(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107111777 A
(43)申请公布日 2017.08.29

(21)申请号 201580067899.1

(22)申请日 2015.11.20

(30)优先权数据
1461296 2014.11.21 FR

(85)PCT国际申请进入国家阶段日
2017.06.06

(86)PCT国际申请的申请数据
PCT/FR2015/053161 2015.11.20

(87)PCT国际申请的公布数据
WO2016/079455 FR 2016.05.26

(71)申请人 CB投资公司
地址 法国巴黎

(72)发明人 瑟吉·戈蒂埃

(74)专利代理机构 上海天协和诚知识产权代理事务所 31216
代理人 童锡君 张彪

(51)Int.Cl.
G06K 19/077(2006.01)
G06Q 20/10(2012.01)
G06Q 20/24(2012.01)
G06Q 20/34(2012.01)
G06Q 20/36(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G07F 7/10(2006.01)

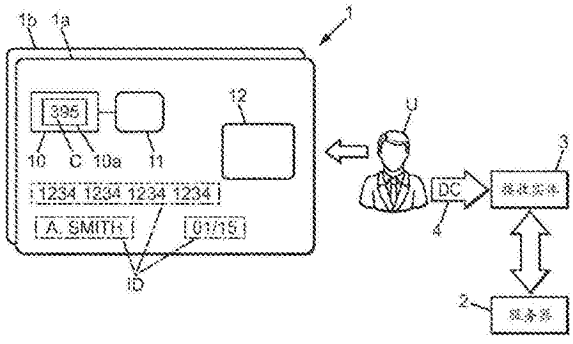
权利要求书2页 说明书7页 附图2页

(54)发明名称

适用于生成并显示支付卡安全码的方法，支付卡

(57)摘要

一种支付卡(1)，包括设置于支付卡表面(1a)的显示器件(10)，显示器件包括用于显示通过卡片验证服务器(2)执行的卡片验证操作的安全码的区域(10a)。该方法包括以下操作：在显示器件的区域显示第一时段(T1)期间的安全码(C1)的第一个值，在显示器件的区域显示第二时段(T2)期间的安全码(C2)的第二个值，所述第二时段在第一时段之后且第一时段和第二时段具有不同的持续时间。



CN 107111777 A

1.适用于生成并显示支付卡安全码的方法(1),所述支付卡包括设置于支付卡表面(1a)的显示器件(10),显示器件包括用于显示通过卡片验证服务器(2)执行的卡片验证操作的安全码的区域(10a),所述方法包括以下步骤:

在显示器件的区域显示(200)第一时段(T1)期间的安全码的第一个值(C1),

在显示器件的区域显示第二时段(T2)期间的安全码的第二个值(C2),所述第二时段在第一时段之后且第一时段和第二时段具有不同的持续时间。

2.根据权利要求1所述的方法,其特征在于,所述从第一时段(T1)到第二时段(T2)的转换操作(300)是在时间计数器(CT)超出与第一时段(T1)相关联的第一个转换阈值(VS1)的情况下进行,时间计数器由支付卡(1)的内部时钟(14)递增计数,内部时钟(14)与卡片验证服务器(2)不同步。

3.根据权利要求2所述的方法,其特征在于,所述从第一时段(T1)到第二时段(T2)的转换操作(300)包括以下步骤:

递增(330)安全码显示值(CV)的计数器的计数,

至少根据与支付卡(1)相关联的唯一数字秘钥(M)以及根据安全码显示值(CV)的计数器来确定(340)将在第二时段(T2)显示的安全码的第二个值(C2),

刷新(350)卡的显示器件(10),以显示安全码的第二个值(C2),以及,

至少根据安全码显示值(CV)的计数器来确定(360)与第二时段相关联的第二个转换阈值(VS2)。

4.根据权利要求1至3任一项所述的方法,其特征在于,所述在显示器件(10)的区域(10a)显示的安全码值(C1,C2)不包含卡片验证服务器(2)的同步数据。

5.根据权利要求1至4任一项所述的方法,包括n个连续的显示操作(200),

在n个显示操作之中的每个显示操作i包括在与所述显示操作相关联的时段(Ti)期间在显示器件(10)的区域(10a)内显示与所述显示操作相关联的安全码值(Ci),

而且,其中,与多个显示操作之中的连续显示操作相关联的连续时段(Ti)构成可计算的非常量序列。

6.根据权利要求1至5任一项所述的方法,其特征在于,所述与时段(Ti)相关联的转换阈值(VSi)根据安全码显示值(CV)的计数器、根据两次转换之间的时段的平均值(MSM)、根据与支付卡相关联的唯一变化范围(PVAR)以及根据卡开始操作的瞬时值(T0)来确定。

