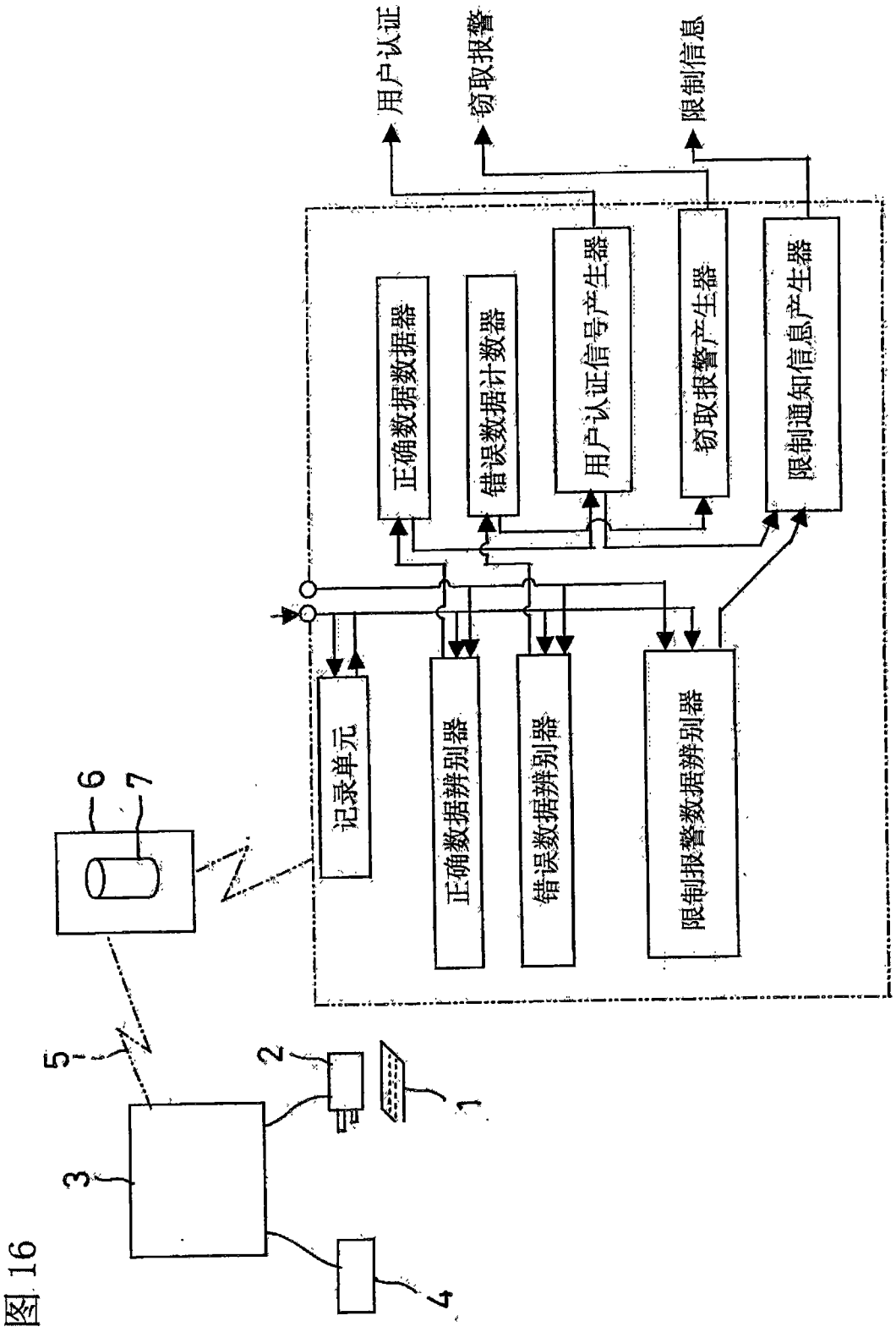

用户认证
窃取报警
限制信息
正确数据数据器
错误数据计数器
用户认证信号产生器
窃取报警产生器
限制通知信息产生器
记录单元
正确数据辨别器
错误数据辨别器
限制报警数据辨别器
6
7
5
2
1
3
4

