(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 106485848 B
(45)授权公告日 2020.05.01

(21)申请号 201610457915.4

(22)申请日 2016.06.22

(65)同一申请的已公布的文献号
申请公布号 CN 106485848 A

(43)申请公布日 2017.03.08

(30)优先权数据
10-2015-0122649 2015.08.31 KR
10-2015-0154494 2015.11.04 KR
10-2015-0154496 2015.11.04 KR
10-2015-0176170 2015.12.10 KR
10-2016-0001814 2016.01.07 KR
10-2016-0008115 2016.01.22 KR
10-2016-0020838 2016.02.22 KR

(73)专利权人 崔胜辛
地址 韩国首尔

(72)发明人 崔胜辛

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 李辉 金玲

(51)Int.Cl.
G07F 19/00(2006.01)
G07F 7/02(2006.01)
G06Q 20/18(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G06F 21/36(2013.01)
G06F 3/0488(2013.01)

(56)对比文件
CN 102469453 A,2012.05.23,
CN 102742256 A,2012.10.17,
CN 103425944 A,2013.12.04,
CN 101808077 A,2010.08.18,
CN 101171604 A,2008.04.30,
CN 101089901 A,2007.12.19,
CN 103460712 A,2013.12.18,
CN 102289867 A,2011.12.21,
US 2016314468 A1,2016.10.27,

审查员 张利

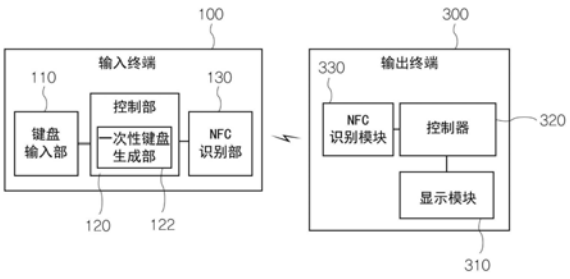
权利要求书10页 说明书25页 附图21页

(54)发明名称

利用一次性键盘的密钥输入系统及方法

(57)摘要

本发明涉及利用一次性键盘的密钥输入系统及方法，使得使用者利用一次性生成的一次性键盘(OTK)而确保物理性的安保的状态下输入密钥(密码)，作为形成有输入终端及输出终端而接收密钥输入的系统，包括：键盘输入部，输出包括删除识别标志的一个以上的无意义暗码(null)键的安全键盘，接收由使用者输入的密钥；控制部，包括生成一次性键盘的一次性键盘生成部而构成；输入终端，包括NFC识别部而构成，所述NFC识别部借助于连接的输出终端和近距离通信，向所述输出终端提供通过所述一次性键盘生成部生成的一次性键盘；显示模块；NFC识别模块，通过所述NFC识别部从所述输入终端接收一次性键盘；输出终端，通过所述显示模块输出从所述NFC识别模块接收的一次性键盘。



CN 106485848 B

1.一种利用一次性键盘的密钥输入系统,作为形成有输入终端及输出终端而接收密钥输入的系统,其特征在于,包括:

键盘输入部,输出包括删除识别标志的一个以上的无意义暗码键的安全键盘,接收由使用者输入的密钥;

控制部,包括生成一次性键盘的一次性键盘生成部而构成;

输入终端,包括NFC识别部而构成,所述NFC识别部借助于连接的输出终端和近距离通信,向所述输出终端提供通过所述一次性键盘生成部生成的一次性键盘;

显示模块;

NFC识别模块,通过所述NFC识别部从所述输入终端接收一次性键盘;

输出终端,通过所述显示模块输出从所述NFC识别模块接收的一次性键盘。

2.根据权利要求1所述的利用一次性键盘的密钥输入系统,其特征在于,

所述输出终端在设定的时间期间持续地输出所述一次性键盘后结束。

3.一种利用一次性键盘的密钥输入系统,作为形成有输入终端及输出终端而接收密钥输入的系统,其特征在于,包括:

键盘输入部,输出包括删除识别标志的一个以上的无意义暗码键的安全键盘,接收由使用者输入的密钥;

控制部,包括生成一次性键盘的一次性键盘生成部而构成;

输入终端,包括用于向所述输出终端提供通过所述一次性键盘生成部生成的一次性键盘的通信模块而构成;

显示模块;

通信部,通过所述通信模块从所述输入终端接收一次性键盘;

输出终端,包括通过所述显示模块输出接收的所述一次性键盘的控制器而构成。

4.根据权利要求3所述的利用一次性键盘的密钥输入系统,其特征在于,

所述控制部将生成的所述一次性键盘生成为SMS或MMS信息,向所述输出终端传送。

5.一种利用一次性键盘的密钥输入系统,作为形成有输入终端及输出终端而接收密钥输入的系统,其特征在于,

所述输出终端,包括:

显示模块;

NFC识别模块,通过NFC识别部从所述输入终端接收一次性键盘;

控制器,包括生成一次性键盘的一次性键盘生成部而构成,

所述输入终端,包括:

键盘输入部,输出包括删除识别标志的一个以上的无意义暗码键的安全键盘,接收由使用者输入的密钥;

所述NFC识别部,通过连接的输出终端和近距离通信接收所述一次性键盘;

控制部,通过所述一次性键盘判断由所述键盘输入部输入的密钥,确认是否解除保安。

6.根据权利要求1或5所述的利用一次性键盘的密钥输入系统,其特征在于,

所述NFC识别模块以外装型模块构成,形成于所述输出终端。

7.一种利用一次性键盘的密钥输入系统,作为形成有输入终端及输出终端而接收密钥输入的系统,其特征在于,

所述输出终端，包括：

显示模块；

控制器，包括生成一次性键盘的一次性键盘生成部而构成；

通信部，通过服务器发送所述一次性键盘，

所述输入终端，包括：

键盘输入部，输出包括删除识别标志的一个以上的无意义暗码键的安全键盘，接收由使用者输入的密钥；

通信模块，接收所述一次性键盘；

控制部，通过所述一次性键盘判断由所述键盘输入部输入的密钥，确认是否解除保安。

8.一种利用一次性键盘的密钥输入系统，作为通过输入终端接收密钥输入的系统，其特征在于，包括：

键盘输入部，输出包括删除识别标志的一个以上的无意义暗码键的输入窗口，接收由使用者输入的密钥；

控制器，包括生成一次性键盘的一次性键盘生成部而构成；

输出部，将通过所述一次性键盘生成部生成的一次性键盘在印刷用纸上印刷并输出，

并且，所述控制器通过所述一次性键盘判断由所述键盘输入部输入的密钥，确认是否解除保安。

9.根据权利要求8所述的利用一次性键盘的密钥输入系统，其特征在于，

所述输出部在输出所述印刷用纸时使得印刷有所述一次性键盘的印刷面向下方。

10.一种利用一次性键盘的密钥输入系统，作为形成有输入终端及输出终端而接收密钥输入的系统，其特征在于，

所述输出终端，包括：

显示模块；

控制器，包括生成一次性键盘的一次性键盘生成部而构成；

存储模块，存储由所述一次性键盘生成部生成的一次性键盘，

所述输入终端，包括：

输入部，输出包括删除识别标志的一个以上的无意义暗码键的输入窗口，接收由使用者输入的密钥键盘；

存储部，从所述输出终端接收所述一次性键盘并存储；

控制部，通过所述一次性键盘判断由键盘输入部输入的密钥，确认是否解除保安。

11.根据权利要求10所述的利用一次性键盘的密钥输入系统，其特征在于，

所述控制部在确认所述保安解除后删除在所述存储部存储的一次性键盘。

12.一种利用一次性键盘的密钥输入系统，作为形成有输入终端及输出终端而接收密钥输入的系统，其特征在于，包括：

输入部，输出包括删除识别标志的一个以上的无意义暗码键的输入窗口，接收由使用者输入的密钥键盘；

输入终端，包括控制部，该控制部包括生成一次性键盘的一次性键盘生成部；

显示模块；

输出终端，包括控制器，该控制器生成与通过所述控制部生成的一次性键盘同步化的

一次性键盘，并通过所述显示模块输出。

13.根据权利要求12所述的利用一次性键盘的密钥输入系统，其特征在于，

所述控制部及控制器利用在所述输入终端和所述输出终端共享的共享按键和根据生成时刻生成的同步化按键生成排列按键，并利用所述排列按键生成相互同步化的一次性键盘。

14.根据权利要求13所述的利用一次性键盘的密钥输入系统，其特征在于，

所述生成时刻按已设定的时间单位的单位时间区分；

所述同步化按键根据生成时刻在区分的时间内按生成顺序而生成。

15.根据权利要求13所述的利用一次性键盘的密钥输入系统，其特征在于，

所述一次性键盘将设定的顺序位置的所述排列按键与设定的顺序位置的拨号键位置进行匹配而生成。

16.一种利用一次性键盘的密钥输入系统，作为形成有输入终端、服务器及输出终端而接收密钥输入的系统，其特征在于，包括：

输入部，输出包括删除识别标志的一个以上的无意义暗码键的输入窗口，接收由使用者输入的密钥键盘；

通信模块，用于与所述服务器通信；

输入终端，包括控制部，该控制部通过所述通信模块接收一次性键盘，并判断通过键盘输入部输入的密钥；

服务器，包括生成一次性键盘的一次性键盘提供部而构成，并将生成的一次性键盘提供给所述输入终端和输出终端；

显示模块；

通信部，通过所述服务器接收一次性键盘；

输出终端，包括通过所述显示模块输出从所述通信部接收的一次性键盘的控制器。

17.根据权利要求16所述的利用一次性键盘的密钥输入系统，其特征在于，

所述输入终端为自动取款机或门锁。

18.根据权利要求17所述的利用一次性键盘的密钥输入系统，其特征在于，

所述一次性键盘是非定型地构成排列顺序的拨号键，每次生成时变更所述排列顺序。

19.根据权利要求17所述的利用一次性键盘的密钥输入系统，其特征在于，

所述一次性键盘根据所述密钥的个数而生成，对于各个所述密钥输入分别提供所述一次性键盘。

20.根据权利要求17所述的利用一次性键盘的密钥输入系统，其特征在于，

所述控制部通过所述一次性键盘判断由使用者输入的密钥是否与设定编码一致，并通过所述键盘输入部的颜色变化或音响输出而输出所述输入的密钥的正确/错误的判断结果。

21.根据权利要求17所述的利用一次性键盘的密钥输入系统，其特征在于，

所述输入窗口包括相比输入窗口的全部输入区域个数与设定的密钥的个数的差异值更多的个数的无意义暗码键而构成。

22.根据权利要求17所述的利用一次性键盘的密钥输入系统，其特征在于，

所述输入窗口，输入窗口的全部输入区域由无意义暗码键构成。

23.一种利用一次性键盘的密钥输入系统，作为利用拨号键输入功能及图形要素输入密钥的系统，其特征在于，包括：

控制部，包括图形输入工具生成部而构成，该图形输入工具生成部生成包括多个图形要素和删除识别标志的一个以上的无意义暗码键并形成有能够输入密钥的拨号键的图形输入工具；

显示部，显示所述图形输入工具；

操作部件，能够操作所述图形输入工具；

标示部件，标示所述多个图形要素中与密钥对应的图形要素的信息；

输出终端，与所述控制部同步化，包括所述图形输入工具的识别标志。

24.根据权利要求23所述的利用一次性键盘的密钥输入系统，其特征在于，

所述图形输入工具成为3维形状，3维的各个面形成有相互不同的图形要素；

所述图形要素由颜色、图画、图案中一个以上的组合而构成。

25.根据权利要求24所述的利用一次性键盘的密钥输入系统，其特征在于，

为了输入密钥，操作图形输入工具，设定与所述密钥对应的图形要素，利用对应于在终端设备上标示识别标志的拨号键的图形输入工具的拨号键。

26.根据权利要求24或25所述的利用一次性键盘的密钥输入系统，其特征在于，

对应于所述密钥的图形要素或在拨号键上标示的识别标志以一次性形式提供；

每次所述图形要素或识别标志一次性形式提供，所述3维的多面体更换其形状；

所述识别标志的数字或特殊记号的位置随机地设定。

27.一种利用一次性键盘的密钥输入系统，作为形成有输入终端及输出终端而接收密钥输入的系统，其特征在于，包括：

键盘输入部，由表示拨号键位置的盲人用输入面板构成，输出盲人用识别标示，并接收由使用者输入的密钥；

输入终端，包括控制部，该控制部包括生成一次性键盘的一次性键盘生成部；

语音输出模块；

输出终端，包括控制器而构成，该控制器从所述输入终端接收一次性键盘，并通过所述语音输出模块输出接收的一次性键盘。

28.根据权利要求27所述的利用一次性键盘的密钥输入系统，其特征在于，

所述输出终端为在手机终端设备或所述输入终端上附属设置的语音输出终端。

29.根据权利要求28所述的利用一次性键盘的密钥输入系统，其特征在于，

所述控制部通过所述一次性键盘判断由使用者输入的密钥是否与设定编码一致，并通过所述键盘输入部的颜色变化输出所述输入的密钥的正确/错误。

30.一种利用一次性键盘的密钥输入系统，其特征在于，包括：

密钥存储部，存储已设定的密钥；

连接模块，通过连接端子连接于终端设备；

NFC模块，通过近距离通信方式连接于终端设备；

移动式存储器，包括控制与终端设备的连接及数据收发的控制模块；

连接接口，与所述移动式存储器连接，使得能够收发数据；

密钥输入部，接收由使用者输入；

控制器，包括生成一次性非定型排列结构的一次性键盘的一次性键盘生成模块而构成；

输入终端，包括为了接收由使用者输入的密钥输出从一次性键盘生成的输入键盘的输出部；

NFC通信部，通过近距离通信与所述NFC模块进行通信；

控制部，控制通过所述移动式存储器接收从所述输入终端生成的一次性键盘并输出；

输出终端，包括输出所述一次性键盘的输出部而构成。

31.一种利用一次性键盘的密钥输入系统，其特征在于，包括：

密钥存储部，存储已设定的密钥；

连接模块，通过连接端子连接于终端设备；

NFC模块，通过近距离通信方式连接于终端设备；

移动式存储器，包括控制与终端设备的连接及数据收发的控制模块；

NFC通信部，通过近距离通信与所述NFC模块进行通信；

输出终端，包括控制部而构成，该控制部包括生成一次性非定型排列结构的一次性键盘的一次性键盘生成部而构成，生成一次性键盘，并将生成的一次性键盘向移动式存储器传送；

连接接口，与所述移动式存储器连接，使得能够收发数据；와;

输入部，接收由使用者输入的密钥；

控制器，从所述移动式存储器传送的一次性键盘生成输入键盘；

输入终端，包括为了接收使用者输入的密钥输出所述输入键盘的输出部而构成。

32.一种利用一次性键盘的密钥输入系统，其特征在于，包括：

固有密钥存储部，存储按存储媒介设定的固有密钥；

密钥存储部，存储已设定的密钥；

连接模块，通过连接端子连接于终端设备；

控制模块，控制与终端设备的连接及数据收发；

移动式存储器，包括执行近距离通信功能的NFC模块而构成；

连接接口，与所述移动式存储装置连接，使得能够收发数据收发；

输入部，接收由使用者输入的密钥；

控制器，包括生成一次性非定型排列结构的一次性键盘的一次性键盘生成模块而构成；

输入终端，包括向使用者输出输入键盘的输出部而构成；

NFC通信部，通过近距离通信与所述移动式存储器通信；

控制部，包括一次性键盘生成部而构成，该一次性键盘生成部接收所述移动式存储器传送的固有密钥，通过所述固有密钥生成一次性非定型排列结构的一次性键盘；

输出终端，包括输出通过所述一次性键盘生成部生成的一次性键盘的输出部而构成。

33.根据权利要求30至32中任意一项所述的利用一次性键盘的密钥输入系统，其特征在于，

所述一次性键盘生成模块通过从所述移动式存储器传送的固有密钥生成一次性非定型排列结构的一次性键盘。

34.根据权利要求33所述的利用一次性键盘的密钥输入系统,其特征在于,

所述一次性键盘生成模块及利用一次性键盘生成部利用

所述固有密钥和根据生成时刻生成同步化按键生成排列按键,并且,利用所述排列按键生成相互同步化的一次性键盘。

35.根据权利要求34所述的利用一次性键盘的密钥输入系统,其特征在于,

所述生成时刻根据已设定的时间单位的单位时间区分,

所述同步化按键在区分的时间内根据生成时刻按生成顺序而生成。

36.根据权利要求35所述的利用一次性键盘的密钥输入系统,其特征在于,

所述一次性键盘是将设定的顺序位置的所述排列按键与设定的顺序位置的拨号键位置进行匹配而生成。

37.根据权利要求32所述的利用一次性键盘的密钥输入系统,其特征在于,

所述一次性键盘是以非定型构成排列顺序的拨号键,每次生成时变更所述排列顺序。

38.根据权利要求37所述的利用一次性键盘的密钥输入系统,其特征在于,

所述输入键盘是由所述一次性键盘删除识别标志的安全键盘。

39.根据权利要求38所述的利用一次性键盘的密钥输入系统,其特征在于,

所述控制器根据由使用者输入的密钥与由所述移动式存储媒介传送的密钥的一致与否决定是否解除所述移动式存储器的保安。

40.根据权利要求39所述的利用一次性键盘的密钥输入系统,其特征在于,

所述移动式存储器为USB存储装置,

所述输入终端为PC。

41.一种利用一次性键盘的密钥输入方法,其特征在于,

包括如下步骤进行:

(A)输入终端通过NFC模块识别输出终端的连接的步骤;

(B)键盘输入装置生成一次性键盘的步骤;

(C)将所述输入终端生成的一次性键盘向输出终端传送的步骤;

(D)接收所述一次性键盘的输出终端输出所述一次性键盘的步骤;

(E)所述输入终端输出包括删除识别标志的一个以上的无意义暗码键的输入窗口,接收由使用者输入的密钥步骤;

(F)所述输入终端通过一次性键盘判断所述使用者输入的密钥是否与设定编码一致,判断输入的所述密钥的正确/错误的步骤。

42.根据权利要求41所述的利用一次性键盘的密钥输入方法,其特征在于,

所述第(D)步骤的一次性键盘输出持续设定的时间后结束。

43.一种利用一次性键盘的密钥输入方法,其特征在于,

包括如下步骤进行:

(A)输入终端生成一次性键盘的步骤;

(B)所述输入终端将生成的一次性键盘变换为SMS或MMS信息的步骤;

(C)所述输入终端将变换为SMS或MMS信息的所述一次性键盘传送至输出终端的步骤;

(D)接收所述一次性键盘的输出终端输出所述一次性键盘的步骤;

(E)所述输入终端输出包括删除识别标志的一个以上的无意义暗码键的安全键盘,接

收由使用者输入的密钥步骤；

(F)所述输入终端通过一次性键盘判断所述使用者输入的密钥是否与设定编码一致，判断输入的所述密钥的正确/错误的步骤。

44.一种利用一次性键盘的密钥输入方法，其特征在于，

包括如下步骤进行：

(A)输出终端生成一次性键盘的步骤；

(B)所述输出终端将所述生成的一次性键盘传送至输入终端的步骤；

(C)所述输出终端输出生成的所述一次性键盘的步骤；

(D)所述输入终端输出包括删除识别标志的一个以上的无意义暗码键的安全键盘，接收由使用者输入的密钥步骤；

(E)所述输入终端通过一次性键盘判断所述使用者输入的密钥是否与设定编码一致，判断输入的所述密钥的正确/错误的步骤。

45.根据权利要求44所述的利用一次性键盘的密钥输入方法，其特征在于，

所述第(B)步骤的所述一次性键盘传送通过所述输出终端与所述输入终端之间的连接通过NFC通信进行。

46.根据权利要求44所述的利用一次性键盘的密钥输入方法，其特征在于，

所述第(B)步骤的所述一次性键盘传送通过连接所述输出终端和所述输入终端的服务器进行。

47.根据权利要求41至46中任意一项所述的利用一次性键盘的密钥输入方法，其特征在于，

所述一次性键盘是通过使用者的排列变更命令构成排列顺序的拨号键。

48.根据权利要求47所述的利用一次性键盘的密钥输入方法，其特征在于，

所述一次性键盘是通过识别记号或颜色区分各个按键。

49.一种利用一次性键盘的密钥输入方法，其特征在于，

包括如下步骤进行：

(A)激活输入终端的键盘输入部，一次性键盘生成部生成一次性键盘的步骤；

(B)终端设备生成与通过控制部生成的一次性键盘同步化的一次性键盘的步骤；

(C)所述终端设备将同步化的所述一次性键盘以标示识别标志的状态输出的步骤；

(D)所述输入终端输出包括删除识别标志的一个以上的无意义暗码键的一次性键盘，接收由使用者输入的密钥步骤；

(E)所述输入终端通过一次性键盘判断所述使用者输入的密钥是否与设定编码一致，判断输入的所述密钥的正确/错误的步骤。

50.根据权利要求49所述的利用一次性键盘的密钥输入方法，其特征在于，

所述第(A)步骤及第(B)步骤的利用一次性键盘生成是利用在所述输入终端和所述终端设备共享的共享按键和根据生成时刻生成的同步化按键生成排列按键，并利用所述排列按键生成相互同步化的一次性键盘。

51.根据权利要求50所述的利用一次性键盘的密钥输入方法，其特征在于，

所述生成时刻根据已设定的时间单位的单位时间区分，

所述同步化按键在区分的时间内根据生成时刻按生成顺序而生成。

52.根据权利要求51所述的利用一次性键盘的密钥输入方法,其特征在于,

所述一次性键盘是将设定的顺序位置的所述排列按键与设定的顺序位置的拨号键位置进行匹配而生成。

53.根据权利要求41至46、49至52中任意一项所述的利用一次性键盘的密钥输入方法,其特征在于,

还包括将正确/错误判断结果向使用者输出的(G)步骤。

54.根据权利要求53所述的利用一次性键盘的密钥输入方法,其特征在于,

正确/错误判断及所述第(G)步骤的判断结果输出是每当使用者输入按键时执行。

55.根据权利要求54所述的利用一次性键盘的密钥输入方法,其特征在于,

所述一次性键盘是通过使用者输入生成命令而生成。

56.根据权利要求53所述的利用一次性键盘的密钥输入方法,其特征在于,

所述一次性键盘是通过识别记号或颜色区分各个按键。

57.根据权利要求53所述的利用一次性键盘的密钥输入方法,其特征在于,

所述一次性键盘根据所述密钥的个数而生成,对于各个所述密钥输入分别提供所述一次性键盘。

58.根据权利要求41至46、49至52中任意一项所述的利用一次性键盘的密钥输入方法,其特征在于,

一次性键盘输出是持续设定的时间后结束。

59.一种利用一次性键盘的密钥输入方法,其特征在于,

包括如下步骤进行:

(a)输入终端生成一次性键盘的步骤;

(b)所述输入终端向输出终端传送生成的一次性键盘的步骤;

(c)接收所述一次性键盘的输出终端语音输出所述一次性键盘的步骤;

(d)所述输入终端从输出盲人用识别标示以标示拨号键位置的盲人用输入面板接收由使用者输入的密钥的步骤;