7.支付卡(1),包括:

显示器件(10),设置于支付卡表面(1a)并包括用于显示通过卡片验证服务器(2)执行的卡片验证操作的安全码的区域(10a),以及,

控件电路(11),将其设置为控制在显示器件的所述区域内显示至少在第一时段(T1)期间的安全码的第一个值(C1)以及在第二时段(T2)期间的安全码的第二个值(C2),所述第二时段在第一时段之后且第一时段和第二时段具有不同的持续时间。

8.根据权利要求7所述的支付卡(1),其特征在于,所述控件电路(11)包括:

*存储器(13),用于存储时间计数器(CT)以及至少一个转换阈值(VSi),

*内部时钟(14),与卡外部不同步,用于递增时间计数器的计数,以及,

*处理电路(15),用于在时间计数器超出与第一时段(T1)相关联的第一个转换阈值(VS1)的情况下,从第一时段(T1)转换到第二时段(T2)。

9.根据权利要求8所述的支付卡(1),进一步包括写在支付卡表面(1b)的初始账号PAN。

10.适用于支付卡(1)的计算机程序,所述程序包括执行根据权利要求1至6任一项所述的生成并显示卡片验证操作安全码的方法的步骤的指令。

适用于生成并显示支付卡安全码的方法,支付卡

技术领域

[0001] 本发明涉及一种配有显示器件的支付卡,所述显示器件用于显示卡片验证操作的安全码并设置于支付卡一面;本发明还涉及生成并显示这种支付卡安全码的方法。

[0002] 本发明涉及诸如EMV(泛欧卡、万事达卡、维萨卡)或其它类型卡的银行支付卡领域。

背景技术

[0003] 这类支付卡通过诸如因特网、邮件、传真或电话来进行的远程交易通常涉及提供写在支付卡一面的初始账号PAN以及写在卡上的一些附加信息,比如支付卡的有效期和/或持卡人身份。

[0004] 为了确保远程交易的安全,通常还需要提供卡安全码(CSC),也称之为卡验证值,服务器将其用于卡片的验证操作。安全码通常由写在支付卡上的3个或4个数字组成,通常是在卡上与呈现初始账号PAN的那一面相反的一面。

[0005] 构成安全码的数字可以是通过与支付卡相关联的唯一数字密钥来加密卡的初始账号PAN、其有效期以及卡所用的服务码,并且通过保持所得结果的3位数或4位数而确定的。

[0006] 就此而论,就需要防范那些曾访问过支付卡信息并且保存过初始账号PAN、附加数据及安全码的未获授权的人或机构采集和/或重新使用安全码。

[0007] 为此目的,已经提出了配有显示器件的支付卡,所述显示器件用于显示安全码值并设置于支付卡的一面,其中,安全码值可定期刷新,以便防止或者限制未获授权的人重新使用安全码。

[0008] 文件US7,954,705显示了一个这种支付卡以及生成并显示支付卡安全码的方法的实例。

[0009] 然而,需要进一步提高这种支付卡的安全性,尤其是防止或限制反向制造支付卡的可能性。

发明内容

[0010] 本发明提供一种生成并显示支付卡安全码的方法,所述支付卡包括设置于支付卡表面的显示器件,显示器件包括用于显示卡片验证操作的安全码的区域,所述卡片验证操作是通过卡片验证服务器执行的,方法包括以下步骤:

[0011] -在显示器件的区域显示第一时段期间的安全码的第一个值,

[0012] -在显示器件的区域显示第二时段期间的安全码的第二个值,所述第二时段在第一时段之后且第一时段和第二时段具有不同的持续时间。

[0013] 因此,安全码通过电子墨或者其它显示类型显示在卡上并且按照计算出的时间间隔来刷新。持卡人按照与当前普遍使用的永久不变的安全码相同的方式来使用当前的安全码值。