图 16

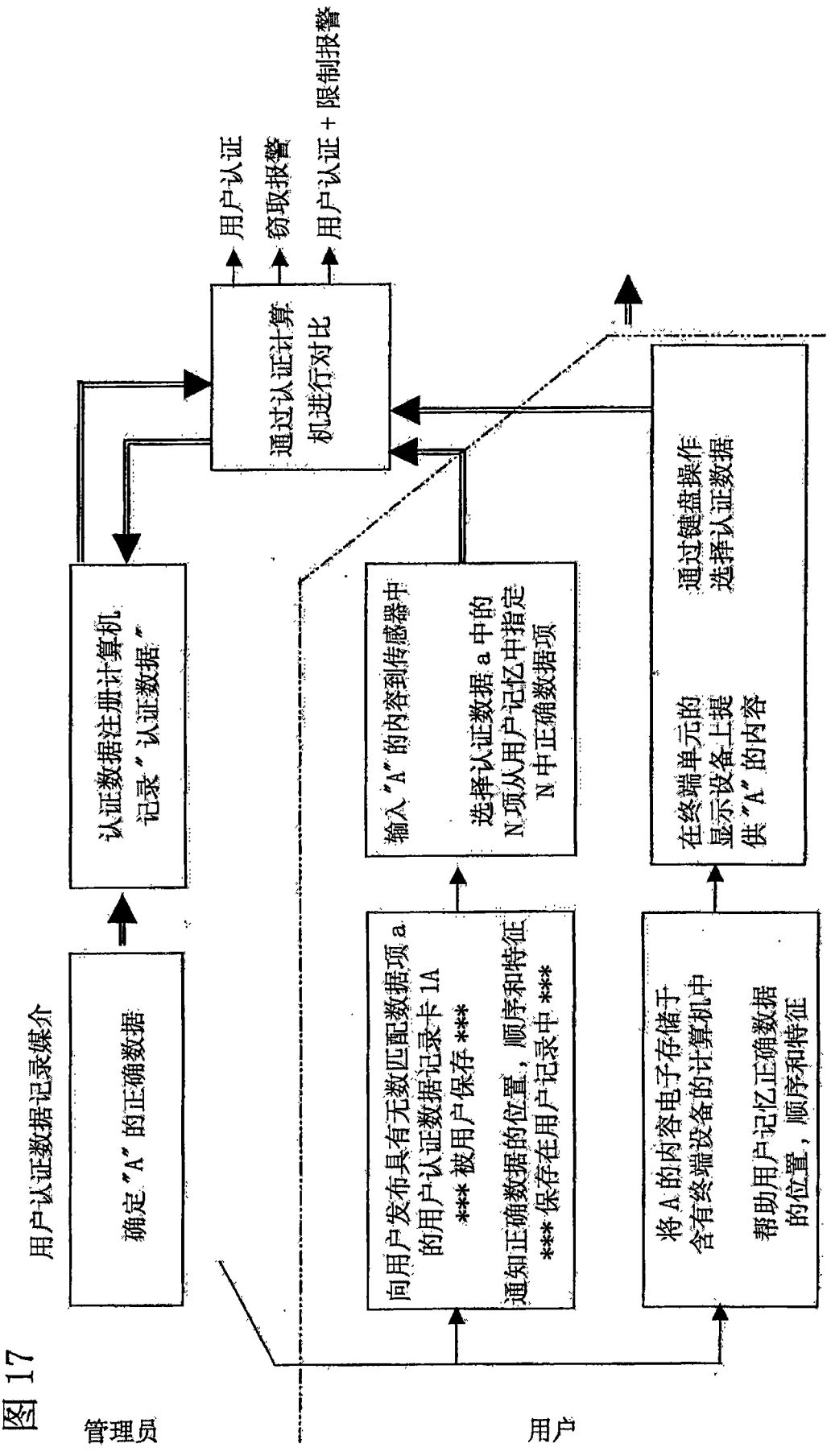