(e)所述输入终端通过一次性键盘判断所述使用者输入的密钥是否与设定编码一致,判断输入的所述密钥的正确/错误的步骤。

60.根据权利要求59所述的利用一次性键盘的密钥输入方法,其特征在于,

所述输出终端是在手机终端设备或所述输入终端附属设置的语音输出终端。

61.根据权利要求60所述的利用一次性键盘的密钥输入方法,其特征在于,

所述输出终端在设定的时间期间反复输出所述一次性键盘。

62.根据权利要求61所述的利用一次性键盘的密钥输入方法,其特征在于,

所述一次性键盘是以非定型构成排列顺序的拨号键,每次生成时变更所述排列顺序。

63.一种利用一次性键盘的密钥输入方法,其特征在于,

包括如下步骤进行:

(A)输入终端识别移动式存储器的连接的步骤;

(B)通过连接接口从所述移动式存储器接收密钥的步骤;

(C)所述输入终端生成一次性非定型排列结构的一次性键盘向所述移动式存储器传送的步骤;

(D)所述移动式存储器将接收的所述一次性键盘向输出终端传送的步骤；

(E)所述输出终端通过输出部输出接收的所述一次性键盘的步骤；

(F)所述输入终端向使用者输出输入键盘的步骤；

(G)将由使用者输入的密钥与由所述移动式存储器传送的密钥进行比较，并根据所述密钥的一致与否决定是否解除所述移动式存储器的保安。

64.一种利用一次性键盘的密钥输入方法，其特征在于，

(A)输出终端识别移动式存储器的连接的步骤；

(B)所述输出终端生成一次性非定型排列结构的一次性键盘向移动式存储器传送的步骤；

(C)所述移动式存储器将接收的所述一次性键盘向输入终端传送的步骤；

(D)所述输入终端从所述移动式存储器通过连接接口接收密钥的步骤；

(E)所述输入终端由接收的一次性键盘生成输入键盘并输出的步骤；

(F)将由使用者输入的密钥与由所述移动式存储器传送的密钥进行比较，并根据所述密钥的一致与否决定是否解除所述移动式存储器的保安。

65.一种利用一次性键盘的密钥输入方法，其特征在于，

(a)输入终端识别移动式存储器的连接的步骤；

(b通过连接接口从所述移动式存储器接收固有密钥及密钥的步骤；

(c)通过接收的所述固有密钥生成一次性非定型排列结构的一次性键盘的步骤；

(d)向使用者输出输入键盘的步骤；

(e)输出终端通过近距离无线通信识别所述移动式存储器的连接的步骤；

(f)从所述移动式存储器通过近距离无线通信接收固有密钥的步骤；

(g)通过接收的所述固有密钥生成一次性非定型排列结构的一次性键盘的步骤；

(h)向使用者输出生成的一次性键盘的步骤；

(i)将由使用者输入的密钥与由所述移动式存储器传送的密钥进行比较，并根据所述密钥的一致与否决定是否解除所述移动式存储器的保安。

66.根据权利要求63至65中任意一项所述的利用一次性键盘的密钥输入方法，其特征在于，

输入键盘是从所述一次性键盘删除识别标志的包括一个以上的无意义暗码键而生成的安全键盘；

使用者的密钥输入是通过所述安全键盘输入。

67.根据权利要求65所述的利用一次性键盘的密钥输入方法，其特征在于，

所述一次性键盘是利用所述固有密钥和根据生成时刻生成的同步化按键生成排列按键，并利用所述排列按键相互同步化而生成。

68.根据权利要求67所述的利用一次性键盘的密钥输入方法，其特征在于，

所述生成时刻按已设定的时间单位的单位时间进行区分；

所述同步化按键是在根据生成时刻区分的时间内根据生成顺序而生成。

69.根据权利要求67所述的利用一次性键盘的密钥输入方法，其特征在于，

所述一次性键盘是将设定的顺序位置的所述排列按键与设定的顺序位置的拨号键位置进行匹配而生成。

70.根据权利要求69所述的利用一次性键盘的密钥输入方法,其特征在于,

所述输入键盘具有与所述一次性键盘相同的排列结构,为删除识别标志的安全键盘。

71.根据权利要求66所述的利用一次性键盘的密钥输入方法,其特征在于,

所述移动式存储器为USB存储装置,

所述输入终端为PC。

72.根据权利要求66所述的利用一次性键盘的密钥输入方法,其特征在于,

还包括所述输入终端接收用于在所述移动式存储器存储的密钥输入的安装程序并安装的步骤。

利用一次性键盘的密钥输入系统及方法

技术领域

[0001] 本发明涉及一种使得使用者在利用一次性生成的一次性键盘(OTK)而确保物理性的安全的状态下输入密钥(密码)的密钥输入系统及方法。

背景技术

[0002] 最近,随着电子结账工具和规模的增加,对于电子认证方式的安全保障成为非常重要的技术和事业领域。

[0003] 并且,安全技术大致可区分为电子性安全技术和物理性安全技术领域。

[0004] 电子性安全技术为用于防止借助于电子方式的安全信息的泄露的技术,是指用于防止网络黑客的系统侵入或间谍软件等非法程序的终端复制等的防火墙或保安程序的技术。

[0005] 并且,物理性安全为通过物理方式防止安全信息的泄露的技术,预防在密钥输入画面上留下指纹的薄膜,在密码输入机上防止他人的视线的防火墙等技术。

[0006] 在如上述的安全技术中,电子性安全技术通过大量的投资和研究和开发其技术得到了较大发展。

[0007] 实际上因物理性手段频繁发生安全事故,但,物理性安全技术被视为使用者个人注意的部分,而在技术方面预防安全事故的努力做得甚少。

[0008] 例如,最近频发在银行ATM机上安装信用卡复制机,并安装小型摄像头通过影像获取使用者输入的密码后,利用复制的信用卡的事故。

[0009] 并且,在家庭房门等安装的出入门开闭装置(门锁)的密码泄露,也频繁发生观察使用者输入的密码而使得密码泄露的情况。

[0010] 如上述的关于密码输入的保安方法,如图1所示,韩国登录专利第10-1045257号公开了一种将密码输入窗口随机排列构成,并通过输入方向键输入密码,而防止密码的泄露的技术。

[0011] 但,以往的技术如上述的实际发生事故示例,在利用小型摄像头等偷拍使用者的密码输入窗口时,无法预防密码的泄露。

[0012] 即,以往技术在通过物理性手段发生密码泄露时,防患其未然方面存在局限性。

[0013] 【先行技术文献】

[0014] 【专利文献】

[0015] (001)韩国登录专利第10-1045257号

[0016] (002)韩国登录专利第10-1016041号

发明内容

[0017] 发明要解决的技术问题

[0018] 本发明为了解决上述的以往问题而提出,本发明提供一种ATM机的输入窗口或门锁等键盘输入装置的密码输入状态被泄露,也能够防止密码泄露的密钥输入系统及方法。

[0019] 并且,本发明提供一种利用智能终端生成的一次性键盘,能够在各个种类的键盘输入装置输入密钥,从而,能够确保安全性,并提高使用性的密钥输入系统及方法。

[0020] 并且,本发明提供一种利用图形要素和密钥输入系统而能够在各个种类的系统输入密钥,从而,提高了安全性、趣味、实用性的密钥输入系统及方法。

[0021] 并且,本发明提供一种将移动式存储媒介(USB)插入于终端设备(PC)后,在终端设备上输入密码时,生成一次性地随机排列输入位置的一次性键盘(OTK,OnetimeKetpad),而能够在一次性键盘上输入密码,提高了移动式存储媒介的安全性的密钥输入系统及方法。

[0022] 发明的效果

[0023] 根据本发明的密钥输入系统及方法,具有如下效果。

[0024] 即,本发明即使ATM机的输入窗口或门锁等键盘输入装置的密码输入状态被泄露,也能够防止密码泄露,并且,即使智能终端被电子性手段入侵,也能够防止密码的泄露。

[0025] 更详细地,本发明中通过键盘输入装置输入密码,一次性键盘排列是通过智能终端提供,因此,在智能终端被电子性手段入侵的情况下,只有所述智能终端使用者所利用的键盘输入装置的密码输入状态被泄露才能够获取密码,因此,实际上无法发生密码泄露。

[0026] 并且,本发明中利用利用智能终端而生成的一次性键盘向各种键盘输入装置输入密钥,因此,使用者能够熟练本发明的密码输入,而提高实用性。

[0027] 并且,本发明中,密钥输入键盘使用数字及色彩图像而构成,从而,不仅加强了安全性,而且,便于扩张安全性。

[0028] 并且,本发明的另一实施例中,存储通过一次性使用而消灭的密钥进行使用,因此,需要认可一次性认证时,维持其原有的安全性,并且,一次性地将密钥提供给他人。

[0029] 并且,本发明利用图形要素和密钥输入系统而在各种系统上输入密钥,因此,提高了安全性,趣味,使用性。

[0030] 并且,本发明在终端设备上输入在移动式存储媒介上设定的密码时,生成输入位置一次性地随机排列的一次性键盘(OTK,OnetimeKetpad),从而,能够在一次性键盘上输入密码,而提高了移动式存储媒介的安全性。

[0031] 并且,根据本发明的另一实施例,分离地提供输出生成的一次性键盘的终端设备和输入密码的终端设备,并且,在输入密码的输入终端(PC)上不输出识别标志,由此,能够更加提高输入的密码的安全性。

附图说明

[0032] 图1为图示根据以往技术的密钥输入方法的一例的示例图;

[0033] 图2为表示根据本发明的利用一次性键盘的密钥输入系统的第1实施例的框图;

[0034] 图3为图示利用根据本发明的输出终端的安全键盘输入方法的详细的实施例的流程图;

[0035] 图4为图示构成本发明的输入终端及输出终端的一例的示例图;

[0036] 图5为图示根据本发明的一次性键盘提供例的示例图;

[0037] 图6为图示根据本发明的第1实施例的另一实施例的利用一次性键盘的密钥输入系统的框图;

[0038] 图7为图示根据本发明的第1实施例的另一实施例的利用一次性键盘的密钥输入

方法的流程图；

[0039] 图8为图示根据本发明的利用一次性键盘的密钥输入系统的第2实施例的框图；

[0040] 图9为图示根据本发明的第2实施例的另一实施例的利用一次性键盘的密钥输入系统的框图；

[0041] 图10为表示适用于根据本发明的利用一次性键盘的密钥输入系统及方法的一次性键盘生成例的示例图；

[0042] 图11为图示适用于根据本发明的利用一次性键盘的密钥输入系统及方法的一次性键盘生成的另一例的示例图；

[0043] 图12为适用于根据本发明的利用一次性键盘的密钥输入系统及方法的一次性键盘的一例的示例图；

[0044] 图13为图示根据本发明的第2实施例的密钥输入方法的流程图；

[0045] 图14为图示根据本发明的第2实施例的另一实施例的密钥输入系统的框图；

[0046] 图15为图示根据本发明的密钥输入系统的第3实施例的框图；

[0047] 图16为表示根据本发明的一次性键盘提供例的示例图；

[0048] 图17为图示根据本发明的第3实施例的利用一次性键盘的密钥输入方法的流程图；

[0049] 图18为图示根据本发明的利用一次性键盘的密钥输入系统的第4实施例的框图；

[0050] 图19为图示根据本发明的第4实施例的利用一次性键盘的密钥输入方法的流程图；

[0051] 图20为利用根据本发明的第5实施例的一次性键盘的密钥输入系统的框图；

[0052] 图21为图示适用于本发明的第5实施例的图形输入工具的一实施例的示例图；

[0053] 图22为图示在本发明的第5实施例中利用图形输入工具输入密码的一例的示例图；

[0054] 图23为图示将本发明的第5实施例适用于金融自动机器的图形输入工具的一例的示例图；

[0055] 图24为图示将本发明的第5实施例利用另外的终端设备适用于金融自动机器的一例的示例图；

[0056] 图25为图示本发明的第5实施例以一次性形式提供图形要素及密钥的实施例的构成的框图；

[0057] 图26为图示本发明的第5实施例通过另外的终端设备提供一次性形式的图形要素及密钥的实施例的构成的框图；

[0058] 图27为本发明的第5实施例通过另外的终端设备提供一次性形式的图形要素及密钥的实施例的示例图；

[0059] 图28为图示根据本发明的利用一次性键盘的密钥输入系统的第6实施例的示例图；

[0060] 图29为图示构成利用本发明的一次性键盘的密钥输入系统的第6实施例的安全键盘的一例的示例图；

[0061] 图30为图示构成利用本发明的第6实施例的一次性键盘的密钥输入系统的安全键盘的另一例的示例图；

[0062] 图31为图示利用本发明的第7实施例的一次性键盘的密钥输入方法的流程图.

[0063] 图32为图示构成利用本发明的第7实施例的一次性键盘的密钥输入系统的输入键盘的一例的示例图;

[0064] 图33为图示根据本发明的利用一次性键盘的密钥输入系统的第8-1实施例的构成的框图;

[0065] 图34为图示本发明的第8-1实施例的移动式存储器保安方法的流程图.

[0066] 图35为图示利用根据本发明的一次性键盘的移动式存储器保安系统的动作例的示例图;

[0067] 图36为图示利用根据本发明的一次性键盘的移动式存储器保安系统的第8-2实施例的构成的框图;

[0068] 图37为图示利用根据本发明的一次性键盘的移动式存储器保安方法的第8-2实施例的流程图;

[0069] 图38为图示利用本发明的第8-3实施例的一次性键盘的移动式存储器保安系统的框图;

[0070] 图39为图示利用根据本发明的第8-3实施例的一次性键盘的移动式存储器保安方法的流程图。

[0071] 标号说明

[0072] 100,700:输入终端 110:键盘输入部

[0073] 120:控制部 122,322:一次性键盘生成部

[0074] 130:NFC识别部 131:通信模块

[0075] 200:服务器 210:一次性键盘提供部

[0076] 300,600:输出终端 310:显示模块

[0077] 320:控制器 330:NFC识别模块

[0078] 331:通信部 800:移动式存储器

具体实施方式

[0079] 图2为图示根据本发明的利用一次性键盘的密钥输入系统的第1实施例的框图。

[0080] 根据本发明的利用一次性键盘的密钥输入系统的第1实施例,作为在输入终端上生成一次性键盘的实施例,如图2所示,根据本发明的密钥输入系统的第1实施例包括输入终端(100)和输出终端(300)而构成。

[0081] 此时,所述输入终端(100)可适用ATM机(100A)、门锁(100B)、金库(100C),电脑终端设备(100D)等输入密码(以下称为'密钥')的各种设备。

[0082] 所述输入终端(100)包括键盘输入部(110)、控制部(120)及NFC识别部(130)而构成。

[0083] 所述键盘输入部(110)为形成于所述输入终端(100)的输入窗口,通过所述键盘输入部(110)接收使用者输入的密钥。一般而言,所述键盘输入部(110)由触摸屏构成,但,也可适用物理性的按压方式的按键式输入装置。

[0084] 并且,所述控制部(120)包括用于生成一次性键盘的一次性键盘生成部(122)而构成。.

[0085] 所述一次性键盘生成部(122)为用于生成随机地排列顺序而构成的拨号键的部分,每当使用者输入密钥时,生成提供新的一次性键盘。

[0086] 并且,所述NFC识别部(130)向所述输出终端(300)提供通过形成于连接的输出终端(300)的NFC识别模块(330)和近距离通信由所述一次性键盘生成部(122)生成的一次性键盘。

[0087] 并且,所述输出终端(300)包括显示模块(310)、控制器(320)及NFC识别模块(330)而构成。

[0088] 如上所述,所述NFC识别模块(330)从所述输入终端(100)接收一次性键盘,通常为在智能手机上设置的NFC模块。

[0089] 并且,所述控制器(320)通过所述显示模块(310)输出从所述NFC识别模块(330)接收的一次性键盘。

[0090] 此时,通常所述显示模块(310)为在智能手机上形成的输出窗口。

[0091] 以下参照附图详细说明如上所述的利用本发明的输出终端的安全密钥输入方法。

[0092] 图3为图示根据本发明的利用一次性键盘的密钥输入方法的详细的实施例的流程图;图4为图示构成本发明的输入终端及输出终端的一例的示例图,图5为图示根据本发明的一次性键盘提供例的示例图。

[0093] 如图4中图示,根据本发明的利用一次性键盘的密钥输入方法,在使用者要输入密钥时,开始将输出终端(300)连接于输入终端(100)(S110)。

[0094] 即,如图4所示,所述输入终端(100)为ATM机时,使用者使用通常的方法插入卡选择所需的交易,如需向输入终端(100)输入密钥时,向形成于输入终端(100)的NFC识别部(130)连接输出终端(300)。

[0095] 所述拨号键识别装置(100)当识别所述输出终端(300)的NFC识别模块(330)时,生成一次性键盘(S120,S130)。

[0096] 此时,所述一次性键盘是指随机地设定按键排列的一次性键盘。

[0097] 然后,生成的一次性键盘通过NFC通信被传送至输出终端(300)(S140)。

[0098] 并且,如图5所示,接收所述一次性键盘的输出终端(300)将所述一次性键盘通过显示模块(310)输出。

[0099] 如图5所示,一次性键盘为变形排列而一次性生成的输入键盘。

[0100] 并且,所述输出终端(300)计算时间(S160),在设定的时间期间输出一次性键盘后,结束一次性键盘的输出(S170)。

[0101] 并且,向所述输出终端(300)输出一次性键盘的输入终端(100)向键盘输入部(110)输出只表示拨号键的区分领域的安全键盘,并从使用者接收按键输入。

[0102] 即,如图5所示,输入终端(100)输出未表示数字或记号的按键输入窗口(安全键盘),使用者通过输出终端(300)确认一次性键盘,并通过键盘输入部(110)输入密钥。

[0103] 以下将未表示数字或记号的输入窗口的按键称为无意义暗码(null)键。

[0104] 并且,识别使用者的密钥输入后,所述输入终端(100)解读(变换)按生成的一次性键盘的排列输入的密钥(S210,S220)。

[0105] 然后,所述输入终端(100)判断输入的密钥和设定编码是否一致(S230)。

[0106] 此时,所述设定编码是指设定的密码,如果为ATM机,当使用者插入卡时进行解读,

如果是门锁为设定的密码,如果是电脑终端设备,为需要使用者确认的网站上设定的密码等。

[0107] 并且,输出所述输入的密钥与设定编码是否一致(S240)。

[0108] 在此,所述输入密钥与设定编码的一致与否可对于一个按键输入分别进行,也可在设定的长度的密钥都被输入之后进行。

[0109] 此时,所述第240步骤的输出为通过显示的输出,也可为通过音响的输出。例如,所述密钥输入与设定编码一致时,以特定颜色(绿色)输出输入的按键位置,如果不一致的输入时,以其他颜色(红色)输出输入的按键位置,而能够即刻知晓按键输入的正确/错误。

[0110] 以下参照附图说明根据本发明的第1实施例的另一实施例。

[0111] 根据本发明的第1实施例的另一实施例涉及一种不利用NFC而是通过SMS或MMS将在所述输入终端生成的一次性键盘传送至输出终端的实施例。

[0112] 为此,根据本发明的第1实施例的另一实施例,如图6所示,包括输入终端(100)和输出终端(300)而构成。

[0113] 并且,所述输入终端(100)形成有为输入密钥的键盘输入部(110)。

[0114] 如图6所示,根据本发明的利用一次性键盘的密钥输入系统的细部构成,根据本发明的利用一次性键盘的安全密钥输入系统,包括输入终端(100)、服务器(200)、输出终端(300)而构成。

[0115] 所述输入终端(100)是接收输入的密钥,而决定保安的解除与否的终端设备,为此,所述输入终端(100)包括键盘输入部(110)、控制部(120)及通信模块(131)而构成。

[0116] 所述键盘输入部(110)是形成于所述输入终端(100)的输入窗口,优选地,由形成有触摸屏的显示装置构成。

[0117] 此时,所述通信模块(131)是用于通过有线/无线通信连接于所述服务器(200)而向输出终端(300)传送生成的一次性键盘,通常,适用有线通信模块,但,根据安装场所及环境也可适用Wi-Fi等无线通信模块。

[0118] 并且,所述控制部(120)生成一次性键盘并将其向所述输出终端(300)提供,并判断使用者通过所述键盘输入部(110)输入的输入按键是否一致。为此,所述控制部(120)包括一次性键盘生成部(122)而构成。

[0119] 所述一次性键盘生成部(122)是生成随机地构成排列顺序的拨号键(参照图5)的部分,每次使用者输入密钥时生成新的一次性键盘,并提供给所述输出终端(300)。

[0120] 并且,所述控制部(120)将由所述一次性键盘生成部(122)生成的所述一次性键盘通过所述服务器(200)传送给所述输出终端(300),优选地,以SMS或MMS形态的信息传送。

[0121] 为此,所述控制部(120)将生成的一次性键盘变换为所述SMS或MMS形态。

[0122] 并且,所述控制部(120)利用生成的一次性键盘生成安全键盘,并将所述安全键盘输出至所述键盘输入部(110)。

[0123] 此时,所述安全键盘的排列形态与一次性键盘相同,但,如图5所示,各个按键以无意义暗码(null)键(未表示数字或记号的按键)表示,成为只表示拨号键的区分领域的输入窗口,从而,即使在所述安全键盘上暴露输入密钥的状态,也无法知晓实际输入的密钥是什么。

[0124] 并且,所述安全键盘以各种实施例构成。

[0125] 即，根据所述安全键盘的另一实施例，可输出表示一部分数字或记号的输入窗口。由此，使用者与所述安全键盘进行匹配识别在输出终端(300)表示的一次性键盘的排列。

[0126] 此时，优选地，在所述键盘输入部(110)表示的数字或记号的个数设定为少于设定的密钥个数。

[0127] 即，在所述键盘输入部(110)表示的数字或记号的个数大于设定的密钥个数时，可能使得要输入的全部密钥都在所述键盘输入部(110)上表示，因此用于防止发生此类情况。

[0128] 例如，为由12个区域构成的输入窗口时，密钥以4位设定时，可能有以大约1/11880左右的概率输入的全部的密钥都在所述键盘输入部(110)上表示的可能性。为了防止上述情况，优选地，在所述键盘输入部(110)上表示的数字或记号的个数设定成少于设定的密钥个数。

[0129] 并且，所述服务器(200)作为由所述输入终端(100)接收所述一次性键盘而向所述输出终端(300)传送的服务器，可为提供文字信息的移动通信社的服务器，也可为在网络上的各种通讯服务器。