[0014] 安全性的提高得益于所捕捉到的数字的快速失效，因此，捕捉的数字失效必须足够快，以至于不允许广泛使用卡，但是也必须足够长，以至于使用者容易获得安全码。

[0015] 尤其是，如果使用者在卡上读取安全码的第一个值并随后将其发送到卡片验证服务器，与此同时，卡显示器就已经转换到了安全码的第二个值，那么卡验证便会失败。

[0016] 为了减少卡用户所经历的伤脑筋的情况，可对其进行设置，以便在改变值的时刻前后的时段内能接收到安全码的两个值，这两个值具体是在时间上一个接一个的第一个值和第二个值。

[0017] 因此，所述改变安全码值的时刻前后的时段是一段时间，在这段时间中，随机生成可接收的安全码的可能性是这段时间以外其它时段的二倍。根据本发明所生成并显示安全码的方法使之更难通过反向工程来识别出这个时段，因为改变安全码值的时刻不是定期连续的。

[0018] 在一个实施例中，在时间计数器超出与第一时段相关联的第一个转换阈值的情况下，进行从第一时段到第二时段的转换操作，时间计数器由支付卡的内部时钟计数并且该内部时钟与卡片验证服务器不同步。

[0019] 这样，就不可能通过拦截卡与验证服务器之间的交换来获取表示卡何时将要转换的同步信息。

[0020] 这就增强了安全码的安全性。

[0021] 最好，从第一时段到第二时段的转换操作包括以下步骤：

[0022] -递增安全码显示值的计数器的计数，

[0023] -至少根据与支付卡相关联的唯一数字秘钥并且根据安全码显示值的计数器来确定将在第二时段显示的安全码的第二个值，

[0024] -刷新卡的显示器件以显示安全码的第二个值，以及，

[0025] -至少根据安全码显示值的计数器来确定与第二时段相关联的第二个转换阈值。

[0026] 在一个有利的实施例中，在显示器件的区域显示的安全码值不包含卡片验证服务器的同步数据。

[0027] 在一个特殊实施例中，该方法包括多个连续的显示操作，

[0028] 在多个显示操作之中的每个显示操作包括在与所述显示操作相关联的时段期间在显示器件的区域内显示与所述显示操作相关联的安全码值，

[0029] 而且，其中，与多个显示操作之中的连续显示操作相关联的连续时段构成可计算的非常量序列。

[0030] 最好，与时段相关联的转换阈值根据安全码显示值的计数器，根据两次转换之间的时段平均值，根据与支付卡相关联的唯一变化范围以及根据卡片操作开始的瞬时值来确定。

[0031] 本发明的另一方面涉及一种支付卡，包括：

[0032] -显示器件，设置于支付卡表面且包括用于显示卡片验证操作的安全码的区域，所述卡片验证操作通过卡片验证服务器进行，以及，

[0033] -控件电路，将其设置为控制在显示器件的所述区域内显示至少在第一时段期间的安全码的第一个值以及在第二时段期间的安全码的第二个值，所述第二时段在第一时段之后且第一时段和第二时段具有不同的持续时间。

