(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 106656471 B
(45)授权公告日 2019.05.14

(21)申请号 201611199027.3

(22)申请日 2016.12.22

(65)同一申请的已公布的文献号
申请公布号 CN 106656471 A

(43)申请公布日 2017.05.10

(73)专利权人 武汉信安珞珈科技有限公司
地址 430071 湖北省武汉市东湖开发区珞瑜东路4号慧谷时空1608室

(72)发明人 李涛 胡进

(74)专利代理机构 武汉臻诚专利代理事务所（普通合伙）42233
代理人 宋业斌

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 103996011 A,2014.08.20,
CN 204791026 U,2015.11.18,
CN 104244235 A,2014.12.24,
US 2015281224 A1,2015.10.01,

审查员 吕小倩

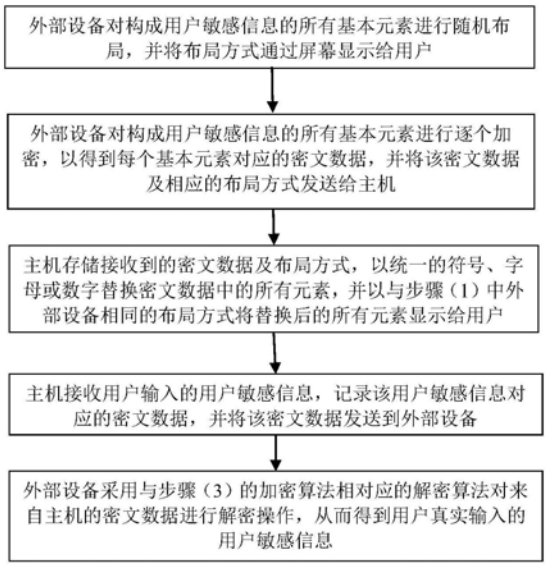
权利要求书3页 说明书6页 附图2页

(54)发明名称

一种用户敏感信息的保护方法和系统

(57)摘要

本发明公开了一种用户敏感信息的保护方法，包括：外部设备对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户，外部设备对构成用户敏感信息的所有基本元素进行逐个加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机，主机存储接收到的密文数据及布局方式，以统一的符号、字母或数字替换密文数据中的所有元素，并以与外部设备相同的布局方式将替换后的所有元素显示给用户。本发明能够解决现有身份认证或交易认证系统存在的敏感信息容易被黑客非法盗取，给用户的使用带来巨大的安全风险、以及由于需要为外部设备配置键盘所带来的硬件成本增加的技术问题。



CN 106656471 B

1.一种用户敏感信息的保护方法,其特征在于,包括以下步骤:

(1)外部设备对构成用户敏感信息的所有基本元素进行随机布局,并将布局方式通过屏幕显示给用户,构成用户敏感信息的所有基本元素可以为数字、字符、字母或其任意组合;

(2)外部设备对构成用户敏感信息的所有基本元素进行逐个加密,以得到每个基本元素对应的密文数据,并将该密文数据及相应的布局方式发送给主机;

(3)主机存储接收到的密文数据及布局方式,以统一的符号、字母或数字替换密文数据中的所有元素,并以与步骤(1)中外部设备相同的布局方式将替换后的所有元素显示给用户;

(4)主机接收用户通过查看外部设备屏幕上显示的基本元素及其布局后输入的用户敏感信息,记录该用户敏感信息对应的密文数据,并将该密文数据发送到外部设备;

(5)外部设备采用与步骤(3)的加密算法相对应的解密算法对来自主机的密文数据进行解密操作,从而得到用户真实输入的用户敏感信息。

2.根据权利要求1所述的保护方法,其特征在于,所述加密算法为古典加密中的替换加密算法,步骤(2)的具体实现过程是,依次对每个构成用户敏感信息的基本元素,在事先存储的字典中找到对应的字典元素,并将该字典元素作为该基本元素对应的加密结果,并判断得到的加密结果是否与之前的加密结果相同,如果不同,则建立二者之间的一对一映射关系,转入下一个基本元素,如果相同,则在字典中重新随机取一个字典元素,将随机取的该字典元素作为该基本元素对应的加密结果,重复上述步骤,直到所有构成用户敏感信息的基本元素都具有相应的密文数据为止。

3.根据权利要求1所述的保护方法,其特征在于,

所述加密算法为古典加密中的移位加密算法;