[0130] 并且，所述输出终端(300)是用于将接收的一次性键盘向使用者输出，包括显示模块(310)、控制器(320)及通信部(331)而构成。

[0131] 所述通信部(331)是从所述服务器(200)接收一次性键盘的部分。

[0132] 并且，所述控制器(320)将从所述通信部(331)接收的一次性键盘输出至所述显示模块(310)。

[0133] 此时，所述显示模块(310)通常为形成于输出终端(300)的输出窗口。

[0134] 以下参照附图详细说明如上所述的根据本发明的第1实施例的另一实施例的密钥输入方法。

[0135] 图7为表示根据本发明的详细的实施例的利用一次性键盘的密钥输入方法的流程图。

[0136] 如图所示，利用本发明的一次性键盘的密钥输入方法的详细的实施例从在输入终端(100)生成按键输入信息开始(S1110)。

[0137] 并且，生成所述按键输入信息时，所述一次性键盘生成部(122)生成一次性键盘(S1120)。

[0138] 此时，如上所述，所述一次性键盘是指随机地设定按键排列的拨号键。

[0139] 然后，所述输入终端(100)以SMS或MMS形态构成生成的一次性键盘，通过服务器(200)传送至所述输出终端(300)(S1130)。

[0140] 此时，所述输出终端(300)的固有号码(电话号码等)要预先存储在所述输入终端内。

[0141] 并且，传送所述一次性键盘的所述输入终端(100)从所述一次性键盘生成安全键盘，并向所述键盘输入部(110)输出(S1140)。

[0142] 此时，所述安全键盘如上述。

[0143] 并且，接收所述一次性键盘的输出终端(300)将接收的一次性键盘通过所述显示模块(310)输出(S1150)。

[0144] 并且，所述一次性键盘的输出可伴随使用者确认接收的SMS或MMS信息的顺序进行。

[0145] 并且，输出所述一次性键盘的所述输出终端(300)的控制器(320)计算时间(S1160)，在设定的时间期间输出一次性键盘之后，结束一次性键盘的输出(S1170)。

[0146] 此时，所述一次性键盘为一次性键盘，因此，所述控制器控制随着结束所述一次性键盘的输出，删除接收的SMS或MMS。

[0147] 并且，输出所述安全键盘的输入终端(100)接收由使用者输入的密钥(S1210)。

[0148] 并且，当识别使用者的密钥输入时，所述输入终端(100)按生成的一次性键盘的排列解读(变换)输入的密钥(S1220)。

[0149] 然后，所述输入终端(100)判断输入的密钥和设定编码是否一致(S1230)。

[0150] 并且，输出所述输入的密钥是否与设定编码一致(S1240)。

[0151] 图8为表示根据本发明的利用一次性键盘的密钥输入系统的第2实施例的框图。

[0152] 根据本发明的利用一次性键盘的密钥输入系统的第2实施例，为在输出终端生成一次性键盘的实施例，如图8所示，根据本发明的密钥输入系统的第2实施例，包括输入终端(100)和输出终端(300)而构成。

[0153] 所述输入终端(100)由键盘输入部(110)，控制部(120)及NFC识别部(130)而构成。

[0154] 以下，省略对于执行与上述的实施例相同的功能的构成要素的重复说明。

[0155] 此时，所述NFC识别部(130)从所述输出终端(300)通过在连接的输出终端(300)上形成的NFC识别模块(330)和近距离通信接收生成的一次性键盘。

[0156] 并且，所述输出终端(300)包括显示模块(310)、控制器(320)及NFC识别模块(330)而构成。

[0157] 如上述，所述NFC识别模块(330)是用于向所述输入终端(100)传送一次性键盘。

[0158] 此时，所述控制器(320)包括生成一次性键盘的一次性键盘生成部(322)而构成。

[0159] 所述一次性键盘生成部(322)是生成随机地形成排列顺序的拨号键的部分，是根据使用者的生成命令生成新的一次性键盘的部分。

[0160] 并且，所述控制器(320)通过所述显示模块(310)输出通过所述一次性键盘生成部(322)生成的一次性拨号。

[0161] 并且，如图9所示，本发明的第2实施例的另一实施例，可包括输入终端(100)、服务器(200)及输出终端(300)而构成。

[0162] 即，图9中图示的实施例是在未形成有NFC模块的输出终端适用本发明，由所述输出终端(300)生成的一次性键盘通过所述服务器(200)提供给所述输入终端(100)。

[0163] 为此，所述输入终端(100)包括键盘输入部(110)、控制部(122)及通信模块(131)而构成。

[0164] 所述键盘输入部(110)为形成于所述输入终端(100)的输入窗口，所述控制部(122)通过后述的服务器(200)接收提供的一次性键盘，并判断是否与使用者通过所述键盘输入部(110)输入的输入按键一致。

[0165] 所述通信模块(131)为通过上网使得能够连接服务器(200)的通信模块，通常除了有线通信之外还可适用Wi-Fi等无线通信。

[0166] 并且，所述服务器(200)将由所述输出终端(300)生成的一次性键盘传送给所述输入终端(100)，当所述输入终端接收分配的另外的通信地址而能够进行独自的通信时，也可省略。

[0167] 并且，所述输出终端(300)包括显示模块(310)、控制器(320)及通信部(331)而构成。

[0168] 所述通信部(331)通过上网连接于所述服务器(200)，并将通过所述控制器(320)生成的一次性键盘提高给所述输入终端(100)。

[0169] 并且，所述控制器(320)包括一次性键盘生成部(322)而构成，通过所述一次性键盘(322)生成一次性键盘，并通过所述显示模块(310)输出生成的所述一次性键盘。

[0170] 以下详细说明所述一次性键盘及安全键盘。

[0171] 所述一次性键盘是通过随机的运算法则随意地排列拨号键的位置的拨号键，一次性地生成并消灭。

[0172] 即，以通常的4by3排列的拨号键为例，是指在各个输入按键上没有按顺序排列1至#，而是在各个输入按键上配列随机的输入命令的拨号键。

[0173] 如上所述的一次性键盘通过使用者的特定输入命令而生成。

[0174] 即，如图10所示，在拨号键输入窗口输入特定形态的触摸输入(圆形)，或输入特定形态的动作(晃动等)，而将排列按键以洗牌(Shuffle)形态生成。

[0175] 并且，如上述，所述一次性键盘可通过随机运算法则而生成，但也可通过使用者的任意操作而生成。

[0176] 即，图11中所示，使用者在基本拨号键状态下拖拽各个排列按键的位置而变更，由此，能够生成自己所需的一次性键盘。

[0177] 从而，使用者能够使用自己喜爱的排列的一次性键盘，并且，如上述地通过使用者生成的一次性键盘在一定期间(使用者变更之前)存储于所述输出终端而使用。

[0178] 此时，所述一次性键盘的一次性并非意味着每次使用时变更拨号键排列，而是指在一定时间之后变更。

[0179] 并且，所述一次性键盘与通常的拨号键相同地，将数字和一系列的记号(*,#)为区分记号而构成，但如图12所示，也可与数字等的记号以颜色进行区分。

[0180] 在图12中，根据专利说明书的特性，以阴影的差异区分颜色而图示。

[0181] 当然，所述拨号键的大小也可由通常的4by3形成，但也可扩大排列而提高安全性。

[0182] 即，在通常的密钥输入时，要将密钥的长度及种类设定得较长，而提高安全性，因此，使得使用者难以记住密钥，导致使用的不便，但，本发明既可以维持既定长度的密钥又能够扩张拨号键的大小而提高了安全性，从而，提高安全性也不妨碍使用方面的不便。

[0183] 并且，如图4中说明，向输入终端(100)输出的安全键盘与所述一次性键盘相同地排列构成，但，是指删除识别标志的形态的拨号键。

[0184] 以下参照附图详细说明如上所述的本发明的第2实施例的密钥输入方法。

[0185] 图13为表示本发明的第2实施例的密钥输入方法的详细的实施例的流程图。

[0186] 如图所示，根据本发明的第2实施例的密钥输入方法，从使用者通过输出终端(300)生成一次性键盘开始(S2110)。

[0187] 此时，所述一次性键盘可通过使用者的命令输入被洗牌随机地发生，也可通过使用者的任意的排列操作而生成。

[0188] 当然，如果有存储的通过使用者的任意的排列操作存储的一次性键盘时，可读取所述存储的一次性键盘而使用。

[0189] 然后，将所述输出终端(300)连接于输入终端(100)而识别近距离无线通信(S2120)。

[0190] 当所述拨号键识别装置(100)和所述输出终端(300)通过近距离无线通信(NFC)被识别时，通过所述近距离无线通信由所述输出终端(300)生成的一次性键盘被传送至所述输入终端(100)，而使得所述一次性键盘同步(S2130,S2140)。

[0191] 并且，根据本发明的另一实施例，所述一次性键盘的传送，所述拨号键识别装置(100)可不与所述输出终端(300)连接，而通过通信部(331)和通信模块(131)通过网络传送。

[0192] 然后，所述输出终端(300)通过显示模块(310)输出生成的一次性键盘(S2150)。

[0193] 并且，所述输出终端(300)计算时间，在设定的时间期间输出一次性键盘后，结束一次性键盘的输出(S2160)。

[0194] 当结束所述一次性键盘的输出后也可删除所述一次性键盘(S2170)。

[0195] 并且，接收从所述输出终端(300)传送的一次性键盘的输入终端(100)，输出在键盘输入部(110)只表示拨号键的区分领域的输入窗口，而接收使用者的按键输入(S2210)。

[0196] 即，输入终端(100)输出未表示数字或记号的密钥形态的输入窗口，使用者通过输出终端(300)确认一次性键盘后，通过键盘输入部(110)输入密钥。

[0197] 并且，当识别使用者的密钥输入后，所述输入终端(100)解读(变换)根据生成的一次性键盘的排列而输入的密钥(S2220)。

[0198] 然后，所述输入终端(100)判断输入的密钥是否与设定编码一致(S2230)。

[0199] 并且，输出所述输入的密钥是否与设定编码一致(S2240)。

[0200] 以下上面本发明的第2实施例的又另一实施例。

[0201] 图14为表示根据本发明的第2实施例的又另一实施例的密钥输入系统的框图。

[0202] 如图14所示，根据本发明的第2实施例的密钥输入系统的又另一实施例，输入终端(100)和输出终端(300)分别包括存储部(140)和存储模块(340)而构成。

[0203] 这是为了本发明的又另一实施例的所述输出终端(300)通过NFC的识别而生成一次性键盘并与所述输入终端(100)同步后，将所述一次性键盘分别存储于所述存储部(140)和存储模块(340)以便使用。

[0204] 如下更详细地说明，从所述输出终端(300)通过NFC识别所述输入终端(100)开始。

[0205] 然后，所述输出终端(300)通过一次性键盘生成部(322)生成一次性键盘，并将所述生成的一次性键盘通过NFC通信传送至输入终端。

[0206] 当然，此时，所述一次性键盘通过使用者的命令生成，并通过NFC通信共享。

[0207] 并且，所述一次性键盘分别存储于输入终端(100)的存储部(140)及所述输出终端(300)的存储模块(340)。

[0208] 然后，所述使用者通过输入终端(100)的键盘输入部(110)输入密钥而解除保安后，在所述存储部(140)存储的一次性键盘被删除消灭。

[0209] 并且，在所述输出终端(300)通过使用者的输入命令或NFC识别生成一次性键盘时，新生成的一次性键盘通过NFC通信被存储于所述输入终端(100)的存储部(140)，并维持存储状态直至通过使用者密钥输入解除保安为止。

[0210] 根据如上所述的本发明的又另一实施例，本发明的又另一实施例能够克服生成一

次性键盘时与密钥输入时的时间性差异及输入终端(100)与输出终端(300)的空间性差异。

[0211] 即,一旦生成一次性键盘,并存储于所述输入终端(100)和输出终端(300后,如果存在时间上的差异或密钥输入者未持有输出终端时,也可通过所述输出终端(300)持有人的帮助而一次性地输入密钥。

[0212] 如上述的本发明的又另一实施例,在所述输入终端(100)上适用门锁时具有很大的实效性。

[0213] 例如,已经生成一次性键盘而被存储于所述输入终端(100)和输出终端(300)后,输出终端(300)持有人(户主等)外出后,发生需要向他人一次性提供门锁的解除的情况时(房产中介人等在户主外出时访问),输出终端(300)持有人向他人只告诉拨号键的输入位置及顺序,而能够弥补解除门锁。

[0214] 此时,一次性地解除门锁的保安后,即消灭存储的一次性键盘,因此,即使输入相同位置的按键,也无法解除保安,而能够防止密码本身泄露给他人。

[0215] 并且,也可将本发明的本发明的详细的实施例和又另一实施例合并实施。

[0216] 即,一般而言,如同本发明的详细的实施例或另一实施例一样,所述输出终端(300)和输入终端(100)用于一次性生成一次性键盘而接收密钥输入,并且,生成单独的一次性键盘存储于所述存储部(140)及存储模块(340),只在需要在远距离允许他人出入时,告知根据存储的一次性键盘的密钥输入位置及顺序。

[0217] 当然,此时也当认可保安解除后,在所述存储部(140)存储的一次性键盘将被删除。

[0218] 并且,根据本发明输入终端的对象设备不同地形成细部性的构成而实施。

[0219] 例如,所述输入终端可为电脑终端设备。

[0220] 此时,所述键盘输入部可由适用于电脑终端设备的显示装置(显示器)和人机界面装置(鼠标等)而构成,并且,由所述输出终端生成的一次性键盘通过有线/无线通信与电脑终端设备共享。

[0221] 并且,本发明如果在所述输入终端形成有另外的输出装置,可不形成所述输出终端而实施。

[0222] 例如,如果所述输入终端为ATM设备时,所述输入终端包括形成一次性键盘生成部而构成的控制部、输出部而构成。

[0223] 所述一次性键盘生成部是每当使用者输入密钥输入时生成一次性键盘的部分,所述输出部将生成的一次性键盘在印刷用纸等输出媒介上印刷,而提供给使用者的部分。

[0224] 即,如果使用者在使用所述输入终端(ATM)时需输入密钥,所述输入终端通过所述一次性键盘生成部生成一次性键盘,并将其通过所述输出部在用纸上印刷输出。

[0225] 在此,为了加强本发明的安全性,所述输出部在输出用纸时可使得印刷有一次性键盘的印刷面向下方,并使得所述输出用纸以被卷曲的形态输出,而防止让人识别印刷有所述一次性键盘的用纸。

[0226] 然后,所述输入终端向键盘输入部输出删除识别标志的安全键盘,使用者根据在所述输出用纸上印刷的一次性键盘,在所述安全键盘上输入与自己的密码(密钥)相应的位置的按键。

[0227] 由此,使用者即使未持有另外的输出终端,也可利用一次性键盘而输入密钥。

[0228] 当然，如上述的本发明的实施形态除了ATM设备之外还可适用于形成有输出部件的各种设备(门锁、金库等)。

[0229] 以下参照附图说明根据本发明的利用一次性键盘的密钥输入系统的第3实施例。

[0230] 根据本发明的利用一次性键盘的密钥输入系统的第3实施例，为输入终端及输出终端共享通过时间同步化方式被同步化的一次性键盘的实施例。

[0231] 图15为表示根据本发明的密钥输入系统的第3实施例的框图，图16为表示根据本发明的一次性键盘提供例的示例图。

[0232] 如图15中表示，根据本发明的利用一次性键盘的密钥输入系统包括输入终端(100)和输出终端(300)而构成。

[0233] 所述输入终端(100)包括键盘输入部(110)、控制部(120)而构成。

[0234] 所述键盘输入部(110)为形成于所述输入终端(100)的输入窗口，并通过所述键盘输入部(110)接收由使用者输入的密钥。

[0235] 并且，所述控制部(120)包括生成一次性键盘的一次性键盘生成部(122)而构成。

[0236] 所述一次性键盘生成部(122)是生成随机地构成排列顺序的拨号键的部分，每当使用者输入密钥时，生成提供新的一次性键盘。

[0237] 并且，所述输出终端(300)包括显示模块(310)及控制器(320)而构成。

[0238] 并且，所述控制器(320)是生成与由所述一次性键盘生成部(122)生成的一次性键盘同步化的(相同的)一次性键盘，并通过所述显示模块(310)输出的部分，所述一次性键盘生成部和所述控制器(320)生成被同步化的一次性键盘的原理，在以下说明图16时详细地说明。

[0239] 此时，所述终端设备可为通常的智能手机，也可为一次性键盘提供用专用终端设备。

[0240] 并且，所述控制部向键盘输入部(110)输出生成的一次性键盘，并以为表示识别标志的无意义暗码(null)键形态的安全键盘输出。

[0241] 并且，所述控制器(320)通过所述显示模块(310)将变形排列生成的一次性键盘以形成识别标志的状态输出。

[0242] 并且，说明生成所述一次性键盘生成部(122)和控制器(320)被同步化的一次性键盘的方法。

[0243] 首先，所述控制部(120)的一次性键盘生成部(122)及控制器(320)分别共享相同的共享按键。此时，所述共享按键的共享通过另外的注册顺序而共享。

[0244] 并且，在生成所述一次性键盘时，利用在所述一次性键盘生成时刻而生成的同步化按键和所述共享按键生成排列按键。此时，所述排列按键生成运算法则可适用单纯演算及各种加密算法。

[0245] 从而，如果所述一次性键盘生成时刻一致，所述一次性键盘生成部(122)和控制器(320)将生成相同的排列按键。

[0246] 当然，为了克服生成所述一次性键盘时的误差，所述同步化按键也可以按既定时间单位(例如分钟单位)区分的单位时间生成。

[0247] 并且，同步化按键可根据生成时刻的生成顺序而生成。

[0248] 即，所述同步化按键可按设定的区分单位的时间根据生成顺序而生成，例如，如果

所述区分单位的时间为1小时，根据按每个小时初期化的生成顺序生成同步化按键。

[0249] 从而，如果在设定的时间内同步化按键生成次数相同，所述输入终端和输出终端能够生成相同的同步化按键。

[0250] 因此，如果将所述区分单位的时间设定较长时，能够减少根据一次性键盘生成时刻的误差发生，但，在发生错误时至生成次数初期化为止的等待时间较长，相反，将所述区分单位的时间设定较短时，根据一次性键盘生成时刻的误差发生可能性较高，但发生错误时生成次数初期化的时间较短。

[0251] 并且，优选地，所述排列按键以对应于要生成的一次性键盘的区分个数的阵法的按键生成。

[0252] 即，优选地，所述一次性键盘的区分个数为4by3形态的12个时，所述排列按键以12阵法的数生成，如果为3by3形态的9个时，所述排列按键以9阵法的数生成。

[0253] 这是为了防止通过所述排列按键生成所述一次性键盘时，剩下匹配区分或不足。

[0254] 并且，所述一次性键盘生成部(122)及控制器(320)分别利用生成的排列按键生成一次性键盘。

[0255] 所述一次性键盘将设定的顺序位置的所述排列按键与设定的顺序位置的拨号键位置进行匹配而生成。

[0256] 即，如图16所示，以排列按键以12阵法'8757214493B560BA81'生成的情况为例说明，在一次性键盘的(1,1)区域匹配匹配单位(在本例中是数字)'8'，在(1,2)区域匹配匹配单位'7'，在(1,3)区域匹配匹配单位'5'的顺序顺次进行匹配。

[0257] 在此，在(2,1)区域应匹配匹配单位'7'，但，匹配单位'7'在(1,2)区域已经匹配，因此，匹配排列按键的以一个匹配单位'2'。

[0258] 通过如上述的方式在一次性键盘的全部区域完成匹配，而生成所述一次性键盘。

[0259] 此时，从所述排列按键的一次性键盘匹配运算法则可以多种类地变形，例如，将所述匹配顺序以所述排列按键的反顺序进行，也可只使用所述排列按键的单数或双数次序的匹配单位。

[0260] 并且，所述匹配过程可除所述一次性键盘的区域中的一个而进行，对于最后一个区域匹配剩余的匹配单位。

[0261] 并且，所述一次性键盘生成部(122)及控制器(320)按要输入的密钥的个数生成所述一次性键盘，并且，每当输入一个所述密钥，提供不同的所述一次性键盘，而提供保安程度。

[0262] 以下参照附图详细说明如上所述的本发明的第3实施例的利用一次性键盘的密钥输入方法。

[0263] 图17为表示本发明的第3实施例的利用一次性键盘的密钥输入方法的详细的实施例的流程图。

[0264] 如图17所示，根据本发明的利用一次性键盘的密钥输入方法，在所述输入终端(100)及输出终端(300)生成拨号键输入信息开始(S3120,S3130)。

[0265] 此时，所述拨号键输入信息是生成一次性键盘的信息，如果为所述输入终端(100)，在一系列的动作过程中自动地生成。即，如果所述输入终端为ATM机，如同信用卡的输入，可在使用者输入密钥(密码)的步骤生成，如果所述输入终端为门锁，在开放盖子等使

用者输入密钥(密码)的步骤生成。

[0266] 并且,如果是所述输出终端(300),所述拨号键输入信息可从输入所述输出终端(300)上的特定按键而生成。

[0267] 并且,所述输入终端(100)和输出终端(300)分别生成所述拨号键输入信息时,所述输入终端(100)的所述一次性键盘生成部(122)及控制器(320)生成一次性键盘(S3140,S3150)。

[0268] 此时,如上述地,准确地,所述一次性键盘为随机地设定按键排列的拨号键,利用共享按键及同步化按键而生成。

[0269] 即,通过所述一次性键盘生成部(122)及控制器(320)共享的共享按键和根据生成时刻的同步化按键生成排列按键。

[0270] 并且,根据所述排列按键在所述一次性键盘的区分区域匹配所述排列按键的匹配单位,而生成所述一次性键盘。

[0271] 如上述地,所述输入终端(100)及输出终端(300)能够持有被同步化的相同的一次性键盘。

[0272] 并且,所述输出终端(300)通过显示模块(310)输出所述一次性键盘(S3160)。

[0273] 并且,所述输出终端(300)计算时间(S3165),在设定的时间期间输出一次性键盘之后,结束一次性键盘的输出(S3170)。

[0274] 并且,所述输入终端(100)向键盘输入部(110)输出只表示拨号键的区分领域的输入窗口,从使用者接收按键输入。

[0275] 即,所述输入终端(100)只输出未表示数字或记号的按键输入窗口,使用者通过输出终端(300)确认一次性键盘,并通过键盘输入部(110)输入密钥。

[0276] 并且,识别使用者的密钥输入时,所述输入终端(100)根据生成的一次性键盘的排列解读(变换)输入的密钥(S3210,S3220)。

[0277] 然后,所述输入终端(100)判断输入的密钥是否与设定编码一致(S3230)。

[0278] 此时,所述设定编码是指设定的密码,输出所述输入的密钥是否与设定编码一致(S3240)。

[0279] 以下参照附图说明根据本发明的利用一次性键盘的密钥输入系统的第4实施例。

[0280] 根据本发明的利用一次性键盘的密钥输入系统的第4实施例,在服务器生成一次性键盘而向输入终端及输出终端传送的实施例。

[0281] 图18为表示根据本发明的利用一次性键盘的密钥输入系统的第4实施例的框图。

[0282] 如图18所示,根据本发明的密钥输入系统的第4实施例包括输入终端(100)、服务器(200)及输出终端(300)而构成。

[0283] 即,本发明的另一实施例是为了在未形成有NFC模块的输出终端适用本发明,通过所述服务器(200)生成一次性键盘,向所述输入终端(100)及输出终端(300)提供。