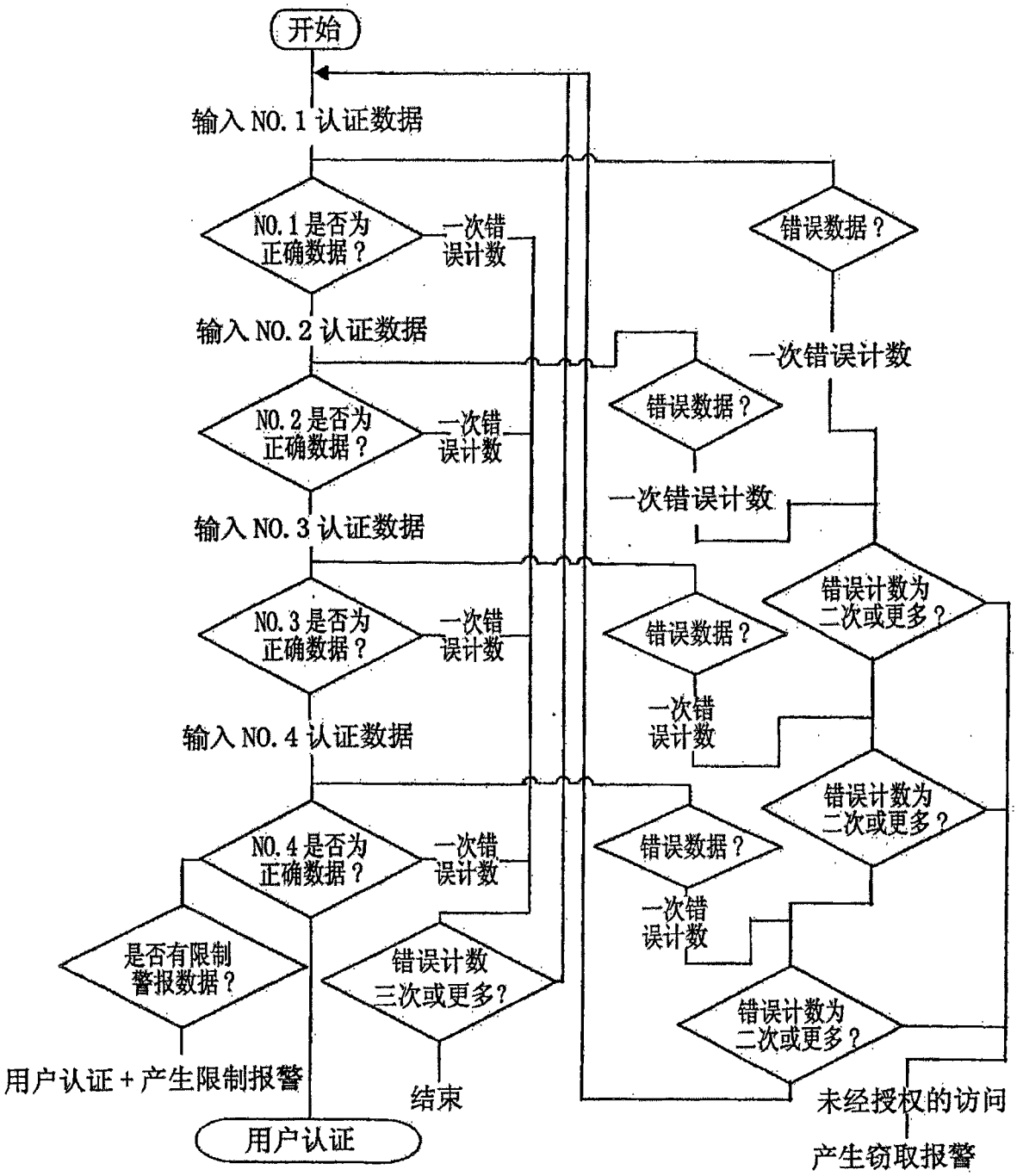