如果构成用户敏感信息基本元素的是纯数字,则经过移位加密算法处理后的加密结果等于(该数字+s)mod n,其中s表示移位的位数,n表示加密采用的进制的位数;

如果构成用户敏感信息基本元素的是字母,则经过移位加密算法处理后的加密结果是(该字母的序号+s)mod 26;

如果构成用户敏感信息基本元素是字符,则先对所有字符进行有序数字编码,随后经过移位加密算法处理后的加密结果等于(该字符对应的数字+s)mod n。

4.一种用户敏感信息的保护方法,其特征在于,包括以下步骤:

(1)外部设备对构成用户敏感信息的所有基本元素进行随机布局,并将布局方式通过屏幕显示给用户,构成用户敏感信息的所有基本元素可以为数字、字符、字母或其任意组合;

(2)外部设备生成随机密钥,利用随机密钥对构成用户敏感信息的所有基本元素进行逐个流密码加密,以得到每个基本元素对应的密文数据,并将该密文数据及相应的布局方式发送给主机;

(3)主机存储接收到的密文数据及布局方式,以统一的符号、字母或数字替换密文数据中的所有元素,并以与步骤(1)中外部设备相同的布局方式将替换后的所有元素显示给用户;

(4)主机接收用户通过查看外部设备屏幕上显示的明文数据对应输入的密文数据,并

将该密文数据发送到外部设备；

(5)外部设备采用与步骤(3)的加密算法相对应的解密算法对来自主机的密文数据进行解密操作，从而得到用户真实输入的敏感信息。

5.根据权利要求4所述的保护方法，其特征在于，步骤(2)的具体实现过程是，首先随机产生一个密钥，并将该密钥与构成用户敏感信息的第一个元素进行流加密运算，然后随机产生下一个密钥，并将随机产生的该下一个密钥与构成用户敏感信息的下一个元素进行流加密运算，并判断得到的运算结果是否与之前的加密结果相同，如果不同，则转入下一个元素并重复上述流加密运算步骤，如果相同，则再次随机产生密钥，并重复上述判断步骤和流加密运算步骤，以此类推，直到构成用户敏感信息的每一个基本元素都处理完毕为止，从而得到每一个元素对应的密文数据。

6.根据权利要求1至5中任意一项所述的保护方法，其特征在于，用户是通过查看外部设备屏幕上显示的基本元素布局，在主机上通过鼠标点击或者触摸步骤(3)的布局方式中该元素相应的位置，从而完成在主机上用户敏感信息的输入操作。

7.一种用户敏感信息的保护系统，其特征在于，包括：

第一模块，其设置于外部设备中，用于对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户，构成用户敏感信息的所有基本元素可以为数字、字符、字母或其任意组合；

第二模块，其设置于外部设备中，用于对构成用户敏感信息的所有基本元素进行逐个加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机；

第三模块，其设置于主机中，用于存储接收到的密文数据及布局方式，以统一的符号、字母或数字替换密文数据中的所有元素，并以与步骤(1)中外部设备相同的布局方式将替换后的所有元素显示给用户；

第四模块，其设置于主机中，用于接收用户通过查看外部设备屏幕上显示的基本元素及其布局后输入的用户敏感信息，记录该用户敏感信息对应的密文数据，并将该密文数据发送到外部设备；

第五模块，其设置于外部设备中，用于采用与步骤(3)的加密算法相对应的解密算法对来自主机的密文数据进行解密操作，从而得到用户真实输入的用户敏感信息。

8.一种用户敏感信息的保护系统，其特征在于，包括：

第一模块，其设置于外部设备中，用于对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户，构成用户敏感信息的所有基本元素可以为数字、字符、字母或其任意组合；

第二模块，其设置于外部设备中，用于生成随机密钥，利用随机密钥对构成用户敏感信息的所有基本元素进行逐个流密码加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机；

第三模块，其设置于主机中，用于存储接收到的密文数据及布局方式，以统一的符号、字母或数字替换密文数据中的所有元素，并以与步骤(1)中外部设备相同的布局方式将替换后的所有元素显示给用户；