[0284] 为此,所述输入终端(100)包括键盘输入部(110)、控制部(122)及通信模块(132)而构成。

[0285] 所述键盘输入部(110)形成于所述输入终端(100)的输入窗口,所述控制部(122)从后述的服务器(200)接收提供的一次性键盘,并判断是否与使用者通过所述键盘输入部(110)输入的输入按键一致。

[0286] 所述通信模块(132)是通过上网能够连接于服务器的通信模块,通常适用有线通信模块,但也可根据安装场所及环境适用Wi-Fi等无线通信模块。

[0287] 并且,所述服务器(200)包括生成一次性键盘的一次性键盘提供部(210)而构成。所述一次性键盘提供部(210)是生成随机地构成排列顺序的拨号键的部分,每当使用者的输入密码时,生成新的一次性键盘,提供给所述输入终端(100)及输出终端(300)。

[0288] 并且,所述输出终端(300)包括显示模块(310)、控制器(320)及通信部(332)而构成。

[0289] 所述通信部(332)通过上网连接于所述服务器(200),从所述服务器(200)接收一次性键盘。

[0290] 并且,所述控制器(320)通过所述显示模块(310)输出从所述通信部(332)接收的一次性键盘。

[0291] 并且,图19为表示根据本发明的第4实施例的利用一次性键盘的密钥输入方法的流程图。

[0292] 如上述图示,根据本发明的第4实施例的密钥输入方法从输入终端(100)生成按键输入信息传送给服务器(200)开始(S4310,S4320)。

[0293] 即,所述输入终端(100)如果为ATM机,使用者如通常的方法插入卡选择要进行的交易,并到密钥输入步骤时,输入终端(100通过所述服务器(200)生成按键输入信息向所述服务器(200)传送。

[0294] 然后,所述服务器(200)的一次性键盘提供部(210)生成一次性键盘(S4330)。

[0295] 并且,所述服务器(200)将生成的一次性键盘分别向所述输入终端(100)及输出终端(300)传送(S4340)。

[0296] 然后,如在本发明的另一实施例中的说明,接收所述一次性键盘的输出终端(300)通过显示模块(310)在设定的时间期间输出所述一次性键盘后,结束输出(S4350,S4360,S4370)。

[0297] 并且,接收所述一次性键盘的输入终端(100)输出在键盘输入部(110)只表示拨号键的区分领域的输入窗口,接收使用者输入的按键,并识别由使用者输入的密钥,根据接收的一次性键盘的排列解读(变换)输入的密钥(S4410,S4420,S4430)。

[0298] 并且,输出所述输入的密钥是否与设定编码一致的过程如上述一样(S4440)。

[0299] 以下说明在所述安全键盘上形成有图形要素而提供的本发明的第5实施例。

[0300] 图20为表示根据本发明的第5实施例的利用一次性键盘的密钥输入系统的构成的框图。

[0301] 如图所示,构成根据本发明的第5实施例的密钥输入系统的输入终端(100),包括控制部(101)、显示部(102)、操作部件(103)、标示部件(104)而构成。

[0302] 控制部(101)包括生成具有能够输入多个图形要素和密钥的拨号键输入功能的图形输入工具(105)的图形输入工具生成部而构成。本发明中多个图形要素可使用图案、颜色、图画及使用者能够识别的图形要素。并且,图形要素可只以图案形成,也可形成为颜色和图案的组合。

[0303] 图形输入工具(105)成为3维形状,并且,3维的各个面形成有相互不同的图形要素。3维形状由正六面体、直六面体等多面体形成。

[0304] 图形输入工具(105)具有除所述图形要素之外还可输入密钥的拨号键输入功能。拨号键可为以往通常使用的输入0～9的数字的拨号键，也可为能够输入1～9数字或各种特殊文字的拨号键。如图21所示，图形输入工具(105)如果形成9个数字的识别标志时构成3x3x3的排列形态的正六面体，如果形成具有9个以上的数字的识别标志时，3维形状的多面体上形成非3x3x3排列形态的4x4x4，也可形成各种形态的形状。

[0305] 图形输入工具(105)在显示部(102)上表示而使得使用者能够识别图形要素，并识别拨号键的信息。显示部(102)利用通常使用额LCD等显示装置体现，也可直接触摸显示部(102)而输入信息。

[0306] 标示部件(104)标示多个图形要素中对应于密钥的图形要素的信息。例如，密钥由4位数字形成时，标示4个对应于各个数字的图形要素，如果密钥为5位数字，标示5个对应的图形要素。此时，各个图形要素可相互不同，可一部分不同，也可全部相同。

[0307] 操作部件(103)具有为了选择对应于在标示部件(104)上标示的图形要素的信息的图形要素，而操作图形输入工具(105)的功能。操作部件(103)如同在图21所示在显示部(102)上与图形输入工具(105)一同表示，单独构成。并且，图形输入工具(105)可通过触摸直接操作。优选地，直接操作地构成时，显示部(102)使用静电式触摸屏。

[0308] 标示部件(104)可与显示部(102)一同表示，也可为了更高的安保，如图23所示，利用另外的面板体现。如上述说明，为了盗窃密钥而获得信息时，通常拍摄显示部(102)获得该信息。此时，在与显示部(102)不同的角度形成的位置上利用另外的面板体现标示部件(104)在保安方面更有利。

[0309] 图22中图示的实施例图示了能够输入具有相互不同的图案的正六面体形状的图形输入工具及1～9的数字的拨号键，标示部件(104)单独构成，操作部件(103)在显示部(102)与图形输入工具(105)一同表示。在标示部件(104)标示对应于密钥4位数字的图形要素，使用者利用操作部件(103)选择具有与所述对应的图形要素相同的图案的面，并利用在该面上表示的拨号键输入一位密钥。然后，利用操作部件(103)选择形成有与在标示部件(104)上表示的第2个图形要素相同的图案的一面，输入密钥。反复上述的过程将4位密钥全部输入才能够完全地输入密钥。

[0310] 为了更好的安全，如图24所示，可将标示部件(104)表示在另外的使用者所持有的输出终端(106)上。此时，输出终端和控制部需通过另外的通信设备(107,301)实现同步化。

[0311] 并且，对应于密钥的图形要素及/或在拨号键上表示的识别标志可一次性形式提供。此时，能够提供相比以往更高的安全性。为了以一次性形式提供图形要素及识别标志，如图25所示，构成包括一次性图形要素及识别标志提供部(210)的服务器(200)和密钥输入系统，并且，需相互同步化。并且，如图26所示，标示部件表示在另外的终端设备(300)的显示部(303)时，密钥输入系统、服务器(200)、终端设备(300)要相互同步化，同步化通过上述的方式进行。

[0312] 并且，识别标志的数字或特殊记号可随机配置，图形输入工具的3维多面体的各个面的识别标志的数字或特殊记号位于与一次性形式提供的情况不同的位置。

[0313] 并且，每当图形输入工具以一次性形式提供时，3维的多面体变换其形状，从而，即使入侵输入的动作等，将变更的多面体作为输入方法使用时，能够保障密钥的安全。

[0314] 图27表示根据本发明的第5实施的另一实施例。

[0315] 本实施例将图形输入工具(505)的识别标志表示在另外的终端设备(300)的显示部(303)。即,所述图形输入工具(505)包括删除多个图形要素和识别标志的一个以上的无意义暗码(null)键,并包括能够输入密钥的拨号键。在终端设备(300)的显示部(303)上表示的识别标志以与图形输入工具(505)相同的形态的形状表示,并能够展开各个面图示。

[0316] 并且,表示对应于密钥的图形要素的信息的标示部件(305)可在终端设备(300)上表示,也可在密钥输入系统的显示部(502)表示。即,根据实施的各种形态,普通的技术人员考虑系统的形态、系统所处位置的安全事项等各种事项而选择标示部件(305)的位置。

[0317] 为了使用另外的终端设备,可利用另外的通信设备实现与密钥输入系统的同步化。优选地,通信设备为NFC、无线局域网、,蓝牙、磁场通信等,并且,为了提供一次性形式的密钥及图形要素,要实现密钥输入系统、服务器、终端设备之间的同步化。

[0318] 利用CPU等处理器体现的控制部,生成具有多个图形要素和拨号键输入功能的图形输入工具,并将所述生成的图形输入工具表示在显示部,并表示对应于密钥的图形要素信息。然后,使用者操作图形输入工具,设定与对应于所述密钥的图形要素相同的图形输入工具的图形要素,并输入密钥。如果有多个密钥时,设定对应于各个密钥的图形要素,并反复输入密钥的过程。

[0319] 以下说明根据本发明的利用一次性键盘的密钥输入系统及方法的实施例的为残疾人的第6实施例。

[0320] 图28为表示根据本发明的利用一次性键盘的密钥输入系统的第6实施例的示例图,图29为表示构成本发明的第6实施例的利用一次性键盘的密钥输入系统的安全键盘的一例示例图,图30为表示构成根据本发明的第6实施例的利用一次性键盘的密钥输入系统的安全键盘的另一例的示例图。

[0321] 本发明的第6实施例是为了使用对象为盲人时,有助于使用者的便利性的实施例,基本的构成和操作方法与本发明的上述实施例相同。

[0322] 只是,如果是盲人,无法通过显示模块确认在所述输出终端上输出的一次性键盘,并且,无法通过通常的触摸屏形成的键盘输入部输入密钥。

[0323] 因此,根据本发明的利用一次性键盘的密钥输入系统的另一实施例中,通过语音输出模块输出所述输出终端(300)接收的一次性键盘。

[0324] 为此,所述一次性键盘可从所述输入终端(100)变换为语音信息形态传送,也可在所述输出终端(300)上变换为语音。

[0325] 并且,所述输出终端(300)可为非普通的便携式设备,而是从属于输入终端而安装的听筒(400)。

[0326] 此时,可不使用通信模块(130),而直接语音输出所述输入终端生成的一次性键盘。

[0327] 并且,所述键盘输入部由用于盲人使用的盲人用输入面板构成。

[0328] 盲人用输入面板是已经开发各种形态进行使用的技术构成,如图29所示,可使用机械性的突出销使得使用者能够识别盲字识别的构成,也可如图30所示,使用通过电性的信号输出使得使用者能够识别盲字识别的构成。

[0329] 以下说明为老弱者的利用一次性键盘的密钥输入系统及方法的第7实施例。

[0330] 图31为表示本发明的第7实施例的利用一次性键盘的密钥输入方法的流程图,图

32为表示构成本发明的第7实施例的利用一次性键盘的密钥输入系统的输入键盘的一例的示例图。

[0331] 根据本发明的利用一次性键盘的密钥输入系统及方法的第7实施例为如果使用对象为老弱者时，有助于使用者的便利性的实施例，基本的构成和操作方法与本发明的另一实施例类似。

[0332] 只是，如果是老弱者，难以与输出至所述输出终端的一次性键盘进行对比，并通过键盘输入部输入密钥，因此，根据本发明的利用一次性键盘的密钥输入系统的第7实施例，当使用者通过输出一次性键盘的输出终端(300)输入密钥时，向键盘输入部(110)输出表示输入顺序的输入键盘。

[0333] 即，根据本发明的利用一次性键盘的密钥输入方法，在输入终端(100)上生成按键输入信息(S5110)，所述一次性键盘生成部(122)生成一次性键盘(S5120)，生成的一次性键盘以SMS或MMS形态向所述输出终端(300)传送(S5130)。

[0334] 然后，接收所述一次性键盘的输出终端(300)将接收的一次性键盘输出至所述显示模块(310)(S5150)。

[0335] 并且，输出所述一次性键盘的所述输出终端(300)判断使用者是否输入密钥(S5152)，当使用者输入密钥时，利用所述密钥生成输入键盘(S5154)。

[0336] 此时，所述输入键盘是指在由无意义暗码(null)键构成的拨号键上表示使用者输入的密钥的输入位置和顺序的拨号键。

[0337] 即，如图32中图示，所述输入键盘的一例将使用者输入的密钥的位置用颜色或阴影表示，并利用一系列序号表示输入顺序。

[0338] 并且，所述输出终端(300)将生成的输入键盘向所述输入终端传送(S5156)。

[0339] 然后，控制器(320)计算时间(S160)，在设定的时间期间输出一次性键盘后，结束一次性键盘的输出(S5170)。

[0340] 并且，从所述输出终端(300)接收输入键盘的输入终端(100)将接收的输入键盘向键盘输入部输出(S5205).

[0341] 并且，输出所述输入键盘的输入终端(100)接收由使用者输入的密钥(S5210)。

[0342] 并且，当识别使用者的密钥输入后，所述输入终端(100)按生成的一次性键盘的排列解读(变换)输入的密钥(S5220)。

[0343] 然后，所述输入终端(100)判断输入的密钥是否与设定编码一致(S5230)。

[0344] 并且，输出所述输入的密钥是否与设定编码一致(S5240)。

[0345] 由此，使用者能够在输出生成的一次性键盘的终端设备上容易地输入密钥，然后，在输出至所述输入终端的输入键盘按顺序输入按键，即可消除向外部泄露密钥的担忧而输入密钥。

[0346] 以下什么根据本发明的利用一次性键盘的密钥输入系统及方法适用于移动式存储器保安的本发明的第8实施例。

[0347] 根据本发明的利用一次性键盘的移动式存储器保安系统根据一次性键盘的生成方式大致区分为三个实施例。

[0348] 根据本发明的利用一次性键盘的移动式存储器保安系统及方法的第8-1实施例为一次性键盘在输出终端生成的实施例。

[0349] 图33为表示根据本发明的利用一次性键盘的密钥输入系统的第8-1实施例的构成的框图。

[0350] 如图33所示，根据本发明的第8-1实施例的密钥输入系统包括输出终端(600)，移动式存储器(800)及输入终端(700)而构成。

[0351] 所述输出终端(600)为当所述移动式存储器(800)通过近距离无线通信连接时生成一次性键盘向使用者显示的部分，为此，所述输出终端(600)包括NFC通信部(610)，输入部(620)，输出部(630)，控制部(640)及存储部(650)而构成，通常适用移动通信终端设备。

[0352] 所述NFC通信部(610)的功能是通过近距离通信识别所述移动式存储器(800)，传送数据。

[0353] 并且，所述输入部(620)是在终端设备上形成的输入装置，由触摸屏等构成。

[0354] 并且，所述输出部(630)是输出生成的一次性键盘的部分，可适用移动通信终端设备的显示装置。

[0355] 并且，所述控制部(640)是当所述移动式存储器(800)通过近距离无线通信连接时，生成一次性键盘，并将生成的所述一次性键盘通过所述NFC通信部(610)传送给所述移动式存储器(800)的部分，为此，包括生成所述一次性键盘的一次性键盘生成部(641)而构成。

[0356] 此时，由所述一次性键盘生成部(641)生成的一次性键盘是通过随机运算法则随意地排列拨号键的排列位置的拨号键，一次性生成后消灭。

[0357] 并且，所述存储部(650)是为了将生成的一次性键盘传送至所述移动式存储器(800)暂时存储的部分。

[0358] 并且，所述移动式存储器(800)是存储已设定的密钥，当输入与在使用设备上设定的密钥一致的密钥时，被激活的移动式存储媒介，为此，所述移动式存储器(800)包括NFC模块(810)，连接模块(820)，控制模块(830)及密钥存储部(850)而构成。

[0359] 所述NFC模块(810)的功能是接收识别所述输出终端(600)的NFC通信部(610)，通过近距离无线通信方式生成的一次性键盘。

[0360] 并且，所述连接模块(820)是连接于电脑的USB端子，其功能是将在移动式存储器(800)上存储的密钥及从所述输出终端(600)传送的一次性键盘传送至输入终端(700)。

[0361] 并且，所述密钥存储部(850)是存储已设定的密钥的部分，所述密钥是用于解除所述移动式存储器(800)的保安的密码，使用者在设置应用程序的PC上设定。

[0362] 并且，所述控制模块(830)是控制所述移动式存储器(800)的驱动的部分，当所述移动式存储器(800)与所述输出终端(600)通过近距离无线通信方式连接时，从所述输出终端(600)接收一次性键盘，并且，当所述移动式存储器(800)与所述输入终端(700)通过连接接口时，控制所述移动式存储器(800)以使通过所述连接模块(820)传送所述密钥及接收的一次性键盘。

[0363] 并且，所述输入终端(700)当连接所述移动式存储器(800)时，接收从所述移动式存储器(800)传送的所述密钥及一次性键盘，并接收使用者输入的密钥，判断从所述移动式存储器(800)传送的密钥是否与由使用者输入的密钥一致，由此，设定是否解除在所述移动式存储器(800)上设定的保安。

[0364] 为此，所述输入终端(700)包括连接接口(710)，控制器(740)，输入模块(720)及输

出模块(730)而构成。

[0365] 所述连接接口(710)是通过所述连接模块(820)使得所述移动式存储器(800)连接的部分,可适用通常的USB连接接口。

[0366] 并且,所述输入模块(720)是接收由使用者输入的密钥的部分,可适用触摸屏或鼠标等人机界面。

[0367] 并且,所述输出模块(730)是输出所述一次性键盘的部分,可适用通常的显示装置。

[0368] 并且,所述控制器(740)将从所述输出终端(600)生成并通过所述移动式存储器(800)接收的一次性键盘输出至所述输出模块(730)。

[0369] 此时,所述控制器(740)生成输出在生成的一次性键盘上未表示识别标志地构成的安全键盘。

[0370] 由此,所述输出终端(600)将生成的一次性键盘以表示识别标志的状态输出,所述输入终端(700)输出生成的一次性键盘上识别标志被删除的安全键盘。

[0371] 并且,所述控制器(740)接收输出的安全键盘上由使用者输入密钥,并判断从所述移动式存储器(800)传送的密钥是否与使用者输入的密钥一致,设定是否解除在所述移动式存储器(800)上设定的保安。

[0372] 以下详细说明根据本发明的密钥输入方法的第8-1实施例。

[0373] 图34为表示根据本发明的第8-1实施例的移动式存储器保安方法的流程图,图35为表示根据本发明的利用一次性键盘的移动式存储器保安系统的动作例的示例图。

[0374] 根据本发明的第8-1实施例的移动式存储器保安方法的详细的实施例,如图34所示,从所述输出终端(600)识别移动式存储器(800)连接于输出终端(600)开始(S6110)。

[0375] 即,所述移动式存储器(800)通过近距离无线通信连接于所述输出终端(600)时,所述输出终端(600)生成一次性键盘(OTK)(S6140)。

[0376] 此时,所述一次性键盘已进行说明,因此省略详细的说明。

[0377] 然后,所述输出终端(600)将所述生成的一次性键盘传送至所述移动式存储器(S6150),并且,如图35所示,通过所述输出部(630)输出所述一次性键盘(S6160)。

[0378] 然后,所述移动式存储器(800)将接收的一次性键盘向输入终端(700)传送(S6170),与此同时,将在密钥存储部(850)上存储的密钥传送至所述输入终端(700)(S6180)。

[0379] 并且,所述移动式存储器(800)通过连接接口与所述输入终端(700)连接时,所述输入终端(700)从所述移动式存储器(800)接收所述一次性键盘及密钥(S6210,S6220)。

[0380] 然后,所述输入终端(700)从接收的一次性键盘生成安全键盘,并通过输出模块(730)输出(S6230)。

[0381] 此时,如图35所示,所述安全键盘是指与所述一次性键盘的排列相同地构成,但删除识别标志的形态的拨号键。

[0382] 并且,使用者通过输入模块(720)在所述安全键盘上输入密钥后,所述控制器(740)判断从所述移动式存储器(800)传送的密钥是否与使用者输入的密钥一致(S6510,S6520)。

[0383] 然后,从所述移动式存储器(800)传送的密钥与使用者输入的密钥一致时,解除在

移动式存储器(800)上设定的保安,而使得能够进行数据的移动及记录(S6530)。

[0384] 相反,从所述移动式存储器(800)传送的密钥与使用者输入的密钥不一致时,维持所述移动式存储器(800)的保安设定状态,并输出密钥输入发生错误的错误信息(S6540)。

[0385] 在此,各个执行步骤的时间序列执行顺序是为了便于说明而示例性地区分,因此,在不妨碍单位功能的执行的范围内可进行更改。

[0386] 例如,从移动式存储器(800)至输入终端(700)的密钥传送,在判断是否与使用者输入的密钥一致之前的全部时间进行也无妨。

[0387] 然后,根据本发明的利用一次性键盘的移动式存储器保安系统及方法的第8-2实施例为在输入终端生成一次性键盘的实施例。

[0388] 图36为表示根据本发明的利用一次性键盘的移动式存储器保安系统的第8-2实施例的构成的框图,图37为表示根据本发明的利用一次性键盘的移动式存储器保安方法的第8-2实施例的流程图。

[0389] 如图36所示,根据本发明的第8-2实施例的移动式存储器保安系统包括输出终端(600),移动式存储器(800)及输入终端(700)而构成。

[0390] 所述输出终端(600)当所述移动式存储器(800)通过近距离无线通信连接时,接收所述移动式存储器(800)传送的一次性键盘并输出的部分,为此,所述输出终端(600)包括NFC通信部(610)、输出部(630)及控制部(640)而构成,可适用通常的移动通信终端设备。

[0391] 所述NFC通信部(610)通过近距离通信连接于所述移动式存储器(800),并从所述移动式存储器(800)接收一次性键盘。

[0392] 并且,所述移动式存储器(800)是存储已设定的密钥,并且输入的密码与在使用设备上设定的密钥一致时,被激活的移动式存储媒介,为此,所述移动式存储器(800)包括NFC模块(810),连接模块(820),控制模块(830)及密钥存储部(850)而构成。

[0393] 所述NFC模块(810)的功能是识别所述输出终端(600)的NFC通信部(610),传送通过近距离无线通信方式生成的一次性键盘。

[0394] 并且,所述连接模块(820)是连接于电脑,所述密钥存储部(850)是存储已设定的密钥的部分。

[0395] 并且,所述控制模块(830)是控制所述移动式存储器(800)的驱动的部分,当所述移动式存储器(800)通过连接接口连接于所述输入终端(700)时,向所述输入终端(700)提供所述密钥,并从所述输入终端(700)接收一次性键盘,并且,当所述移动式存储器(800)通过近距离无线通信连接于所述输出终端(600)时,控制所述移动式存储器(800)将所述接收的一次性键盘向所述输出终端(600)传送。

[0396] 并且,所述输入终端(700)当与所述移动式存储器(800)连接时,从所述移动式存储器(800)接收所述密钥,并生成一次性键盘传送给所述移动式存储器(800),并接收由使用者输入的密钥,判断从所述移动式存储器(800)传送的密钥是否与使用者输入的密钥一致,而设定是否解除在所述移动式存储器(800)上设定的保安。

[0397] 为此,所述输入终端(700)包括连接接口(710),控制器(740),输入模块(720)及输出模块(730)而构成。

[0398] 此时,所述控制器(740)包括一次性键盘生成模块(741)而构成,通过所述一次性键盘生成模块(741)生成一次性键盘。

[0399] 如上述地，所述一次性键盘是拨号键的排列位置通过随机运算法则随意地排列的拨号键，一次性生成后消灭。

[0400] 并且，所述控制器(740)由所述一次性键盘生成安全键盘，通过所述输出模块(730)输出。

[0401] 并且，所述控制器(740)接收在输出的安全键盘上由使用者输入的密钥，并判断从所述移动式存储器(800)传送的密钥是否与使用者输入的密钥一致，而设定是否解除所述移动式存储器(800)上设定的保安。