[0034] 在一个特殊实施例中，控件电路包括：

[0035] *存储器，用于存储时间计数器以及至少一个转换阈值，

[0036] *内部时钟，与卡外部不同步，以便递增时间计数器的计数，以及，

[0037] *控制电路，用于在时间计数器超出与第一时段相关联的第一个转换阈值的情况下，从第一时段转换到第二时段。

[0038] 在这种情况下，支付卡优选进一步包括写在支付卡表面的初始账号PAN。

[0039] 本发明的另一方面涉及一种支付卡的计算机程序，该程序包括执行上文所述的生成并显示卡片验证操作安全码的方法的步骤的指令。

附图说明

[0040] 本发明的其它特征和优点将通过下列非限制性的示例性实施例的说明并参考附图而更加显而易见，在附图中：

[0041] 图1是包括根据本发明的支付卡的支付卡验证系统以及卡片验证服务器和接收实体的示意图；

[0042] 图2是图1所示的支付卡的详细框图；

[0043] 图3是生成并显示适用于诸如图1和图2所示的支付卡的安全码的操作流程图；

[0044] 图4是在根据本发明生成并显示安全码的方法过程中进行转换操作的详细流程图。

具体实施方式

[0045] 下文通过利用EMV卡(泛欧卡、万事达卡、维萨卡)进行远程交易的非限制性应用对本发明进行说明。

[0046] 图1所示的实体1是支付卡1，例如，EMV卡(泛欧卡、万事达卡、维萨卡)。

[0047] 实体2是卡片验证服务器，包括至少一个卡数据输入单元20以及处理单元21。

[0048] 实体3是接收实体3，支付卡1的使用者U可通过诸如因特网、邮件、传真或电话等通信信道4在远程交易过程中实现接收实体与支付卡的通信。

[0049] 因此，接收实体3可以是互联网零售商网站的服务器或者互联网在线支付网站或者通过邮件、传真或电话接收交易请求的提供商。因此，接收实体3适合经由各种通信信道4来接收来自支付卡2使用者U的卡数据DC。接收实体3进一步适合经由第二通信信道5将数据发送到卡片验证服务器2，第二通信信道例如是诸如因特网、内联网或者点到点的有线或无线连接的网络。

[0050] 因此，接收实体3处于支付卡1的使用者U与卡片验证服务器2的之间。

[0051] 卡数据DC包括来自支付卡1的待测试的安全码值C以及所述支付卡的识别信息ID，例如，支付卡的初始账号PAN、支付卡的有效期和/或支付卡持卡人的身份。

[0052] 卡片验证服务器2适合并用于执行卡片验证操作，所述卡片验证操作包括：

[0053] -通过输入单元20接收卡数据的操作，

[0054] -通过处理单元21来确定可接受安全码值的操作。尤其是，可以通过卡数据中所包含的识别信息来确定可接受安全码值，例如，通过初始账号PAN、支付卡的有效期和/或支付卡持卡人的身份。在不使用卡数据中包含的待测试的安全码值的情况下确定可接受安全码

值。

[0055] -将待测试的安全码值与可接受安全码值进行比较的操作，以便确定是否接受卡数据。

[0056] 在确定可接受安全码值的操作过程中，卡片验证服务器2可以从数据库3提取关于支付卡的附加信息。该附加信息可以是例如下文详细说明的计算安全码值的算法的种子值。然后，根据卡数据所包含的识别信息以及根据从数据库3所获得的附加信息来确定可接受安全码值。

[0057] 所述数据库3可将所述附加信息与诸如初始账号PAN这类支付卡识别信息相关联，从而有助于访问所述附加信息。

[0058] 当然，卡片验证操作可包括本文未提及的附加操作，例如，验证支付卡识别信息，验证支付卡的初始账号PAN、支付卡的有效期和/或支付卡持卡人的身份。

[0059] 卡片验证操作通常在可能的程度上使之能够确定支付卡是否真实属于请求远程交易的使用者U。

[0060] 支付卡1是已知形式的卡，例如，ISO7810ID-1，ISO7813所定义的卡，即，其基本形状为便于携带的半刚性片材，其厚度可为数毫米和每面边长数厘米，至少局部可由塑料制成。

[0061] 它包括两个相反面1a和1b。至少其中一面1b可提供某些信息，尤其是诸如支付卡的初始账号PAN、支付卡的有效期和/或支付卡持卡人的身份这类支付卡识别信息ID。

[0062] 支付卡1还包括显示器件10。

[0063] 显示器件10设置于支付卡1的表面1a。显示器件10包括用于显示安全码的区域10a。显示器件10设置于卡的表面1a，以便支付卡1的使用者能够看见区域10a。

[0064] 显示器件10可以设置于与某些支付卡识别信息相同的表面。或者，显示器件10可设置于一个表面1a，而支付卡识别信息设置于相反的表面1b，使得不能同时看见安全码和支付卡识别信息。这降低了欺诈风险。

[0065] 在一个实施例中，允许重新使用现有的通信信道，在显示器件10的区域10a中显示的每个安全码值包括3或4个数位。

[0066] 支付卡1还包括控件电路11，用于控制在显示器件10的区域10a中显示200用于通过卡片验证服务器执行如上所述的卡片验证操作的安全码值。

[0067] 因此，在通过这种支付卡1进行远程交易中，例如，通过因特网、邮件、传真或电话，卡的使用者U可以在支付卡1上读取上文详细说明的卡数据，意即包括待测试的安全码值、支付卡的初始账号PAN、支付卡的有效期和/或支付卡持卡人的身份的数据，并且可以通过适当的信道(根据实施例：通过把数据输入网页或计算机程序的区域，通过信件、传真或电话进行的书面或口头的通信)将这些数据提供给接收实体3，由其传递到卡片验证服务器2，以确定是否接收数据以及是否可以对交易进行授权。