第四模块，其设置于主机中，用于接收用户通过查看外部设备屏幕上显示的明文数据

对应输入的密文数据，并将该密文数据发送到外部设备；

第五模块，其设置于外部设备中，用于采用与步骤(3)的加密算法相对应的解密算法对来自主机的密文数据进行解密操作，从而得到用户真实输入的敏感信息。

9.根据权利要求7和8中任意一项所述的保护系统，其特征在于，外部设备是智能密钥设备、移动POS机或版权保护设备，主机是PC、笔记本电脑或手机。

一种用户敏感信息的保护方法和系统

技术领域

[0001] 本发明属于信息安全技术领域和互联网通信领域，更具体地，涉及一种用户敏感信息的保护方法和系统。

背景技术

[0002] 随着互联网和移动互联网的快速发展，网上信息及业务系统的安全防护问题日益突出，各政府部门或企事业单位为了保证身份认证或交易认证过程中用户的敏感信息不被窃取，往往采用专门的信息安全外设(例如智能密钥设备、智能卡等)配合主机实现登录或网上交易，目前用户的敏感信息(包括pin码、用户账号和密码、转账信息等)通常都是在主机端接收来自用户的录入，然后传送到外部设备，或在专用的信息安全外设上直接录入。

[0003] 然而，目前这种身份认证或交易认证系统存在两方面的技术问题：首先，目前通过主机接收用户录入敏感信息然后传送到外部设备的方式，敏感信息在录入的过程中必然会有明文出现在主机内存中的过程，从而导致敏感信息容易被黑客通过键盘劫持、内存攻击、截屏等方式非法盗取，给用户的使用带来巨大的安全风险；此外，通过专用的信息安全外设直接录入敏感信息的方式，需要信息安全外设具有键盘以供用户输入，这会增加信息安全外设的硬件成本。

发明内容

[0004] 针对现有技术的以上缺陷或改进需求，本发明提供了一种数据输入的保护方法和系统，其目的在于，解决现有身份认证或交易认证系统存在的敏感信息容易被黑客非法盗取，给用户的使用带来巨大的安全风险、以及由于需要为外部设备配置键盘所带来的硬件成本增加的技术问题。

[0005] 为实现上述目的，按照本发明的一个方面，提供了一种用户敏感信息的保护方法，包括以下步骤：

[0006] (1)外部设备对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户，构成用户敏感信息的所有基本元素可以为数字、字符、字母或其任意组合；

[0007] (2)外部设备对构成用户敏感信息的所有基本元素进行逐个加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机；

[0008] (3)主机存储接收到的密文数据及布局方式，以统一的符号、字母或数字替换密文数据中的所有元素，并以与步骤(1)中外部设备相同的布局方式将替换后的所有元素显示给用户；

[0009] (4)主机接收用户通过查看外部设备屏幕上显示的基本元素及其布局后输入的用户敏感信息，记录该用户敏感信息对应的密文数据，并将该密文数据发送到外部设备；

[0010] (5)外部设备采用与步骤(3)的加密算法相对应的解密算法对来自主机的密文数据进行解密操作，从而得到用户真实输入的用户敏感信息。

[0011] 优选地，所述加密算法为古典加密中的替换加密算法，步骤(2)的具体实现过程是，依次对每个构成用户敏感信息的基本元素，在事先存储的字典中找到对应的字典元素，并将该字典元素作为该基本元素对应的加密结果，并判断得到的加密结果是否与之前的加密结果相同，如果不同，则建立二者之间的一对一映射关系，转入下一个基本元素，如果相同，则在字典中重新随机取一个字典元素，将该字典元素作为该基本元素对应的加密结果，重复上述步骤，直到所有构成用户敏感信息的基本元素都具有相应的密文数据为止。

[0012] 优选地，所述加密算法为古典加密中的移位加密算法；如果构成用户敏感信息基本元素的是纯数字，则经过移位加密算法处理后的加密结果等于(该数字+s)mod n，其中s表示移位的位数，n表示加密采用的进制的位数，如果构成用户敏感信息基本元素的是字母，则经过移位加密算法处理后的加密结果是(该字母的序号+s)mod 26，如果构成用户敏感信息基本元素是字符，则先对所有字符进行有序数字编码，随后经过移位加密算法处理后的加密结果等于(该字符对应的数字+s)mod n。

[0013] 按照本发明的另一方面，提供了一种用户敏感信息的保护方法，包括以下步骤：

[0014] (1)外部设备对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户，构成用户敏感信息的所有基本元素可以为数字、字符、字母或其任意组合；

[0015] (2)外部设备生成随机密钥，利用随机密钥对构成用户敏感信息的所有基本元素进行逐个流密码加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机；