[0402] 并且，如图37所示，根据本发明的第8-2实施例的移动式存储器保安方法，从所述输入终端(600)识别移动式存储器(800)连接于输入终端(600)开始(S7330)。

[0403] 然后，所述移动式存储器(800)通过连接接口连接于所述输入终端(700)时，所述输入终端(700)从所述移动式存储器(800)接收密钥(S7340,S7350)。

[0404] 然后，所述输入终端(700)生成一次性键盘(OTK)，将所述一次性键盘传送给所述移动式存储器(800)(S7360)。

[0405] 此时，所述一次性键盘已在上述中说明，因此，省略对其的说明。

[0406] 并且，所述输入终端(700)从生成的一次性键盘生成安全键盘，并通过输出模块(730)输出(S7370,S7380)。

[0407] 此时，所述安全键盘是指与所述一次性键盘的排列相同地构成，但删除识别标志的形态的拨号键。

[0408] 并且，使用者通过输入模块(720)在所述安全键盘上输入密钥时，所述控制器(740)判断从所述移动式存储器(800)传送的密钥是否与使用者输入的密钥一致(S7510,S7520)。

[0409] 然后，从所述移动式存储器(800)传送的密钥与使用者输入的密钥一致时，解除再移动式存储器(800)上设定的保安，使得能够进行数据的移动及记录(S7530)。

[0410] 相反，从所述移动式存储器(800)传送的密钥与使用者输入的密钥不一致时，维持所述移动式存储器(800)的保安设定状态，并输出密钥输入发生错误的错误信息(S7540)。

[0411] 并且，接收所述一次性键盘的移动式存储器(800)将所述一次性键盘向所述输出终端(600)传送。

[0412] 并且，接收所述一次性键盘的所述输出终端(600)将所述接收的一次性键盘通过所述输出部(630)输出(S7410,S7420,S7430)。

[0413] 在此，从所述移动式存储器(800)至输入终端(700)的密钥传送，在判断是否与使用者输入的密钥一致之前的全部时间进行也无妨。

[0414] 根据本发明的利用一次性键盘的移动式存储器保安系统及方法的第8-3实施例是一次性键盘通过时间同步化方式从输出终端及输入终端生成的实施例。

[0415] 根据本发明的利用一次性键盘的移动式存储器保安系统的第8-3实施例，如图38所示，是将一次性键盘的输出终端(600)和输入终端(700)二元化而加强安全性的实施例，以下进行详细的说明。

[0416] 图38为表示本发明的第8-3实施例的利用一次性键盘的移动式存储器保安系统的构成的框图，图39为表示本发明的第8-3实施例的利用一次性键盘的移动式存储器保安方法的流程图。

[0417] 首先，如图38所示，本发明的第8-3实施例的利用一次性键盘的移动式存储器保安系统包括输出终端(600)，移动式存储器(800)及输入终端(700)而构成。

[0418] 所述输出终端(600)是接收从所述移动式存储器(800)传送的固有密钥，生成一次性键盘向使用者显示的部分，为此，所述输出终端(600)包括NFC通信部(610)，输入部(620)，输出部(630)，控制部(640)及存储部(650)而构成，通常可适用移动通信终端设备。

[0419] 所述NFC通信部(610)的功能是通过近距离通信从所述移动式存储器(800)接收固有密钥。

[0420] 并且，所述输入部(620)是形成于终端设备的输入装置，并非执行根据本发明的功能的必需构成要素。

[0421] 并且，所述输出部(630)是输出生成的一次性键盘的部分，可适用移动通信终端设备的显示装置。

[0422] 并且，所述控制部(640)是利用从所述移动式存储器(800)传送的固有密钥而生成一次性键盘的部分，为此，包括生成所述一次性键盘的一次性键盘生成部(641)而构成。

[0423] 此时，所述一次性键盘生成部(641)通过时间同步化方式生成一次性键盘。

[0424] 并且，所述存储部(650)是在生成一次性键盘的期间存储从所述移动式存储器(800)接收的固有密钥的部分，可适用移动通信终端设备的高速缓冲存储器等。

[0425] 并且，所述移动式存储器(800)存储已设定的密钥，而输入与在使用设备上设定的密钥一致的密钥时被激活的移动式存储媒介，为此，所述移动式存储器(800)包括NFC模块(810)，连接模块(820)，控制模块(830)，固有密钥存储部(840)及密钥存储部(850)而构成。

[0426] 所述NFC模块(810)是识别所述输出终端(600)的NFC通信部(610)，使得能够通过近距离无线通信方式进行数据传送的部分。

[0427] 并且，所述连接模块(820)是连接于电脑的USB端子，收发移动式存储器(800)与电脑之间的数据。

[0428] 并且，所述密钥存储部(850)是存储已设定的密钥的部分，所述固有密钥存储部(840)是存储固有密钥的部分，所述固有密钥是按所述移动式存储器(800)固有地设定的值，可由序列号等构成，所述固有密钥用于向所述输出终端(600)和后述的输入终端(700)传送，通过时间同步化方式生成一次性键盘。

[0429] 并且，所述控制模块(830)是控制所述移动式存储器(800)的驱动的部分，当所述移动式存储器(800)通过近距离无线通信方式连接于所述输出终端(600)时，向所述输出终端(600)传送所述固有密钥，所述移动式存储器(800)连接于所述输入终端(700)时，通过所述连接模块(820)传送所述密钥及固有密钥。

[0430] 并且，所述输入终端(700)连接于所述移动式存储器(800)时，生成一次性键盘，接收通过所述一次性键盘由使用者输入的密钥，并接收从所述移动式存储器(800)传送的密钥，判断是否与从使用者输入的密钥一致，而稍等是否解除在所述移动式终端设备上设定的保安。

[0431] 为此，所述输入终端(700)包括连接接口(710)，控制器(740)，输入模块(720)及输出模块(730)而构成。

[0432] 所述连接接口(710)是通过所述连接模块(820)与所述移动式存储器(800)连接的部分，适用通常的USB连接接口。

[0433] 并且,所述输入模块(720)是接收从使用者输入的密钥的部分,可适用触摸屏或鼠标等的人机界面。

[0434] 并且,所述输出模块(730)是输出所述一次性键盘的部分,可适用通常的显示装置。

[0435] 并且,所述控制器(740)包括一次性键盘生成模块(741)而构成,生成所述一次性键盘,从生成的一次性键盘生成安全键盘,并通过所述输出模块(730)输出,并且,将从所述移动式存储器(800)传送的密钥与通过所述输入模块(720)输入的密钥进行对比,两个密钥一致时解除在所述移动式存储器(800)上设定的保安。

[0436] 以下详细说明从所述一次性键盘生成部(641)及一次性键盘生成模块(741)生成的一次性键盘的生成方法。

[0437] 并且,所述一次性键盘为一次性地生成被消灭,使得拨号键的排列位置随机地(在此所谓随机是通过运算法则随机地生成)生成,详细的生成方法在本发明的第3实施例中详细说明,因此省却。

[0438] 以下详细说明根据本发明的第8-3实施例的利用一次性键盘的移动式存储器保安方法。

[0439] 根据本发明的第8-3实施例的利用一次性键盘的移动式存储器保安方法,如图39所示,从识别移动式存储器(800)连接于输入终端(700)或输出终端(600)开始。

[0440] 首先,说明所述移动式存储器(800)通过近距离无线通信与输出终端(600)连接的情况,所述移动式存储器(800)连接于所述输出终端(600)时(S8200),所述移动式存储器(800)将固有密钥传送给所述输出终端(600)(S8340)。

[0441] 并且,所述输出终端(600)接收所述固有密钥时,利用所述接收的固有密钥通过时间同步化方式生成一次性键盘(OTK)(S8360)。

[0442] 此时,所述一次性键盘的生成方法已进行说明,因此,省却详细的说明。

[0443] 然后,所述输出终端(600)通过输出部(630)输出所述生成的一次性键盘(S8380)。

[0444] 然后,说明所述移动式存储器(800)连接于输入终端(700)的情况,所述移动式存储器(800)通过连接接口连接于所述输入终端(700)时(S8100),所述移动式存储器(800)将固有密钥向所述输入终端(700)传送,使得所述输入终端(700)接收所述固有密钥(S8300,S8320)。

[0445] 并且,所述移动式存储器(800)向所述输入终端(700)传送密钥,使得所述输入终端(700)接收所述密钥(S8400,S8420)。

[0446] 并且,所述输入终端(700)从所述移动式存储器(800)通过连接接口接收固有密钥及密钥时,所述输入终端(700)的一次性键盘生成模块通过接收的所述固有密钥通过时间同步化方式生成一次性键盘(S8500)。

[0447] 在此,所述一次性键盘如上述。

[0448] 然后,所述输入终端(700)从生成的所述一次性键盘生成删除识别标志的形态的安全键盘,通过输出模块(730)输出(S8600)。

[0449] 然后,使用者通过输入模块(720)在所述安全键盘上输入密钥时,所述控制器(740)判断从所述移动式存储器(800)传送的密钥是否与使用者输入的密钥一致(S8700,S8800)。

[0450] 并且，从所述移动式存储器(800)传送的密钥与使用者输入的密钥一致时，解除在移动式存储器(800)上设定的保安，使得能够进行数据的移动及记录(S8920)。

[0451] 相反，从所述移动式存储器(800)传送的密钥与使用者输入的密钥不一致时，维持所述移动式存储器(800)的保安设定状态，并输出密钥输入发生错误的错误信息(S8940)。

[0452] 在此，各个执行步骤的时间序列执行顺序是为了便于说明示例性地区分，在不妨碍单位功能的执行的范围内可进行变更。

[0453] 例如，所述移动式存储器(800)的输出终端(600)或输入终端(700)的连接顺序可互换，也可同时进行。即，只要在时间同步化区分单位时间内实现互相连接，即可生成相同的一次性键盘，因此，时间的顺序可变更。

[0454] 并且，从移动式存储器(800)至输入终端(700)的密钥传送，在判断是否与由使用者输入的密钥一致之前的全部时间内进行也无妨。

[0455] 根据如上所述的本发明的另一实施例，使得一次性键盘的输出位置(终端设备)和密钥输入位置二元化，从而，即使输入终端被入侵或密钥输入状态暴露给他人，也能够防止泄露输入的号码，由此，能够显著提高设定的密钥的安全性。

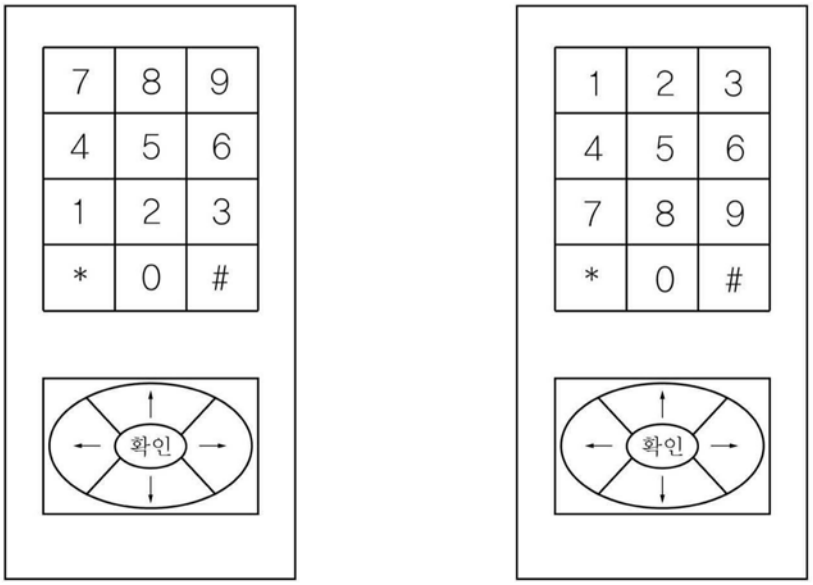

7 8 9
4 5 6
1 2 3
* 0 #
확인
1 2 3
4 5 6
7 8 9
* 0 #
확인

图1

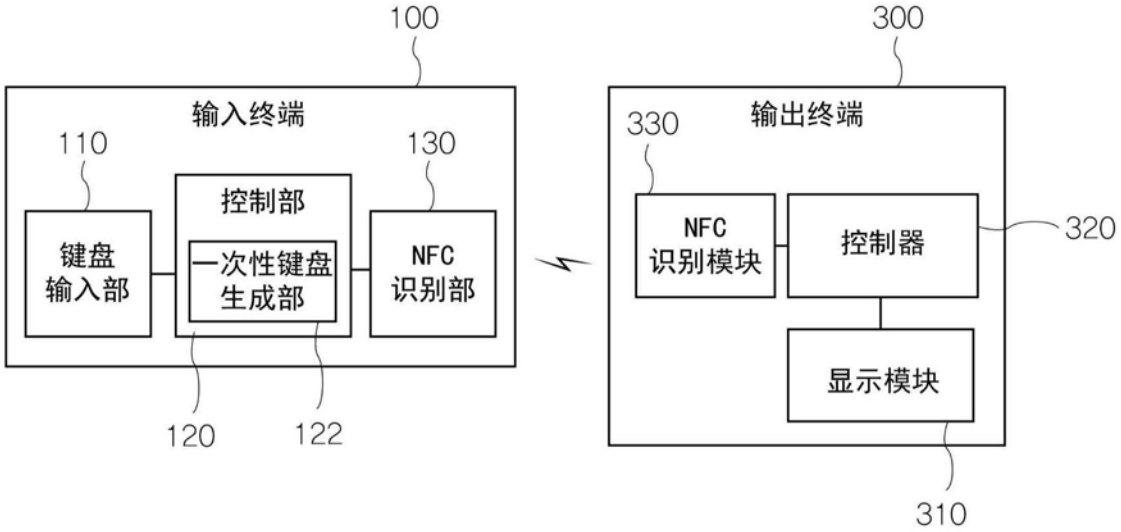

100
输入终端
110
键盘
输入部
控制部
一次性键盘
生成部
130
NFC
识别部
120
122
300
输出终端
330
NFC
识别模块
控制器
320
显示模块
310

图2

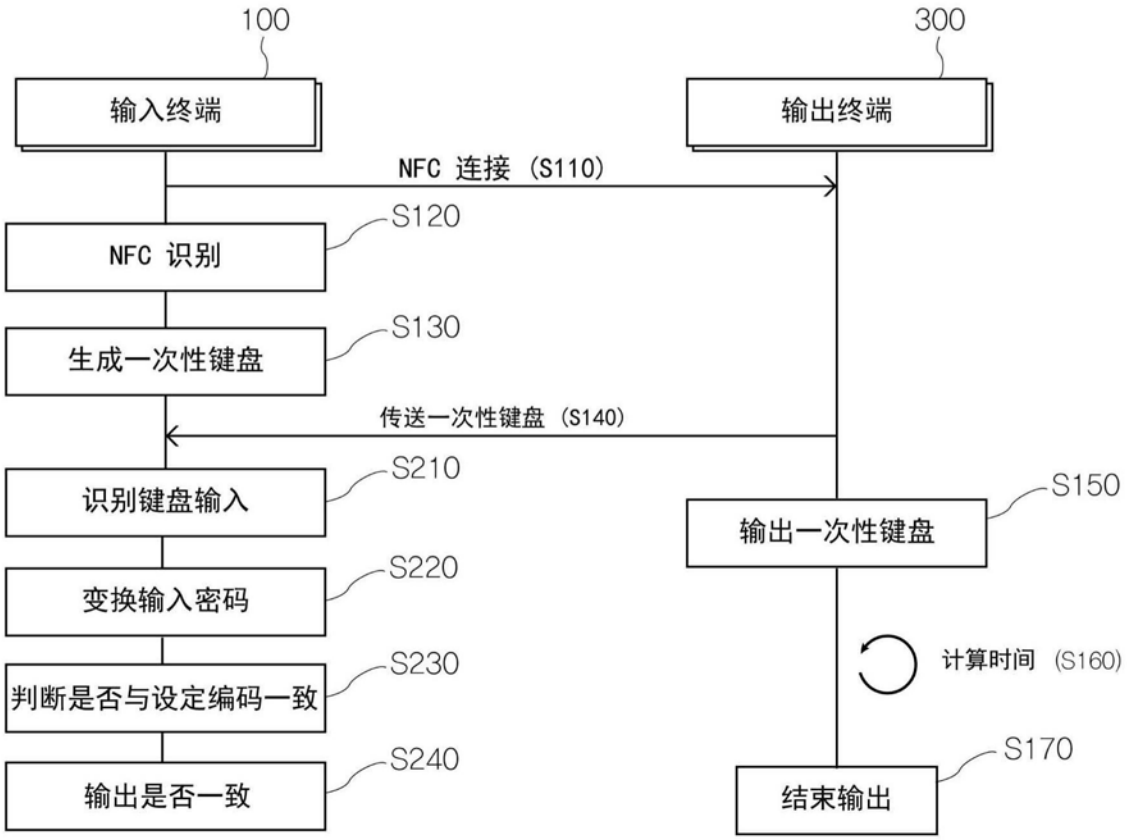

100
300
输入终端
输出终端
NFC 连接 (S110)
S120
NFC 识别
S130
生成一次性键盘
传送一次性键盘 (S140)
S210
识别键盘输入
S150
输出一次性键盘
S220
变换输入密码
计算时间 (S160)
S230
判断是否与设定编码一致
S240
输出是否一致
S170
结束输出

图3

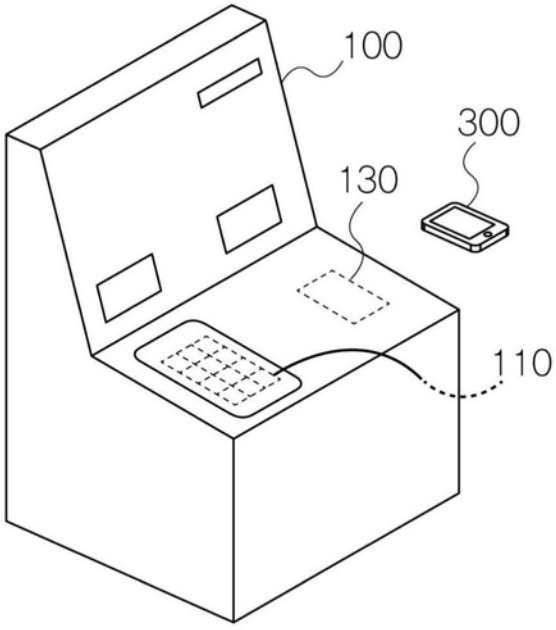

100
300
130
110

图4

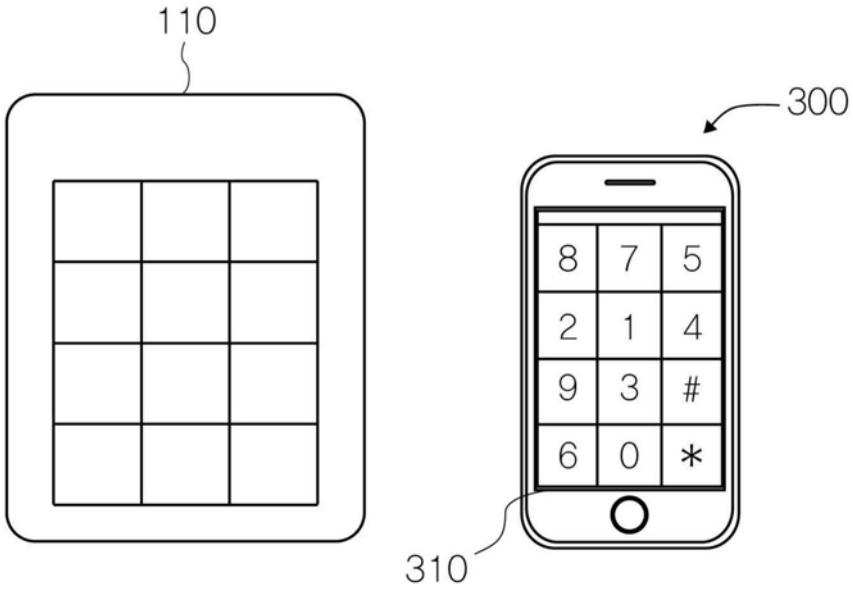

110
300
8 7 5
2 1 4
9 3 #
6 0 *
310

图5

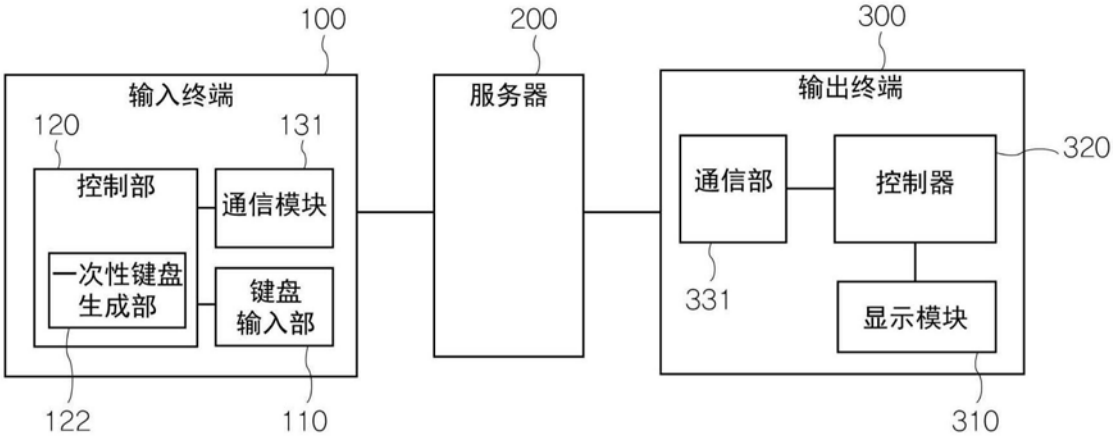

100
200
300
输入终端
120
131
控制部
通信模块
一次性键盘
生成部
键盘
输入部
122
110
服务器
输出终端
通信部
控制器
320
331
显示模块
310