[0068] 在一个实施例中，接收实体3可直接作为卡片验证服务器2。

[0069] 支付卡1还可以包括芯片10，所述芯片能够与终端，尤其是与支付终端进行电子通信或无接触的通信，例如，从而像通过普通支付卡所实践的那样进行直接付款交易。控件电路11可以集成于芯片12，或者可以是在物理上与所述芯片12分开的电路。

[0070] 很显然，在这种直接付款交易中，卡的提供者与商家(机器或个人)亲自出现并彼

此接近。商家通常能够在视觉上或者通过接触或检测来确认支付卡确实属于请求交易的使用者。本发明感兴趣的是远程交易，在所述远程交易中通常并不验证是否亲自这样出现。

[0071] 更具体而言，控件电路11设置成控制在显示器件10的区域10a显示200至少在第一时段T1期间的安全码的第一个值C1以及在第一时段T1之后的第二时段T2期间的安全码的第二个值C2。

[0072] 图3阐释了一个这种方法的实施例，其中，循环100、200、300、400连续显示安全码的不同值。转换操作300使之能够切换从一个安全码值到另一个安全码值的显示。

[0073] 图3所示的流程图是一个程序的典型实例，可以在所述设备上执行所述程序的某些指令。因此，图3可以对应于就本发明意义而言的计算机程序的通用算法的流程图。

[0074] 应该理解的是，在指定时刻，区域10a从C1和C2中显示唯一安全码值。但是，这个显示的唯一值能够随着时间而改变。在本发明的一个实施例中，区域10a特别适合仅显示指定时刻的一个安全码值，并且不能同时显示多个安全码值。这样，就减少了显示器件10的尺寸和能耗。

[0075] 为此目的，控件电路11具体可包括存储器13和内部时钟14。

[0076] 存储器13适合包含时间计数器CT以及至少一个转换阈值VS1。

[0077] 内部时钟14适合按照有规律的时间间隔递增所述时间计数器TC的计数。有利的是，内部时钟14与支付卡1外部不同步，尤其是与卡片验证服务器2不同步。这就使其更难预测在不同安全码值之间切换的时刻并且降低了欺诈风险。

[0078] 为此目的，例如，在显示器件10的区域10a显示的安全码值不包括同步数据。

[0079] 控件电路11可进一步包括控制电路15以及与显示器件10通信的通信电路16。

[0080] 控制电路15可与内部时钟14、存储器13和通信电路16通信。

[0081] 在本发明的一个特殊实施例中，控件电路11可以集成于显示器件10中。

[0082] 在其它实施例中，控件电路11和显示器件10可以物理分隔并形成两个单独的芯片。

[0083] 例如，控件电路11和/或控制电路15可以是：

[0084] -处理器，适合以计算机程序的形式来解释指令，或者，

[0085] -微芯片，尤其是以硅形式定义本发明方法的步骤的芯片，或者，

[0086] -可编程微芯片。

[0087] 图4更具体地描述了转换操作300所包括的子步骤。

[0088] 如图3和图4所示，控制电路15能够执行从第一时段T1到第二时段T2的至少一个转换操作300。尤其是，该转换操作300可以在时间计数器TC超出转换阈值VS1的情况下实施。转换阈值VS1可以是与第一时段T1相关联的第一个转换阈值VS1。

[0089] 例如，时间计数器CT由控件电路11的内部时钟14定期计数310，并且当所述时间计数器CT超出针对每个时段320所定义的阈值时，在显示器件10的区域10a显示350安全码的新值。在一个实施例中，接着可以重新设置时间计数器CT或者在考虑时间计数器CT中早已存在的值来确定新的阈值。