[0016] (3)主机存储接收到的密文数据及布局方式，以统一的符号、字母或数字替换密文数据中的所有元素，并以与步骤(1)中外部设备相同的布局方式将替换后的所有元素显示给用户；

[0017] (4)主机接收用户通过查看外部设备屏幕上显示的明文数据对应输入的密文数据，并将该密文数据发送到外部设备；

[0018] (5)外部设备采用与步骤(3)的加密算法相对应的解密算法对来自主机的密文数据进行解密操作，从而得到用户真实输入的敏感信息。

[0019] 优选地，步骤(2)的具体实现过程是，首先随机产生一个密钥，并将该密钥与构成用户敏感信息的第一个元素进行流加密运算，然后随机产生下一个密钥，并将该密钥与构成用户敏感信息的下一个元素进行流加密运算，并判断得到的运算结果是否与之前的加密结果相同，如果不同，则转入下一个元素并重复上述流加密运算步骤，如果相同，则再次随机产生密钥，并重复上述判断步骤和流加密运算步骤，以此类推，直到构成用户敏感信息的每一个基本元素都处理完毕为止，从而得到每一个元素对应的密文数据。

[0020] 优选地，用户是通过查看外部设备屏幕上显示的基本元素布局，在主机上通过鼠标点击或者触摸步骤(3)的布局方式中该元素相应的位置，从而完成在主机上用户敏感信息的输入操作。

[0021] 按照本发明的另一方面，提供了一种用户敏感信息的保护系统，包括：

[0022] 第一模块，其设置于外部设备中，用于对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户，构成用户敏感信息的所有基本元素可以为数字、字符、字母或其任意组合；

[0023] 第二模块，其设置于外部设备中，用于对构成用户敏感信息的所有基本元素进行逐个加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机；

[0024] 第三模块，其设置于主机中，用于存储接收到的密文数据及布局方式，以统一的符号、字母或数字替换密文数据中的所有元素，并以与步骤(1)中外部设备相同的布局方式将替换后的所有元素显示给用户；

[0025] 第四模块，其设置于主机中，用于接收用户通过查看外部设备屏幕上显示的基本元素及其布局后输入的用户敏感信息，记录该用户敏感信息对应的密文数据，并将该密文数据发送到外部设备；

[0026] 第五模块，其设置于外部设备中，用于采用与步骤(3)的加密算法相对应的解密算法对来自主机的密文数据进行解密操作，从而得到用户真实输入的用户敏感信息。

[0027] 按照本发明的另一方面，提供了一种用户敏感信息的保护系统，包括：

[0028] 第一模块，其设置于外部设备中，用于对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户，构成用户敏感信息的所有基本元素可以为数字、字符、字母或其任意组合；

[0029] 第二模块，其设置于外部设备中，用于生成随机密钥，利用随机密钥对构成用户敏感信息的所有基本元素进行逐个流密码加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机；

[0030] 第三模块，其设置于主机中，用于存储接收到的密文数据及布局方式，以统一的符号、字母或数字替换密文数据中的所有元素，并以与步骤(1)中外部设备相同的布局方式将替换后的所有元素显示给用户；

[0031] 第四模块，其设置于主机中，用于接收用户通过查看外部设备屏幕上显示的明文数据对应输入的密文数据，并将该密文数据发送到外部设备；

[0032] 第五模块，其设置于外部设备中，用于采用与步骤(3)的加密算法相对应的解密算法对来自主机的密文数据进行解密操作，从而得到用户真实输入的敏感信息。

[0033] 优选地，外部设备是智能密钥设备、移动POS机或版权保护设备，主机是PC、笔记本电脑或手机。

[0034] 总体而言，通过本发明所构思的以上技术方案与现有技术相比，能够取得下列有益效果：

[0035] (1)由于在本发明方法中，用户的敏感信息并不会直接显示在主机的屏幕上(显示在主机屏幕上的是统一的符号、字母或数字)，也不会出现在主机的内存中，因此黑客无法通过键盘劫持、内存攻击、截屏等方式非法盗取用户的敏感信息，从而增加了用户使用时的安全性。

[0036] (2)在本发明中，外部设备不需要配备键盘供用户输入，用户仅仅只需要通过点击鼠标或者触摸屏的方式即可完成在主机屏幕上的明文数据输入操作，从而降低了外部设备的硬件成本。