图6

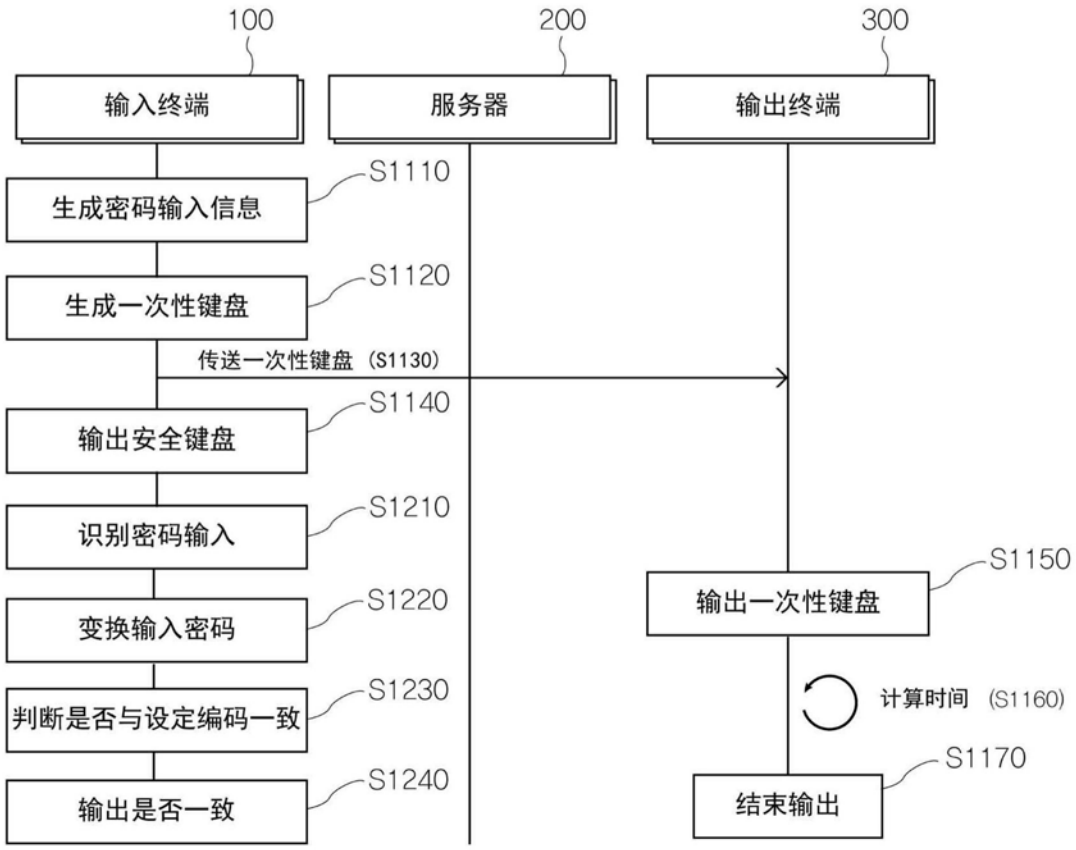

100
200
300
输入终端
服务器
输出终端
S1110
生成密码输入信息
S1120
生成一次性键盘
传送一次性键盘 (S1130)
S1140
输出安全键盘
S1210
识别密码输入
S1220
变换输入密码
S1230
判断是否与设定编码一致
S1240
输出是否一致
S1150
输出一次性键盘
计算时间 (S1160)
S1170
结束输出

图7

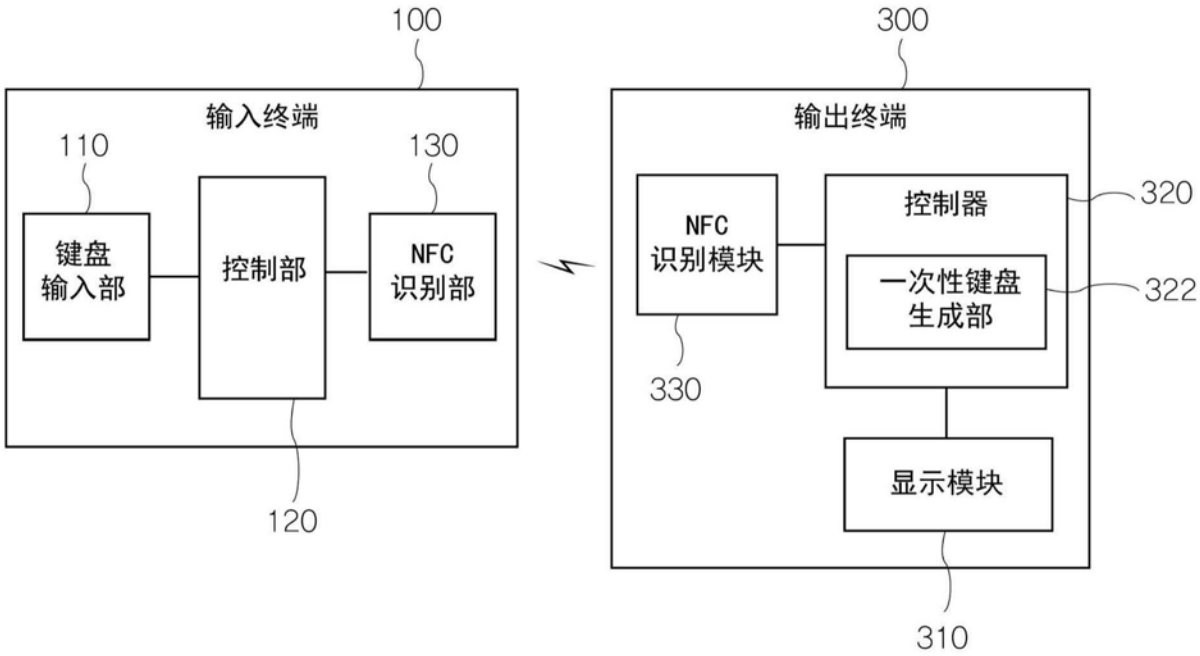

100
300
输入终端
输出终端
110
130
键盘
输入部
控制部
NFC
识别部
120
NFC
识别模块
330
控制器
320
一次性键盘
生成部
322
显示模块
310

图8

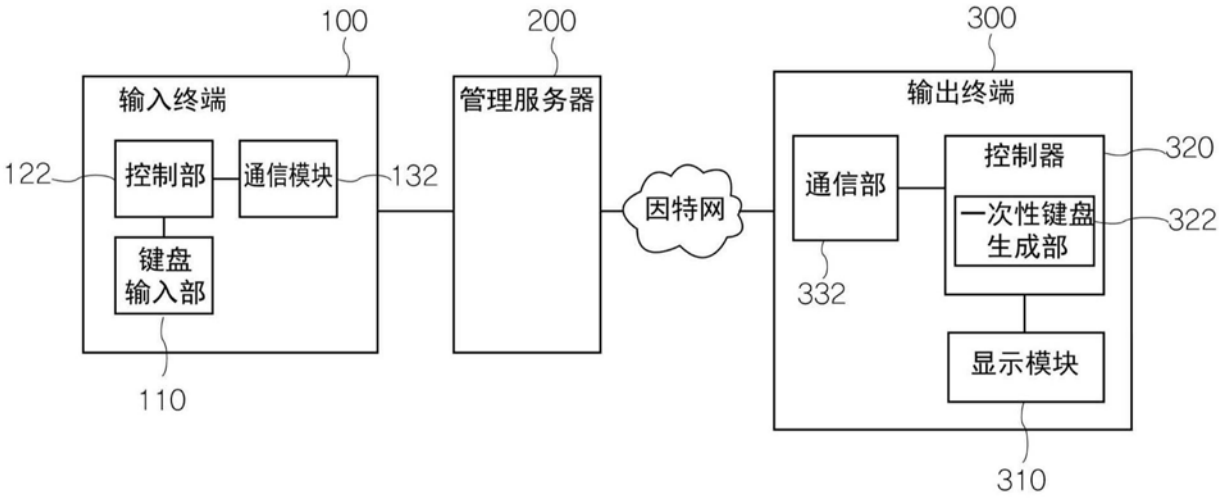

100
200
300
输入终端
管理服务器
输出终端
122
控制部
通信模块
132
因特网
通信部
控制器
320
一次性键盘
生成部
322
键盘
输入部
332
显示模块
110
310

图9

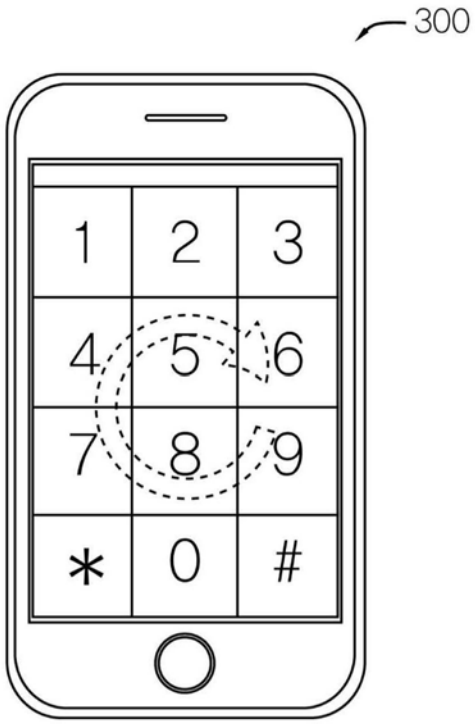

300
1
2
3
4
5
6
7
8
9
*
0
#

图10

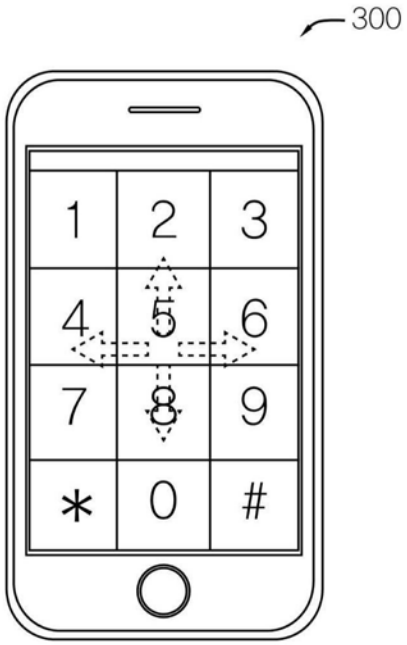


图11

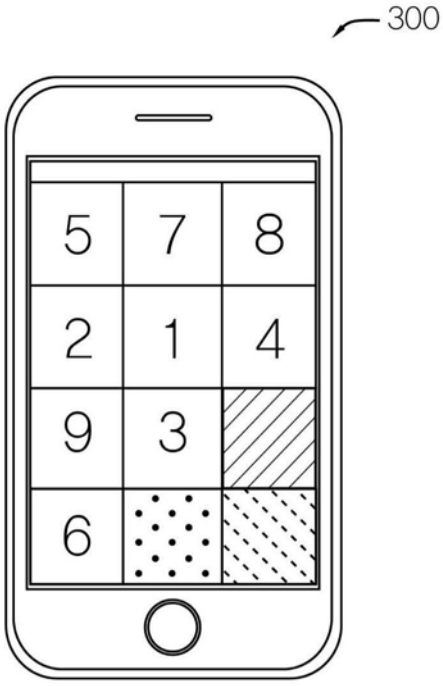


图12

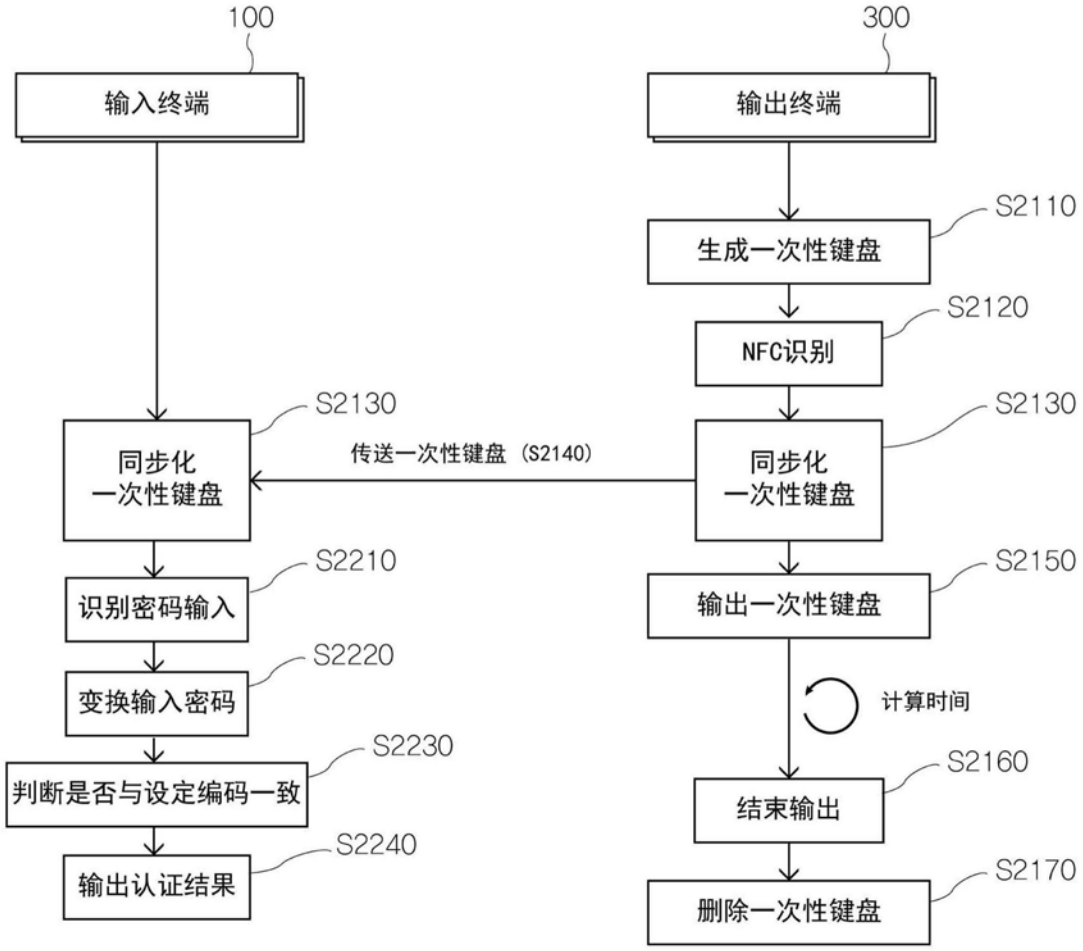

100
输入终端
300
输出终端
S2110
生成一次性键盘
S2120
NFC识别
S2130
同步化
一次性键盘
传送一次性键盘（S2140）
S2130
同步化
一次性键盘
S2210
识别密码输入
S2150
输出一次性键盘
S2220
变换输入密码
计算时间
S2230
判断是否与设定编码一致
S2160
结束输出
S2240
输出认证结果
S2170
删除一次性键盘

图13

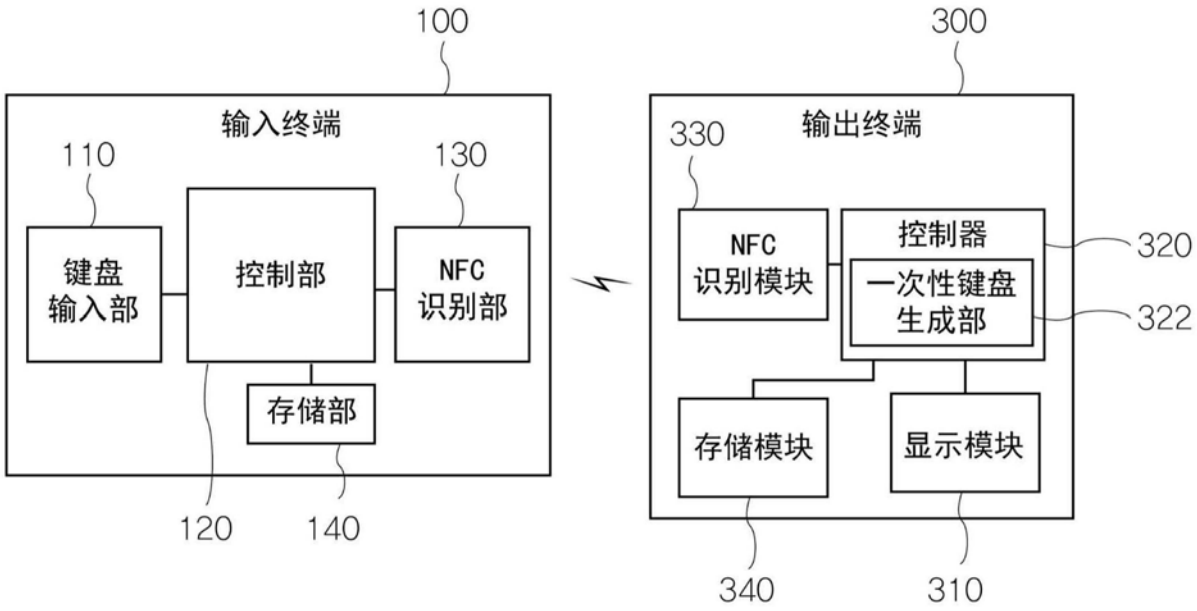

100
输入终端
110
键盘
输入部
控制部
130
NFC
识别部
存储部
120
140
300
输出终端
330
NFC
识别模块
控制器
320
一次性键盘
生成部
322
存储模块
显示模块
340
310

图14

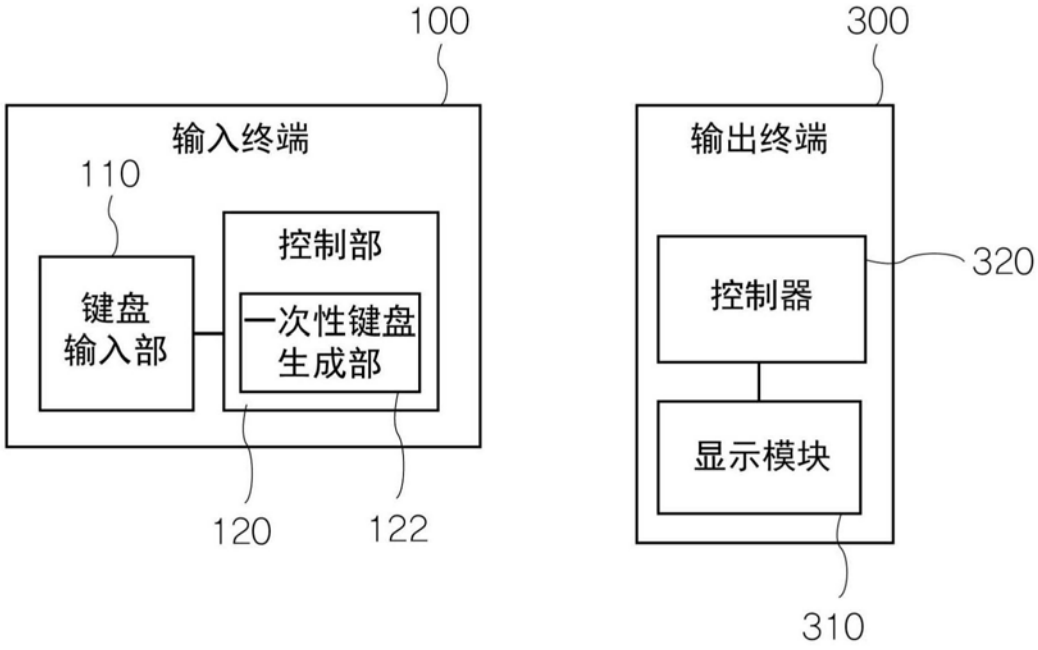


图15

排列按键：8757214493B560BA81

OTK

8	7	5
2	1	4
9	3	A(#)
6	0	B(*)

图16

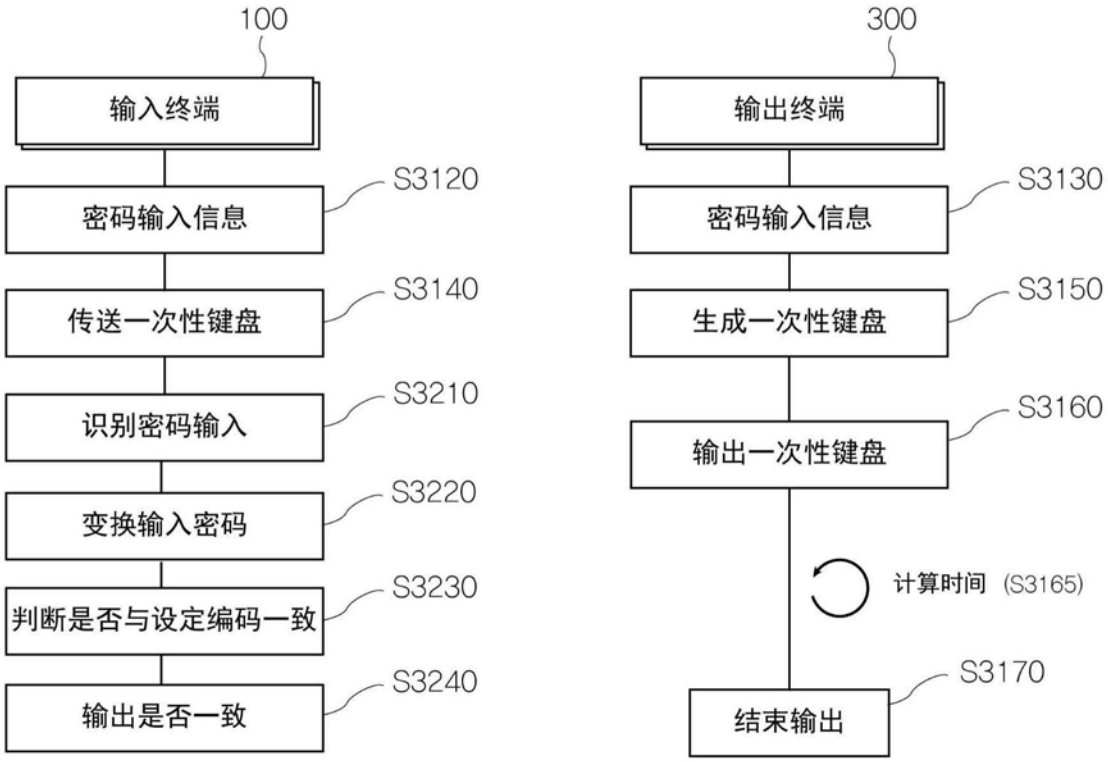

100
输入终端
S3120
密码输入信息
S3140
传送一次性键盘
S3210
识别密码输入
S3220
变换输入密码
S3230
判断是否与设定编码一致
S3240
输出是否一致
300
输出终端
S3130
密码输入信息
S3150
生成一次性键盘
S3160
输出一次性键盘
计算时间 (S3165)
S3170
结束输出

图17

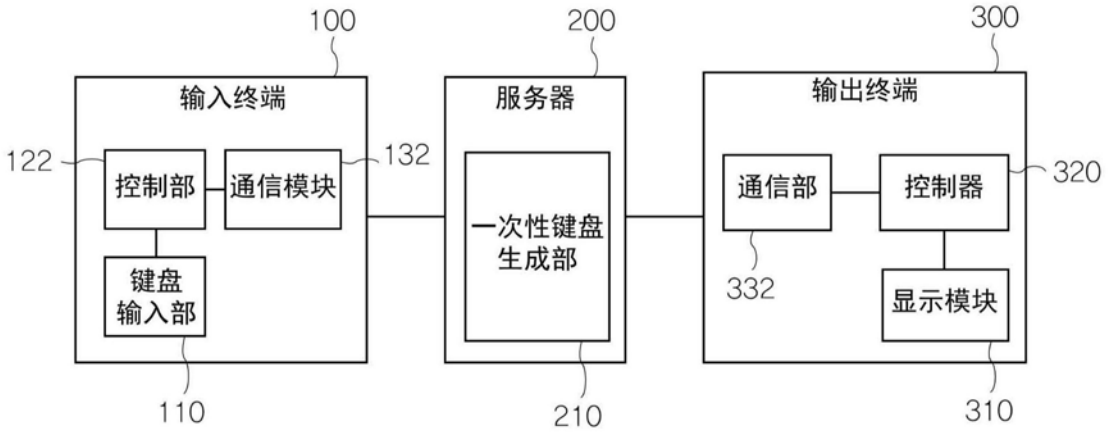

100
输入终端
122
控制部
通信模块
132
键盘
输入部
110
200
服务器
一次性键盘
生成部
210
300
输出终端
通信部
332
控制器
320
显示模块
310