[0090] 更具体而言，从第一时段T1到第二时段T2的转换操作至少可包括以下步骤：

[0091] -递增330安全码显示值CV的计数器的计数，在这种情况下，所述计数器包含第二时段的指数i，意即值2，

[0092] -至少根据与支付卡1相关联的唯一数字密钥M以及根据安全码显示值CV的计数器来确定340将在第二时段T2期间显示的安全码的第二个值C2，

[0093] -刷新350卡的显示器件10，以显示安全码的第二个值C2，以及，

[0094] -至少根据安全码显示值CV的计数器来确定360与第二时段T2相关联的第二个转换阈值VS2。

[0095] 可以看到，这种算法很容易使第一时段和第二时段T1、T2具有不同的持续时间。

[0096] 在一个示例性实施例中，在转换操作的附加步骤过程中可以重新设置时间计数器CT。

[0097] 这些步骤310、320、330、340、350、360可按照上述顺序连续进行。在本发明的一个可能的变体中，上述步骤可以按照与所述顺序不同的顺序执行或者甚至并行地执行这些步骤中的所有步骤或部分步骤。

[0098] 最后，安全码的不同值都可以通过能够获得连续可计算值的任何计算方法来确定，有利的是，所述计算方法是难以可逆或是不可能可逆的。例如，可以采用与已知的安全码计算算法相似的算法，例如，EMV(泛欧卡、万事达卡、维萨卡)规范所定义的算法。

[0099] 这种算法利用与支付卡1相关联的唯一数字密钥M来计算安全码值，有可能利用上文详细说明的卡数据，换言之，例如是待测试的安全码值、支付卡的初始账号PAN、支付卡的有效期和/或支付卡持卡人的身份。

[0100] 为了获取连续的安全码值，因此考虑安全码显示值CV的计数器是足够的。所述算法的一部分输入值可以用安全码显示值CV的计数器的值来代替，例如，所述输入值为与支付卡1相关联的所述唯一数字密钥M的一部分或所述卡的一部分数据。

[0101] 这个计算安全码的方法示例很显然是出于给出信息以及非限制性的目的所提供的，当然可以设想计算这样一系列连续安全码值的变体。

[0102] 应该理解的是，该方法特别适合有n个连续的显示操作200的情况，如图3所示。

[0103] 在这种情况下，多个显示操作之中的每个显示操作i包括在显示器件10的区域10a显示在时段Ti内与所述显示操作i相关联的安全码值Ci，所述时段Ti也与所述显示操作i相关联。

[0104] 当然，在这种情况下，例如，安全码显示值CV的计数器将包括时段的指数i的每个连续值，意即从1至n的连续值。

[0105] 因此，安全码显示值CV的计数器能够存储当前安全码显示值的指数i。为了更好地理解本发明，在本说明中指数i用来表示安全码当前显示值的指数，同时，要记住的是，实际上，所述值包含在变量CV中，这在执行根据本发明的方法时，刷新所述变量CV。

[0106] 现在将详细说明与多个显示操作之中的连续的显示操作相关联的连续时段T1，...，Tn能构成可计算的非常量序列。

[0107] “非常量序列”的含义是：多个连续时段T1，...，Tn之中的至少两个时段Ti，Tj的持续时间彼此相互不同。换言之，这意味显示器件10的转换在时间上不是周期性的。

[0108] 有利的是，大部分连续时段T1，...，Tn可彼此间相互不同，甚至所有的连续时段T1，...，Tn都可以彼此相互不同，没有与另一其它时段T1，...，Tn的持续时间相同的时段T1，...，Tn。

[0109] “可计算序列”的含义是：连续时段T1，...，Tn的顺序是可预测的，并且可以通过一

组预定的和已知的数据来计算的，例如，通过支付卡的制造商对其进行计算。

[0110] 尤其是，在不与支付卡1交换同步信息的情况下，就不可能由卡片验证服务器2来验证当前显示的安全码中的值。

[0111] 所述一组预定的和已知的数据可以包括初始账号PAN、支付卡的有效期和/或支付卡持卡人的身份，但是也可以包括计算安全码值的算法的种子值，现在以根据一个本发明方法的特定实施例对此进行详细说明。

[0112] 例如，如下所述，根据安全码显示值CV的计数器，可以确定与时段Ti相关联的变量TVARi，在这个实例中，所述变量是i，具有与支付卡PVAR相关联的唯一变化范围：

[0113] $TVAR_i = i^2 \bmod PVAR$

[0114] 与时段Ti相关联的转换阈值VSi可以根据与时段Ti相关联的变量TVARi以及根据两次转换VSm之间的时段的平均值以及开始操作卡的瞬时值TO来确定，例如：