附图说明

[0037] 图1是根据本发明第一实施方式的用户敏感信息的保护方法的流程图。

[0038] 图2是根据本发明第二实施方式的用户敏感信息的保护方法的流程图。

具体实施方式

[0039] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。此外，下面所描述的本发明各个实施方式中所涉及到的技术特征只要彼此之间未构成冲突就可以相互组合。

[0040] 如图1所示，本发明用户敏感信息的保护方法包括以下步骤：

[0041] (1)外部设备对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户，构成用户敏感信息的所有基本元素可以为数字、字符、字母或其任意组合；具体而言，当用户敏感信息为纯数字时，则构成其的所有基本元素为数字0到数字9，当用户敏感信息还包含字母时，则构成其的所有基本元素还应包括大小写的字母a至z，当用户敏感信息还包括特殊字符时，则构成其的所有基本元素还应包括键盘上常用的字符，诸如～、!、@、#、$、%、^、&、*、(、)、-、+、{、}、:、“、<、>、?、[、]等。

[0042] 在本实施方式中，外部设备是智能密钥设备、移动POS机(MPOS)、版权保护设备等信息安全外设。

[0043] 构成用户敏感信息的所有基本元素显示时的布局方式可以是任意的，比如显示为一行、一列或者矩阵形式。

[0044] 例如，构成纯数字用户敏感信息的所有基本元素随机布局并显示的方式是

[0045]

9	5	3
2	1	8
7	6	4
	0	

[0046] (2)外部设备对构成用户敏感信息的所有基本元素进行逐个加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机；在本实施方式中，主机是带键盘输入的PC、笔记本电脑、手机等。

[0047] 具体而言，所使用的加密算法包括有古典加密中的替换加密算法、移位加密算法或其组合；

[0048] 例如，针对步骤(1)中的例子，使用替换加密算法、移位加密算法或其组合后，数字0到数字9对应的密文数据分别是：

[0049] 0-ab

[0050] 1-3b

[0051] 2-f5

[0052] 3-e5

[0053] 4-cc

[0054] 5-a2

[0055] 6-aa

[0056] 7-dd

[0057] 8-4a

[0058] 9-c1

[0059] 其相应的排列布局方式为：

[0060]

c1	a2	e5
f5	3b	4a
dd	aa	cc
	ab	

[0061] 当采用古典加密中的替换加密算法时，本步骤的具体实现过程是，依次对每个构成用户敏感信息的基本元素，在事先存储的字典(其中建立有构成用户敏感信息基本元素与事先存储在字典中的字典元素之间的一对一映射关系)中找到对应的字典元素，并将该字典元素作为该基本元素对应的加密结果，并判断得到的加密结果是否与之前的加密结果相同，如果不同，则建立二者之间的一对一映射关系，转入下一个基本元素，如果相同，则在字典中重新随机取一个字典元素，将该字典元素作为该基本元素对应的加密结果，重复上述步骤，直到所有构成用户敏感信息的基本元素都具有相应的密文数据为止。

[0062] 当采用古典加密中的移位加密算法时，如果构成用户敏感信息基本元素的是纯数字，则经过移位加密算法处理后的加密结果等于(该数字+s)mod n，其中s表示移位的位数，其为任意自然数，n表示加密采用的进制的位数。

[0063] 针对上述实例而言，针对元素5而言，如果移位的位数是2，并采用十进制加密，则加密结果是等于(5+2)mod 10＝7。

[0064] 如果构成用户敏感信息基本元素的是字母，则经过移位加密算法处理后的加密结果是(该字母的序号+s)mod 26，其中s表示移位的位数，其为任意自然数。

[0065] 如果构成用户敏感信息基本元素是字符，则先对所有字符进行有序数字编码，随后经过移位加密算法处理后的加密结果等于(该字符对应的数字+s)mod n，其中s表示移位的位数，其为任意自然数，n表示所有字符的个数。

[0066] 如图2所示，作为另一个替换实施方式，本步骤也可以是：

[0067] (2’)外部设备生成随机密钥，利用随机密钥对构成用户敏感信息的所有基本元素进行逐个流密码加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机；

[0068] 具体而言，流密码加密运算包括异或、RC-4、SEAL算法等。

[0069] 本步骤的具体实现过程是，首先随机产生一个密钥，并将该密钥与构成用户敏感信息的第一个元素进行流加密运算，然后随机产生下一个密钥，并将该密钥与构成用户敏感信息的下一个元素进行流加密运算，并判断得到的运算结果是否与之前的加密结果相同，如果不同，则转入下一个元素并重复上述流加密运算步骤，如果相同，则再次随机产生密钥，并重复上述判断步骤和流加密运算步骤，以此类推，直到构成用户敏感信息的每一个基本元素都处理完毕为止，得到每一个元素对应的密文数据。