用户认证数据记录媒介
确定"A"的正确数据
认证数据注册计算机
记录"认证数据"
向用户发布具有无数匹配数据项a
的用户认证数据记录卡1A
*** 被用户保存 ***
通知正确数据的位置，顺序和特征
*** 保存在用户记录中 ***
将A的内容电子存储于
含有终端设备的计算机中
帮助用户记忆正确数据
的位置，顺序和特征
输入"A"的内容到传感器中
选择认证数据a中的
N项从用户记忆中指定
N中正确数据项
在终端单元的
显示设备上提
供"A"的内容
通过键盘操作
选择认证数据
通过认证计算
机进行对比
用户认证
窃取报警
用户认证+限制报警
管理员
用户

图17

图 18


开始
输入 NO. 1 认证数据
NO. 1 是否为正确数据？
一次错误计数
输入 NO. 2 认证数据
NO. 2 是否为正确数据？
一次错误计数
输入 NO. 3 认证数据
NO. 3 是否为正确数据？
一次错误计数
输入 NO. 4 认证数据
NO. 4 是否为正确数据？
一次错误计数
是否有限制警报数据？
用户认证＋产生限制报警
用户认证
错误计数三次或更多？
结束
错误数据？
一次错误计数
错误数据？
一次错误计数
错误数据？
一次错误计数
错误计数为二次或更多？
错误计数为二次或更多？
错误计数为二次或更多？
未经授权的访问
产生窃取报警