[0115] $VS_i = TO + i * VSm + TVAR_i$

[0116] 这样，就可以确定与时段Ti相关联的转换阈值VSi且无需通过卡与服务器进行同步便可以进行计算。

[0117] 有利的是，在连续转换阈值VSi之间的变量本身并非周期性的，或者，换言之，在连续时段T1，...，Tn顺序的持续时间内的变量并非周期性的，因此，不容易预测。

[0118] 应该注意的是，这与简单的显示器件10切换次数的非周期性无关，因为它是非周期性(即连续时段Ti、Ti+1之间的变量是非周期的)，其本身并非周期性的。

[0119] 因此，在该特定实施例中，种子值是两次切换VSm之间时段的平均值、与支付卡PVAR相关联的唯一变化范围以及开始操作卡TO的瞬时值。

[0120] 因此，可以看到，这些种子值很容易在在支付卡1与卡片验证服务器2之间共享，例如，制造支付卡1过程中或者紧接着制造支付卡1之后。

[0121] 此外，与时段Ti相关联的一系列转换阈值VSi是可计算的非常量序列。因此，与多个显示操作之中的连续显示操作i相关联的一系列连续时段Ti也形成可计算的非常量序列。

[0122] 选择不同的种子值，以确保一系列连续时段Ti有足够的变化性，从而降低欺诈风险，同时保持操作者使用方便，意即确保显示每个安全码值时有充足的时间，以便使用者能够按照正常速度对其进行读取和使用。

[0123] 当然，应理解的是，仅通过实例的方式列出了关于确定与时段Ti相关联的转换阈值VSi的上述等式。

[0124] 因此，可以认为，改变这些等式的确切形式并利用诸如确定的时间增量的这种附加种子值，以确保每个安全码值的最短显示时间。

[0125] 当然，本发明不仅仅只限于上文所述的作为示例的实施例；本发明延伸至其它变体。

[0126] 其它实施例也是有可能的。

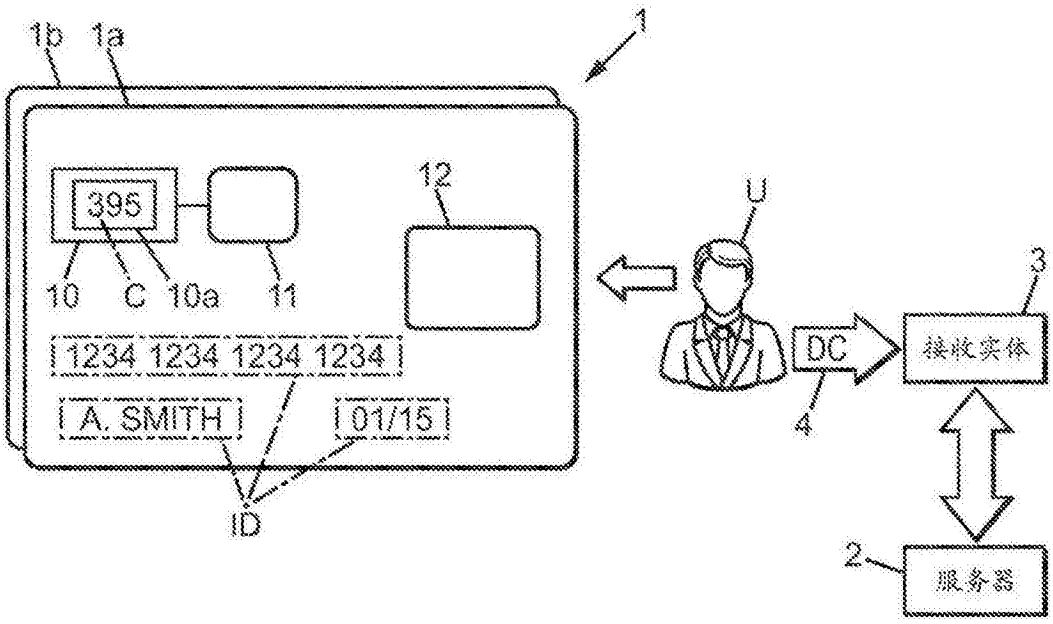

1b
1a
1
395
12
U
10
C
10a
11
3
DC
接收实体
1234 1234 1234 1234
A. SMITH
01/15
ID
4
2
服务器