图18

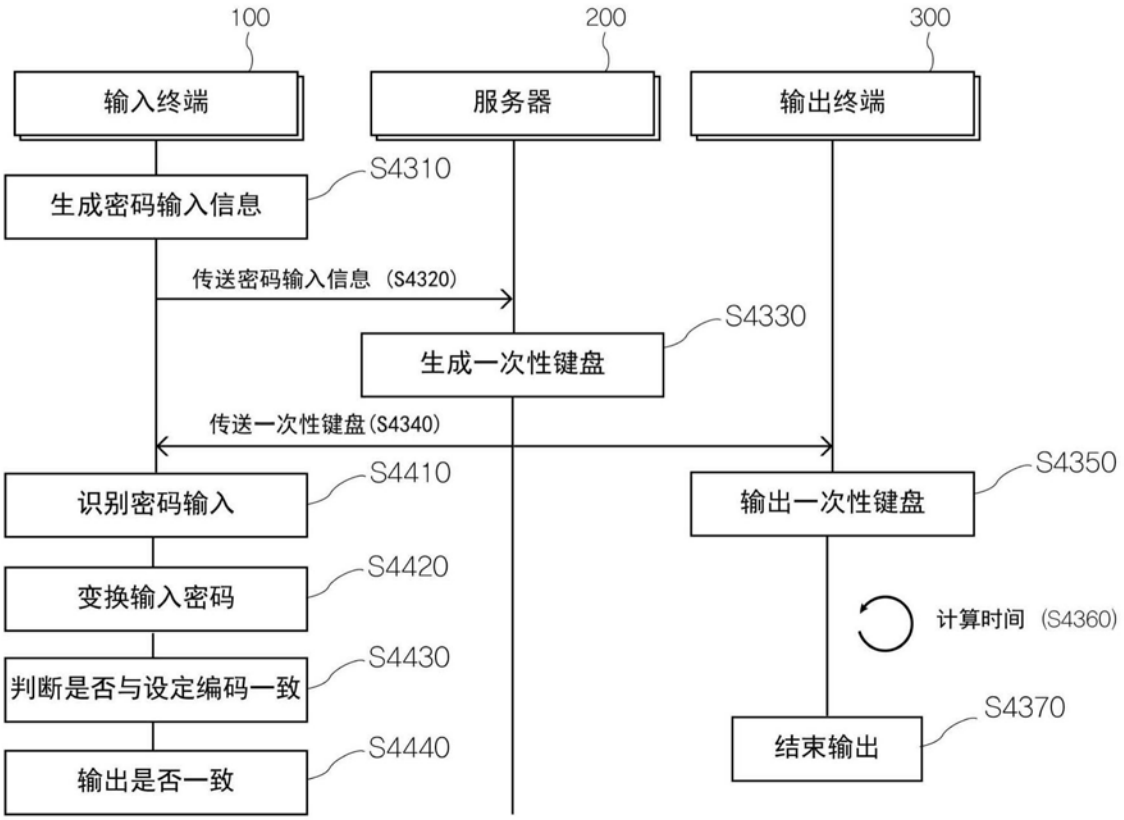

100
200
300
输入终端
服务器
输出终端
S4310
生成密码输入信息
传送密码输入信息 (S4320)
S4330
生成一次性键盘
传送一次性键盘(S4340)
S4410
识别密码输入
S4350
输出一次性键盘
S4420
变换输入密码
计算时间 (S4360)
S4430
判断是否与设定编码一致
S4370
结束输出
S4440
输出是否一致

图19

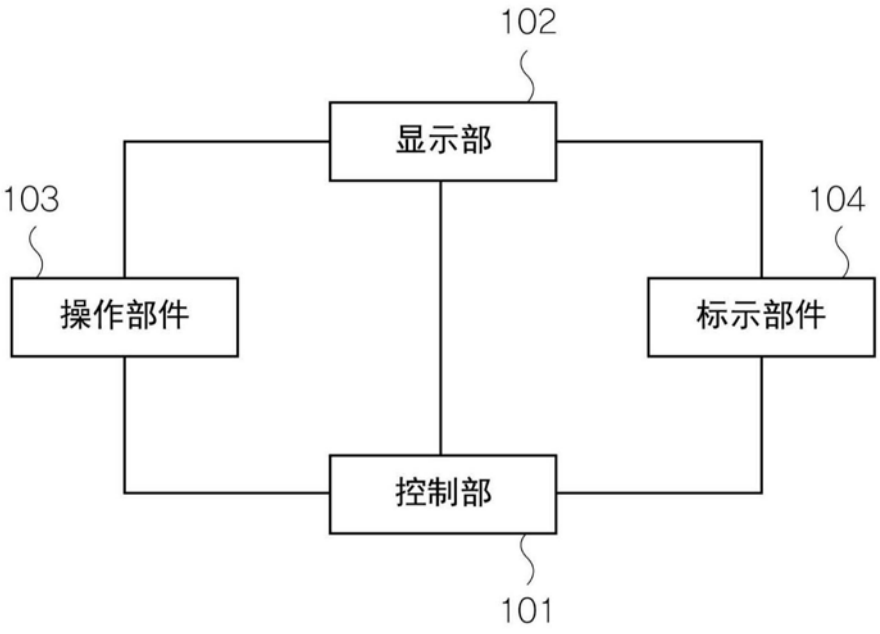

102
显示部
103
104
操作部件
标示部件
控制部
101

图20

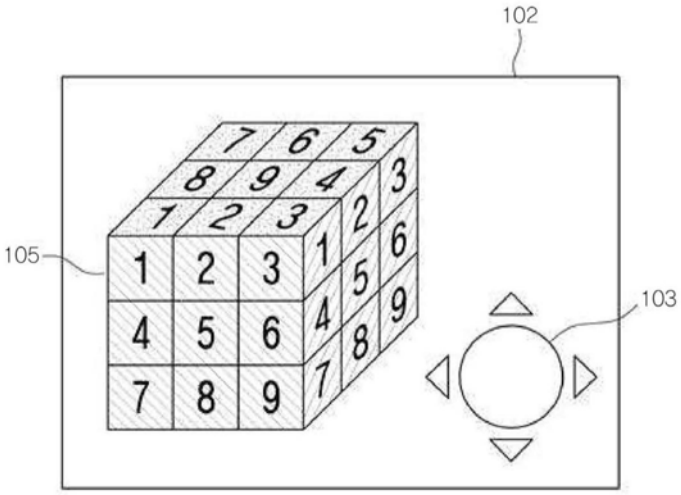


图21

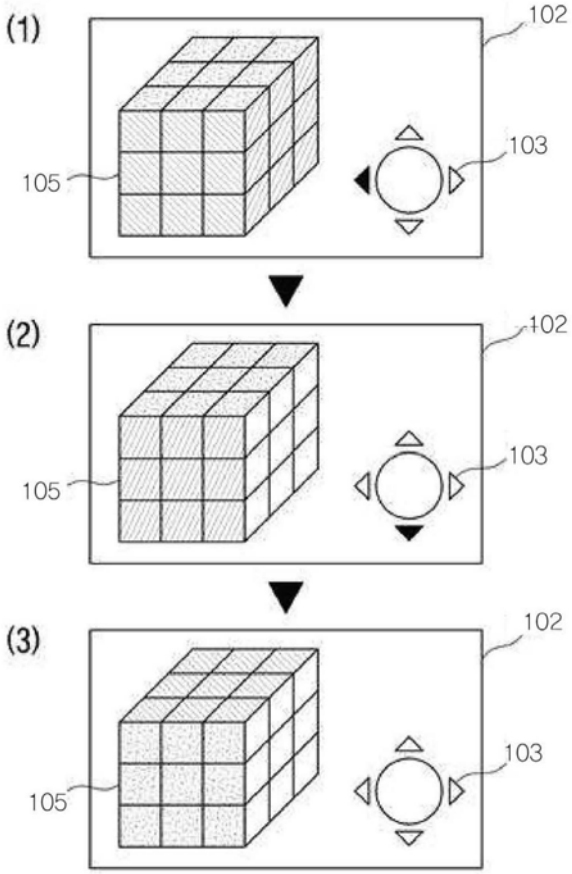


图22

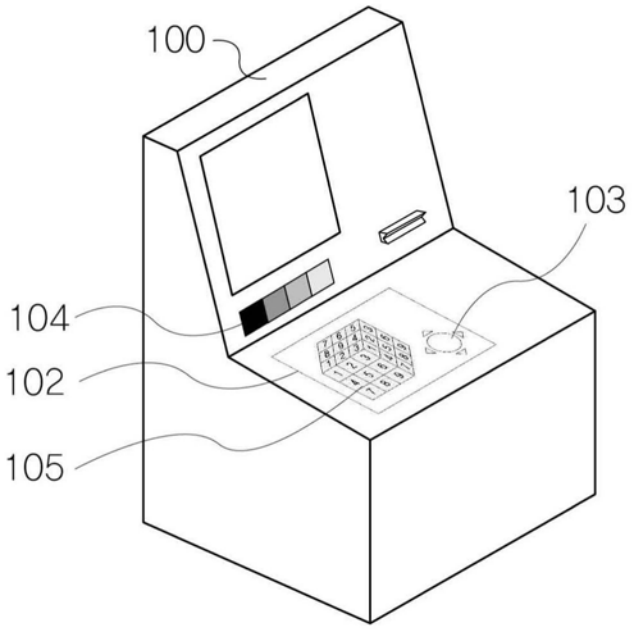


图23

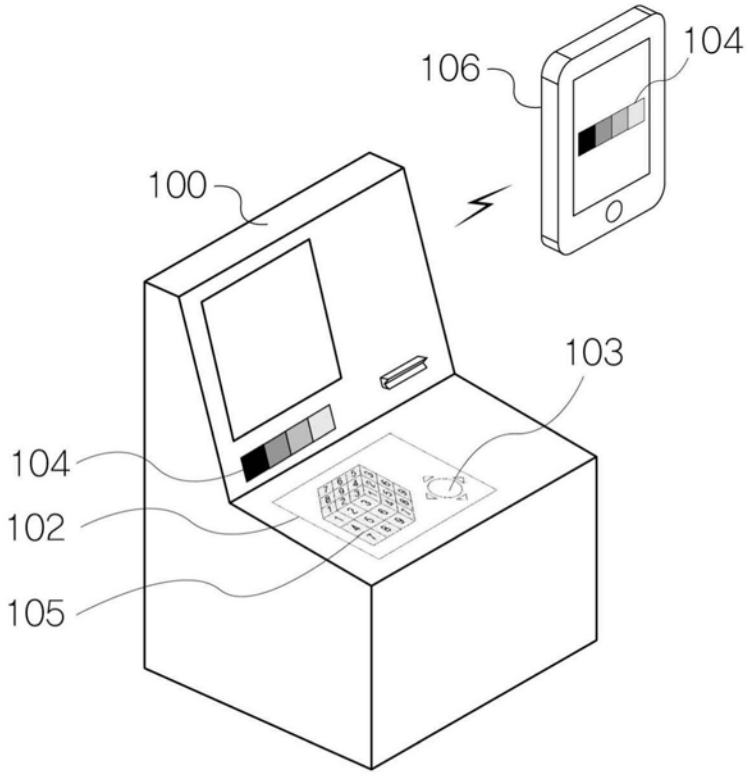


图24

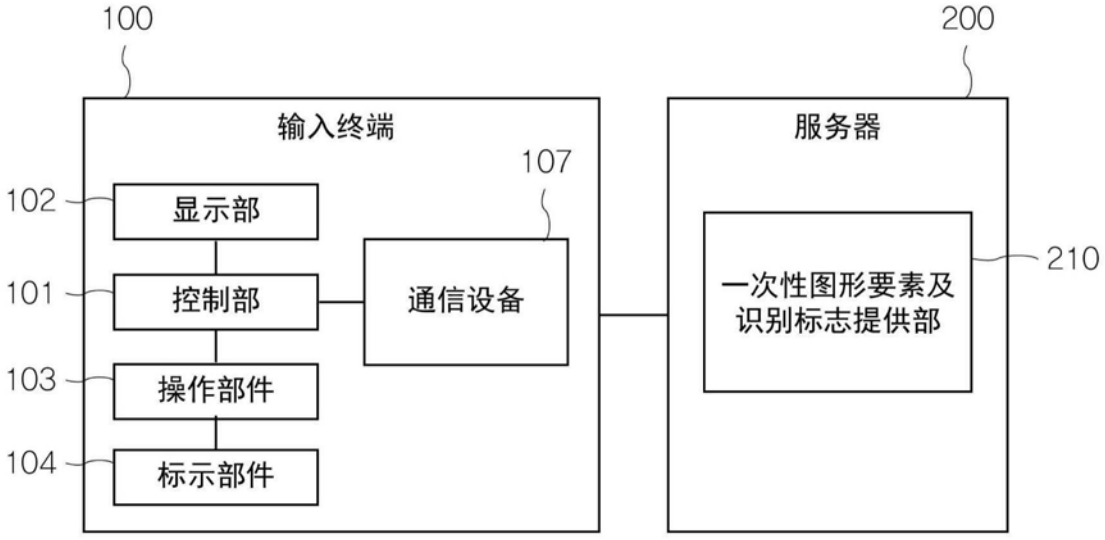

100
200
输入终端
服务器
107
102
显示部
101
控制部
通信设备
103
操作部件
104
标示部件
一次性图形要素及
识别标志提供部
210

图25

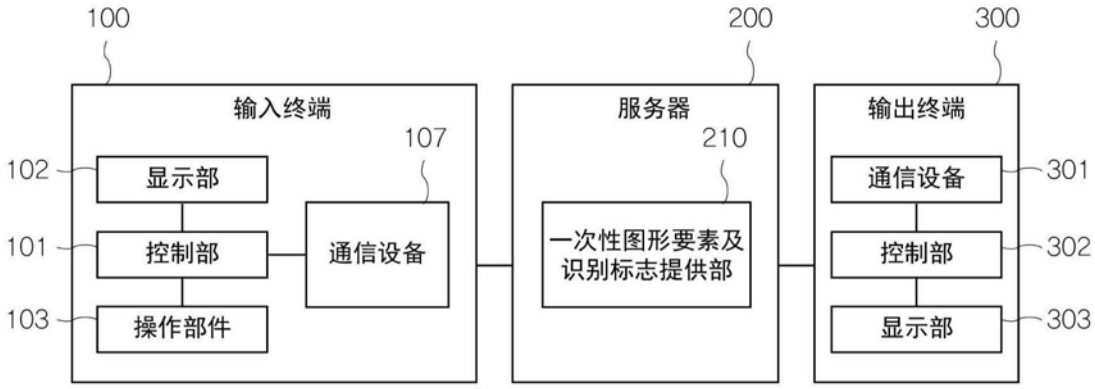

100
200
300
输入终端
服务器
输出终端
107
210
102
显示部
通信设备
301
101
控制部
一次性图形要素及
识别标志提供部
通信设备
302
103
操作部件
显示部
303

图26

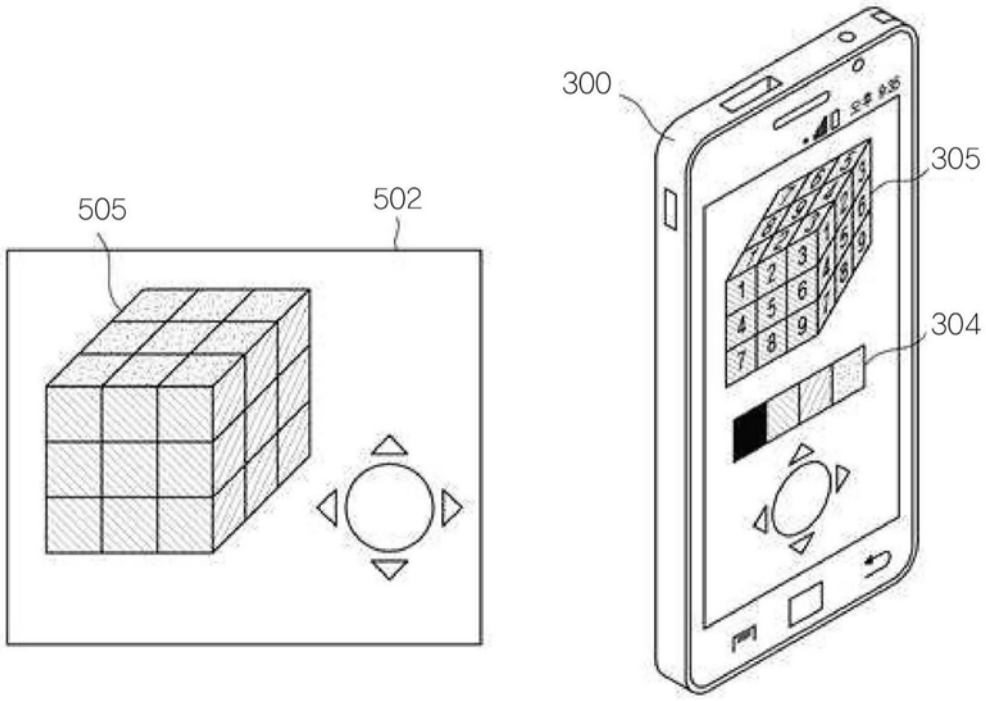


图27

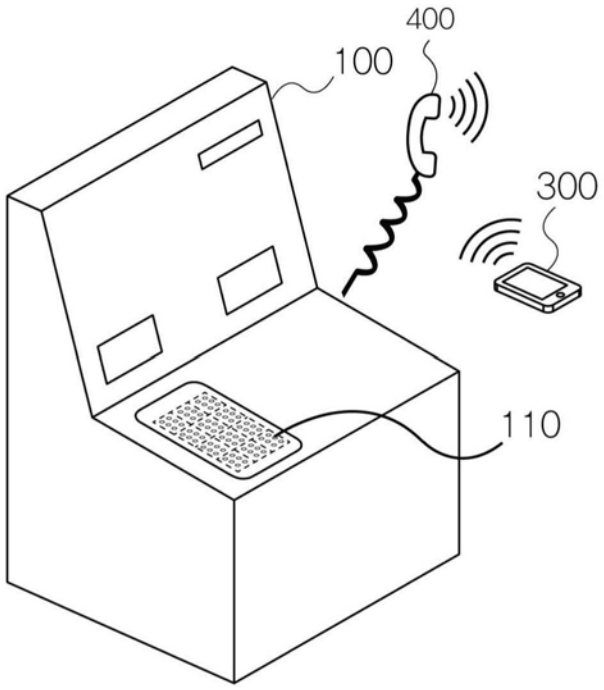


图28

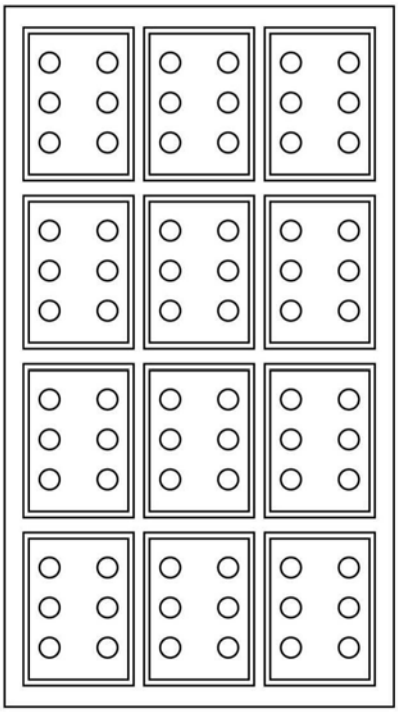


图29

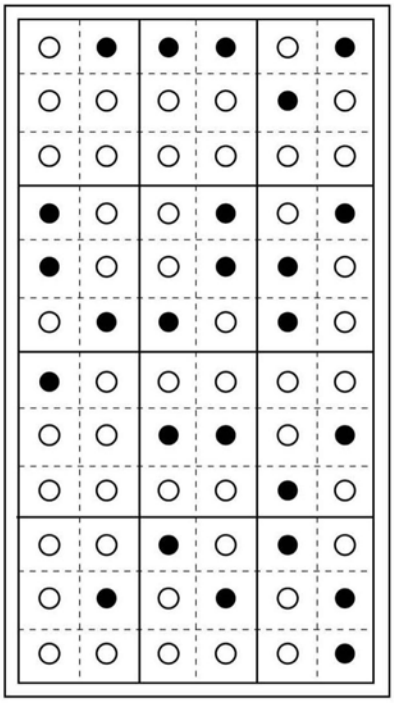


图30

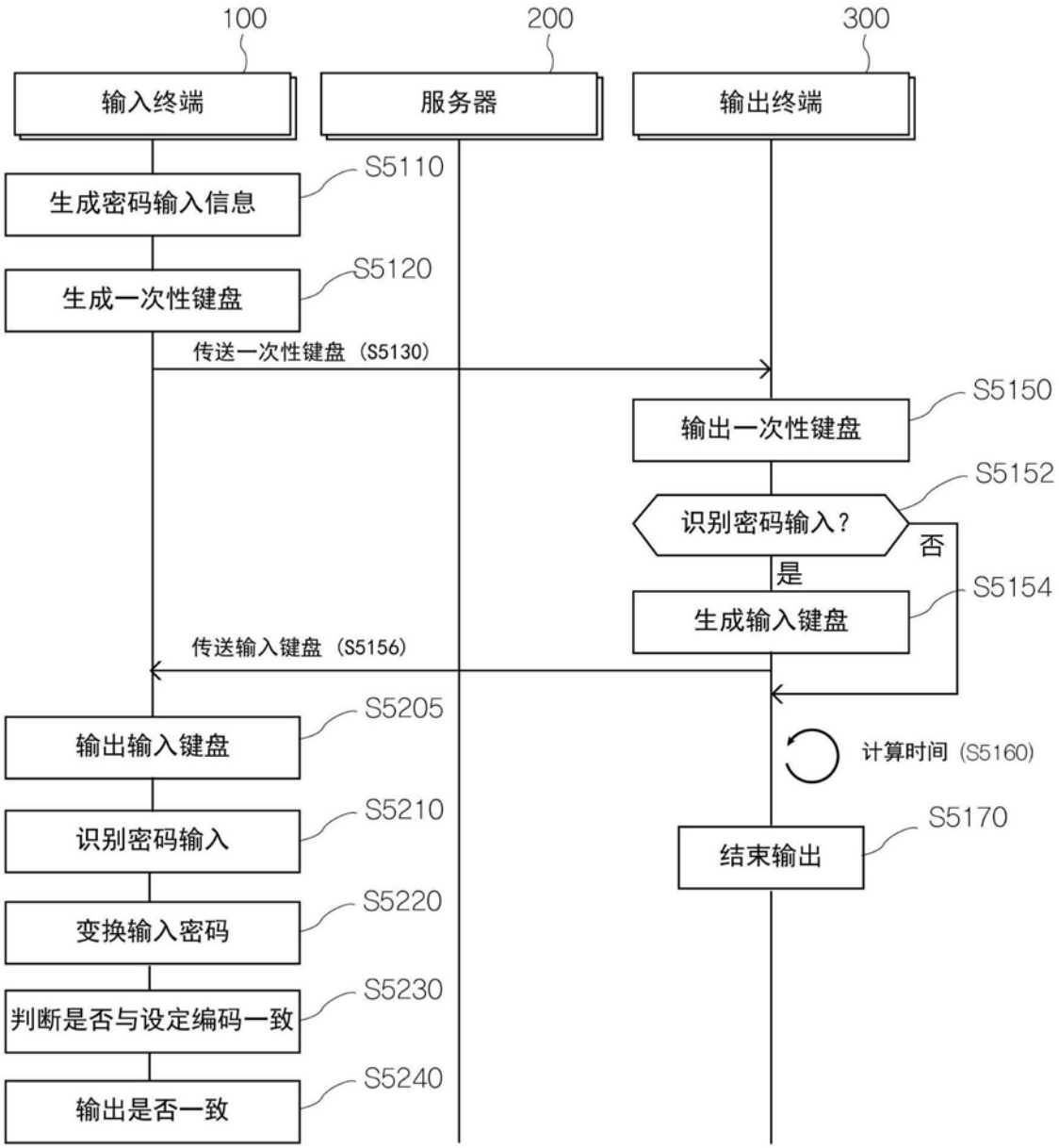

100
200
300
输入终端
服务器
输出终端
S5110
生成密码输入信息
S5120
生成一次性键盘
传送一次性键盘 (S5130)
S5150
输出一次性键盘
S5152
识别密码输入?
否
是
S5154
生成输入键盘
传送输入键盘 (S5156)
S5205
输出输入键盘
计算时间 (S5160)
S5210
识别密码输入
S5170
结束输出
S5220
变换输入密码
S5230
判断是否与设定编码一致
S5240
输出是否一致