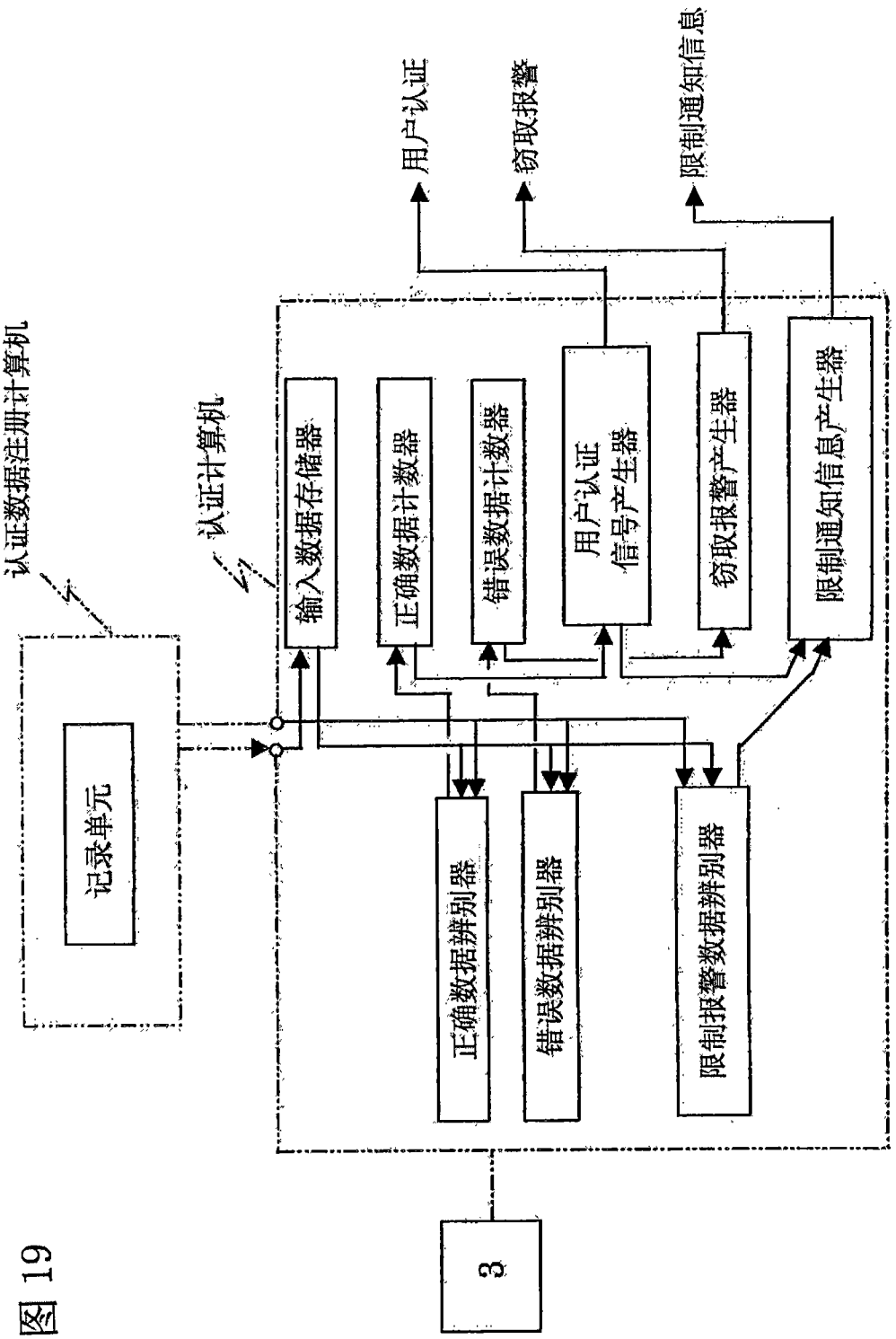
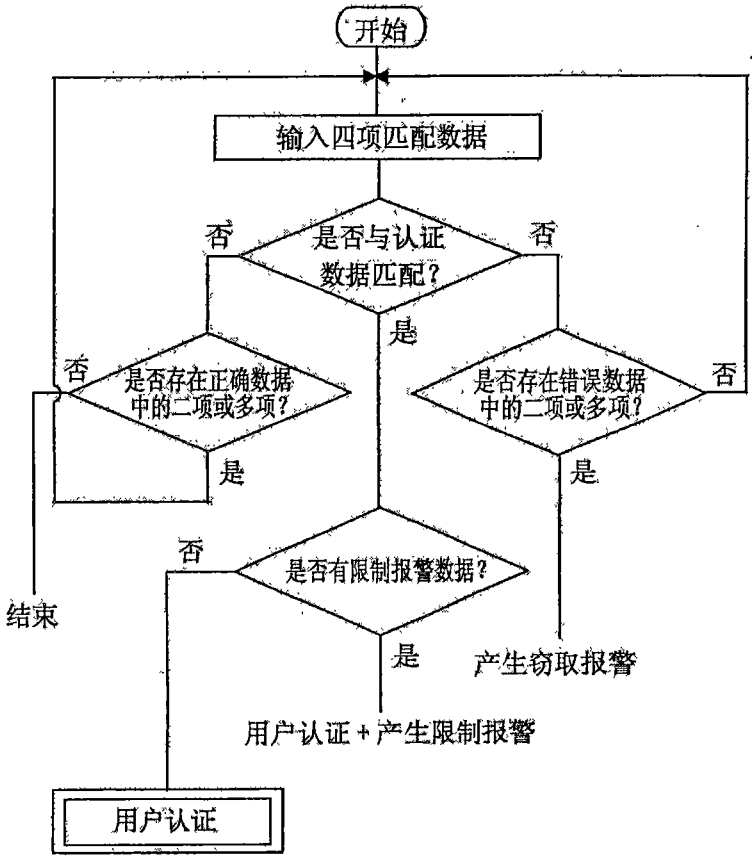

用户认证
窃取报警
限制通知信息
认证数据注册计算机
认证计算机
记录单元
输入数据存储器
正确数据计数器
错误数据计数器
用户认证
信号产生器
窃取报警产生器
限制通知信息产生器
正确数据辨别器
错误数据辨别器
限制报警数据辨别器
3

图 19

图 20


开始
输入四项匹配数据
是否与认证数据匹配?
否
否
是
是否存在正确数据中的二项或多项?
否
是
是否存在错误数据中的二项或多项?
否
是
是否有限制报警数据?
否
是
结束
产生窃取报警
用户认证+产生限制报警
用户认证