图1

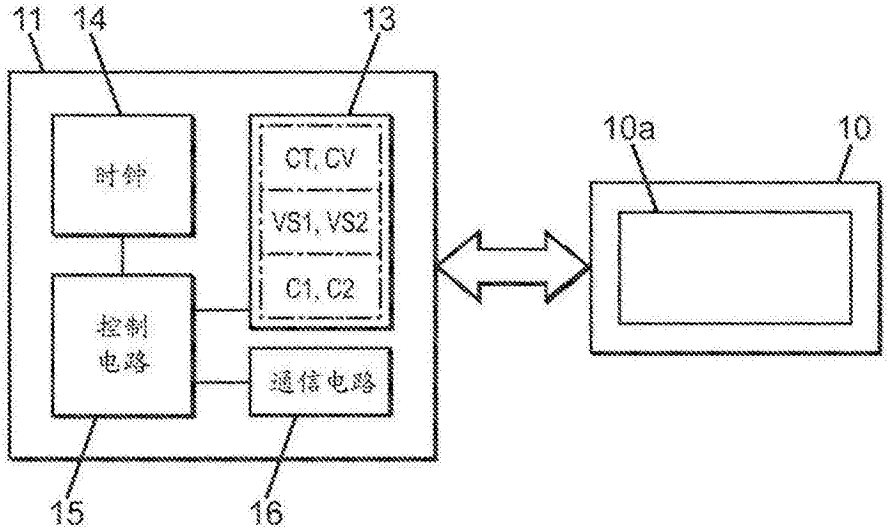

11
14
13
时钟
CT, CV
VS1, VS2
C1, C2
10a
10
控制
电路
通信电路
15
16

图2

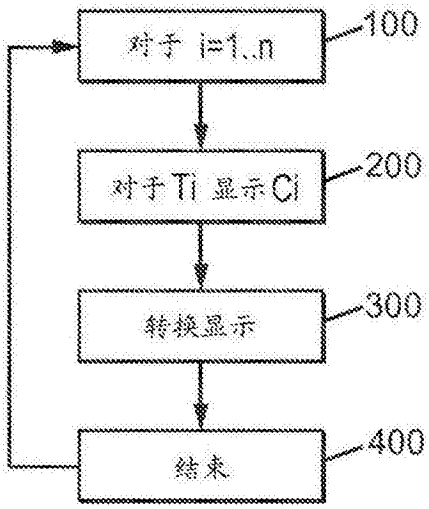

对于 i=1..n
100
对于Ti 显示Ci
200
转换显示
300
结束
400

图3

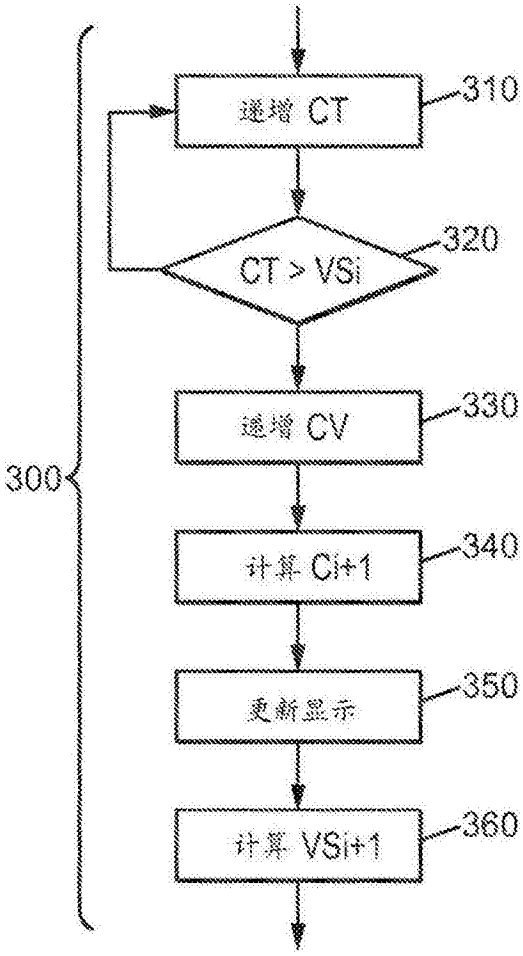

递增 CT
310
CT > VSi
320
递增 CV
330
300
计算 Ci+1
340
更新显示
350
计算 VSi+1
360

图4