图31

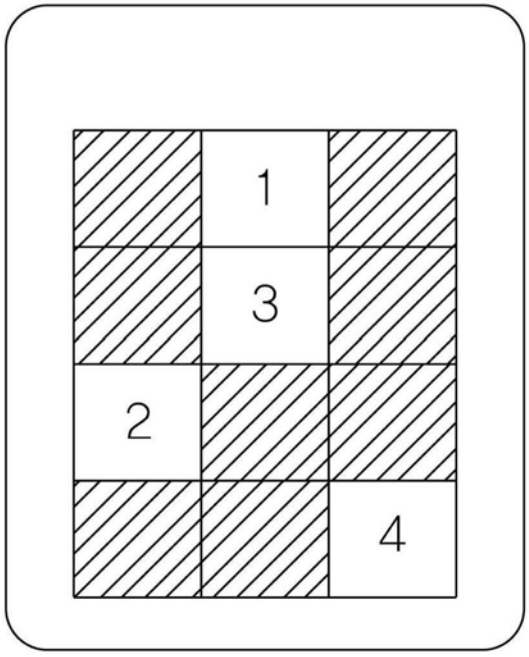

1
3
2
4

图32

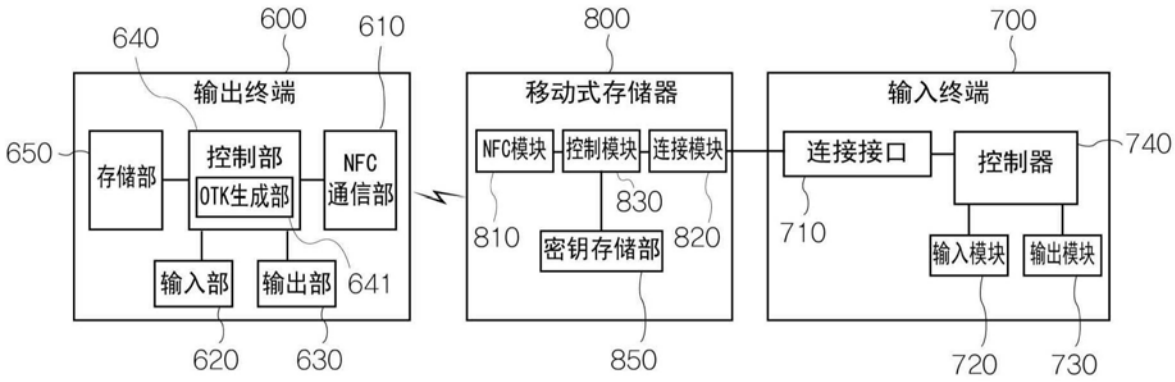

640
600
610
800
700
输出终端
移动式存储器
输入终端
650
存储部
控制部
OTK生成部
NFC
通信部
NFC模块
控制模块
连接模块
连接接口
控制器
740
830
810
密钥存储部
820
710
输入模块
输出模块
输入部
输出部
641
620
630
850
720
730

图33

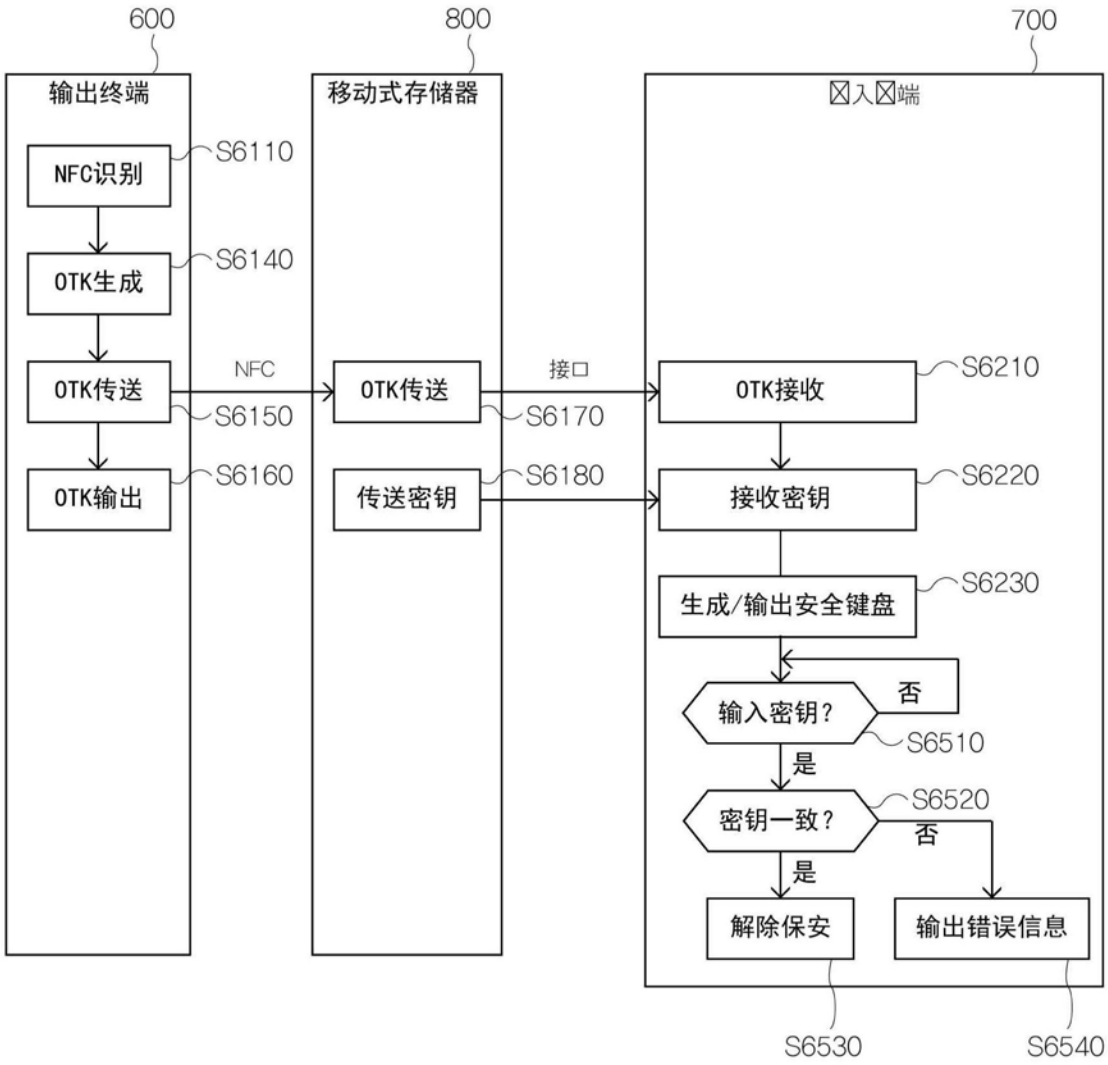

600
800
700
输出终端
移动式存储器
☒入☒端
NFC识别
S6110
OTK生成
S6140
OTK传送
S6150
NFC
OTK输出
S6160
OTK传送
S6170
接口
传送密钥
S6180
OTK接收
S6210
接收密钥
S6220
生成/输出安全键盘
S6230
输入密钥?
否
S6510
是
密钥一致?
S6520
否
是
解除保安
输出错误信息
S6530
S6540

图34

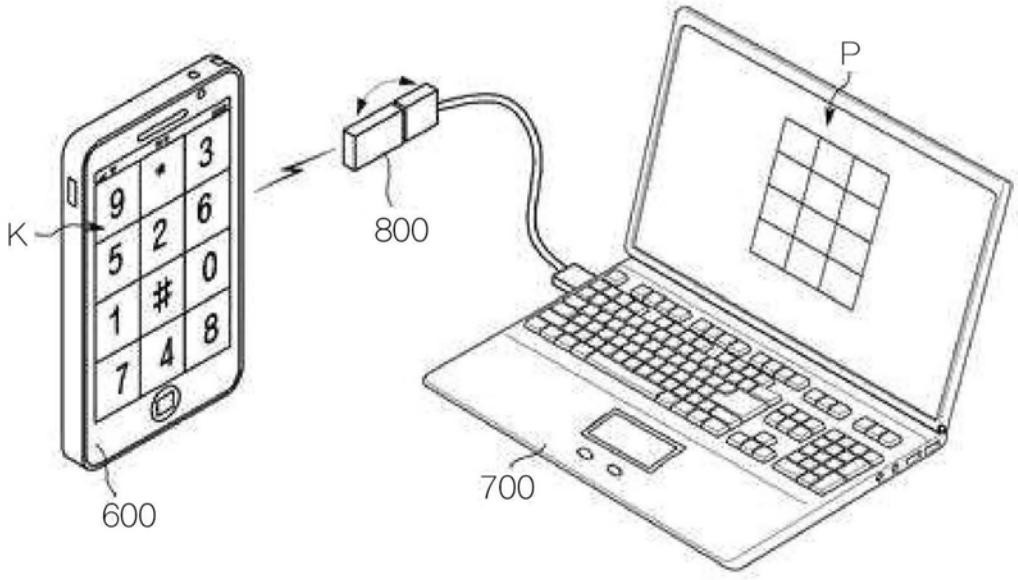

K
9
*
3
5
2
6
1
#
0
7
4
8
800
P
600
700

图35

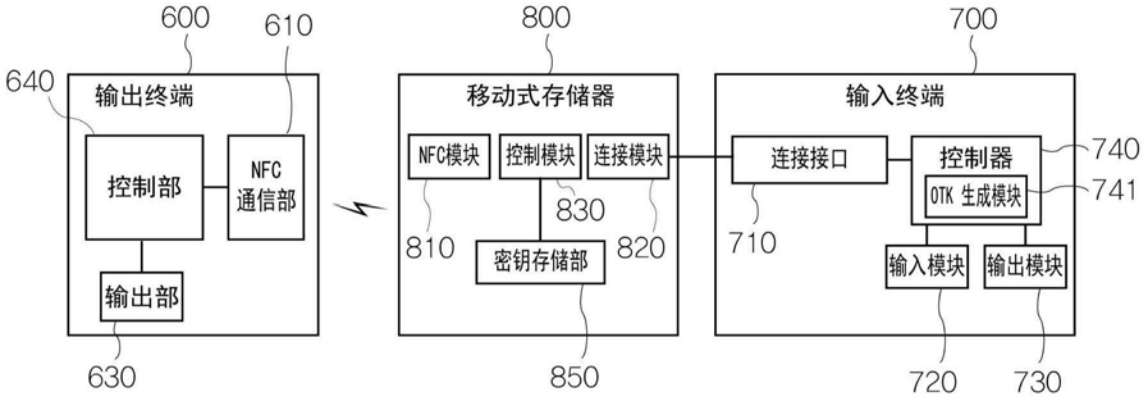

600
610
640
输出终端
控制部
NFC
通信部
输出部
630
800
移动式存储器
NFC模块
控制模块
连接模块
830
810
820
密钥存储部
850
700
输入终端
连接接口
710
控制器
740
OTK 生成模块
741
输入模块
输出模块
720
730

图36

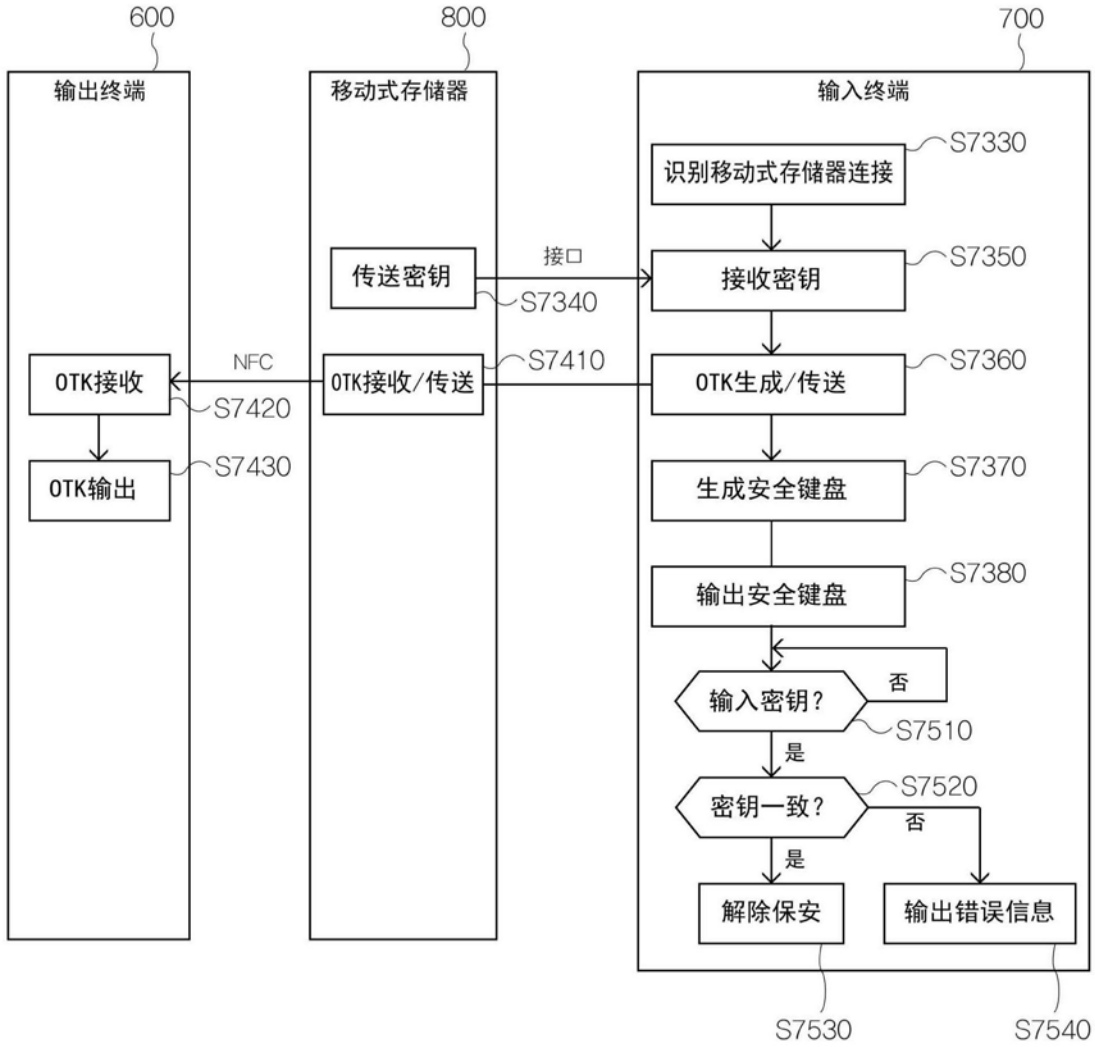

600
输出终端
800
移动式存储器
700
输入终端
识别移动式存储器连接
S7330
传送密钥
接口
接收密钥
S7350
S7340
OTK接收
NFC
OTK接收/传送
S7410
OTK生成/传送
S7360
S7420
OTK输出
S7430
生成安全键盘
S7370
输出安全键盘
S7380
输入密钥?
否
S7510
是
密钥一致?
S7520
否
是
解除保安
输出错误信息
S7530
S7540

图37

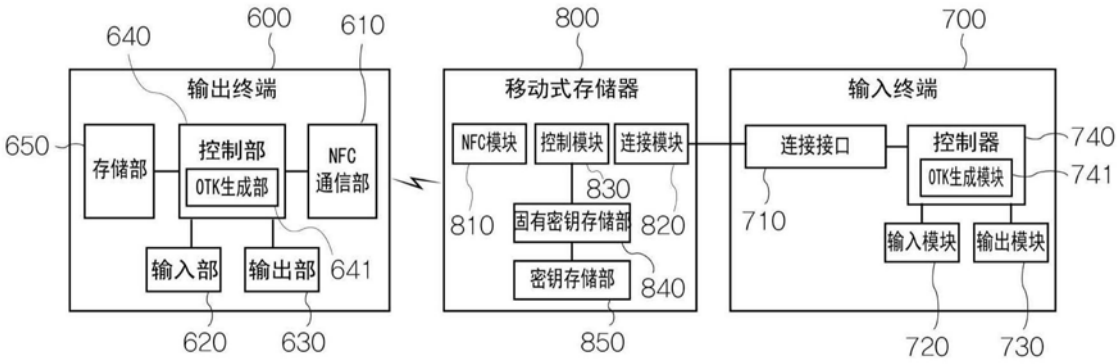

600
640
610
输出终端
650
存储部
控制部
OTK生成部
NFC
通信部
输入部
输出部
641
620
630
800
移动式存储器
NFC模块
控制模块
连接模块
830
810
固有密钥存储部
820
密钥存储部
840
850
700
输入终端
连接接口
控制器
740
OTK生成模块
741
710
输入模块
输出模块
720
730

图38

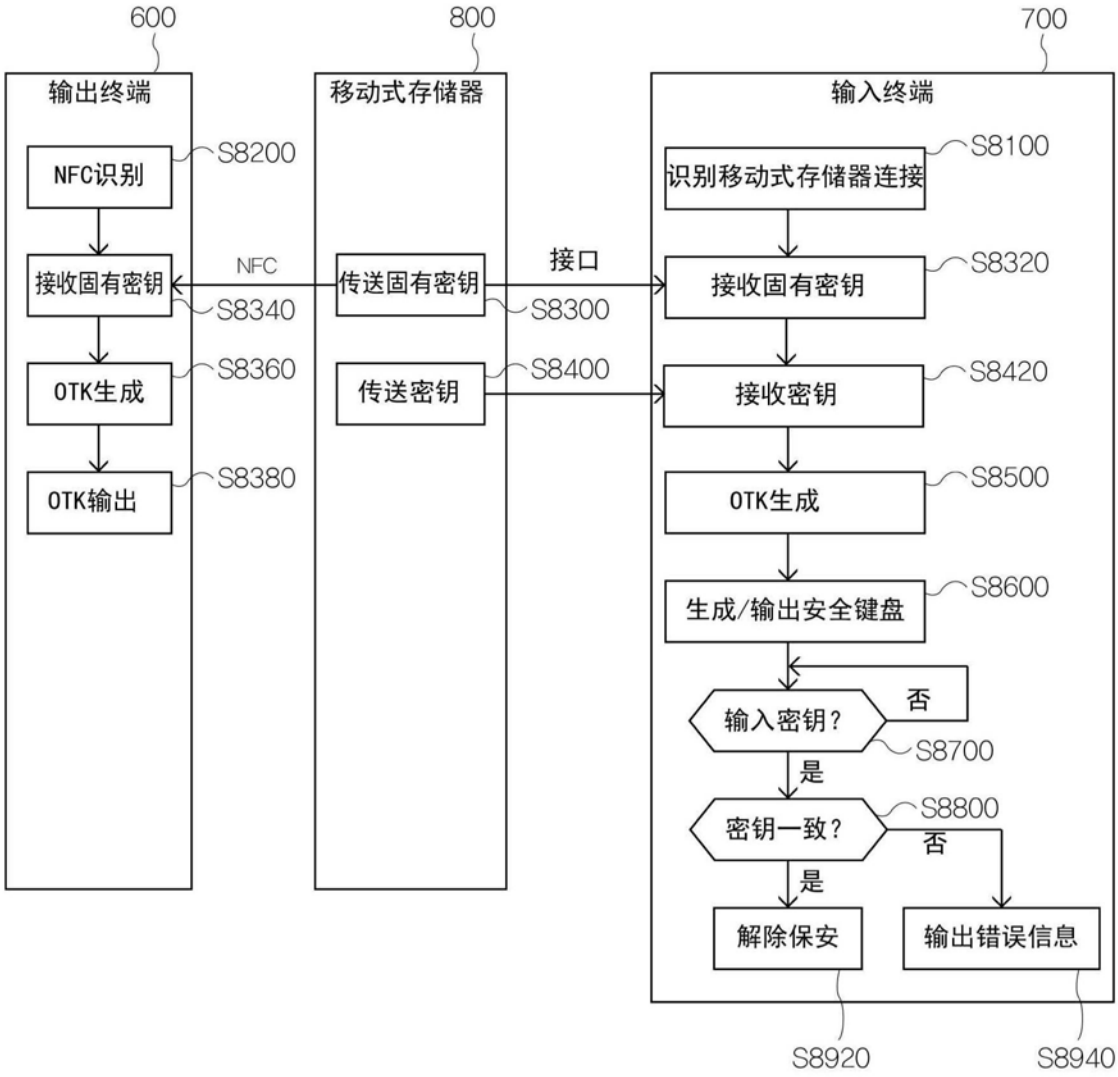

600
800
700
输出终端
移动式存储器
输入终端
NFC识别
S8200
识别移动式存储器连接
S8100
接收固有密钥
NFC
S8340
传送固有密钥
S8300
接口
接收固有密钥
S8320
OTK生成
S8360
传送密钥
S8400
接收密钥
S8420
OTK输出
S8380
OTK生成
S8500
生成/输出安全键盘
S8600
输入密钥?
否
S8700
是
密钥一致?
S8800
否
是
解除保安
输出错误信息
S8920
S8940

图39