[0070] 针对上述实例而言，本步骤中首先生成加密密钥：

[0071]

1	1	1
1	1	1
1	1	1
	1	

[0072] 然后将该加密密钥和步骤(1)中的基本元素数据进行异或,得到密文的排列布局为:

[0073]

8	4	2
3	0	9
6	7	5
	1	

[0074] (3)主机存储接收到的密文数据及布局方式,以统一的符号、字母或数字替换密文数据中的所有元素,并以与步骤(1)中外部设备相同的布局方式将替换后的所有元素显示给用户;

[0075] (4)主机接收用户通过查看外部设备屏幕上显示的基本元素及其布局后输入的用户敏感信息,记录该用户敏感信息对应的密文数据,并将该密文数据发送到外部设备;具体而言,用户是通过查看外部设备屏幕上显示的基本元素布局,在主机上通过鼠标点击或者触摸步骤(3)的布局方式中该元素相应的位置,从而完成在主机上用户敏感信息的输入操作;

[0076] 例如,用户需要输入的pin码是5132,则主机接收到的密文数据就是a2,3b,e5,f5(如果是采用替换加密算法)。

[0077] (5)外部设备采用与步骤(3)的加密算法相对应的解密算法对来自主机的密文数据进行解密操作,从而得到用户真实输入的用户敏感信息。

[0078] 本领域的技术人员容易理解,以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等,均应包含在本发明的保护范围之内。

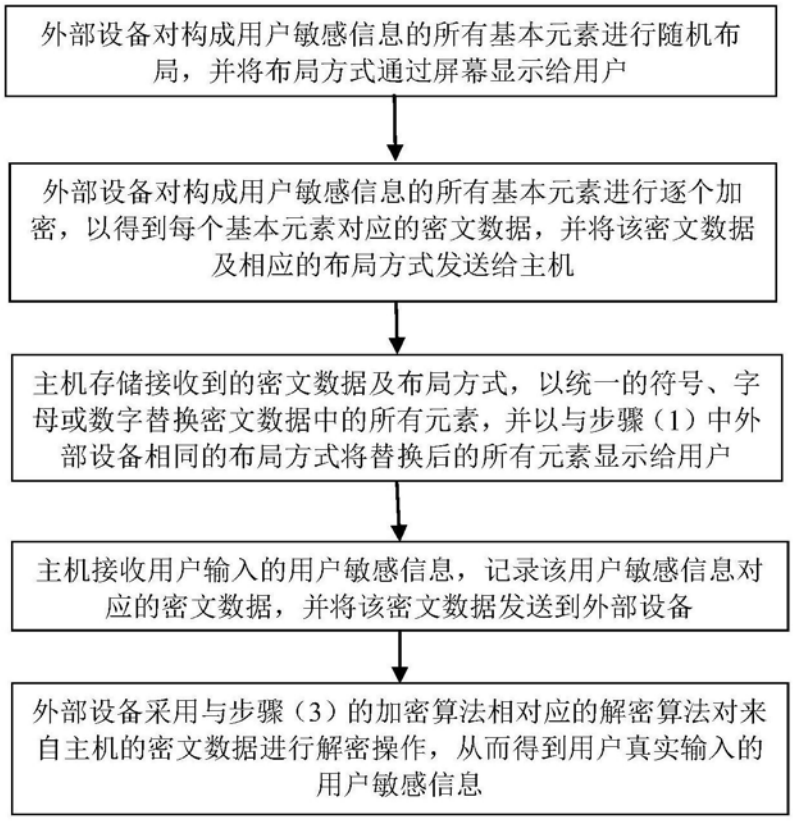

外部设备对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户
外部设备对构成用户敏感信息的所有基本元素进行逐个加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机
主机存储接收到的密文数据及布局方式，以统一的符号、字母或数字替换密文数据中的所有元素，并以与步骤（1）中外部设备相同的布局方式将替换后的所有元素显示给用户
主机接收用户输入的用户敏感信息，记录该用户敏感信息对应的密文数据，并将该密文数据发送到外部设备
外部设备采用与步骤（3）的加密算法相对应的解密算法对来自主机的密文数据进行解密操作，从而得到用户真实输入的用户敏感信息

图1

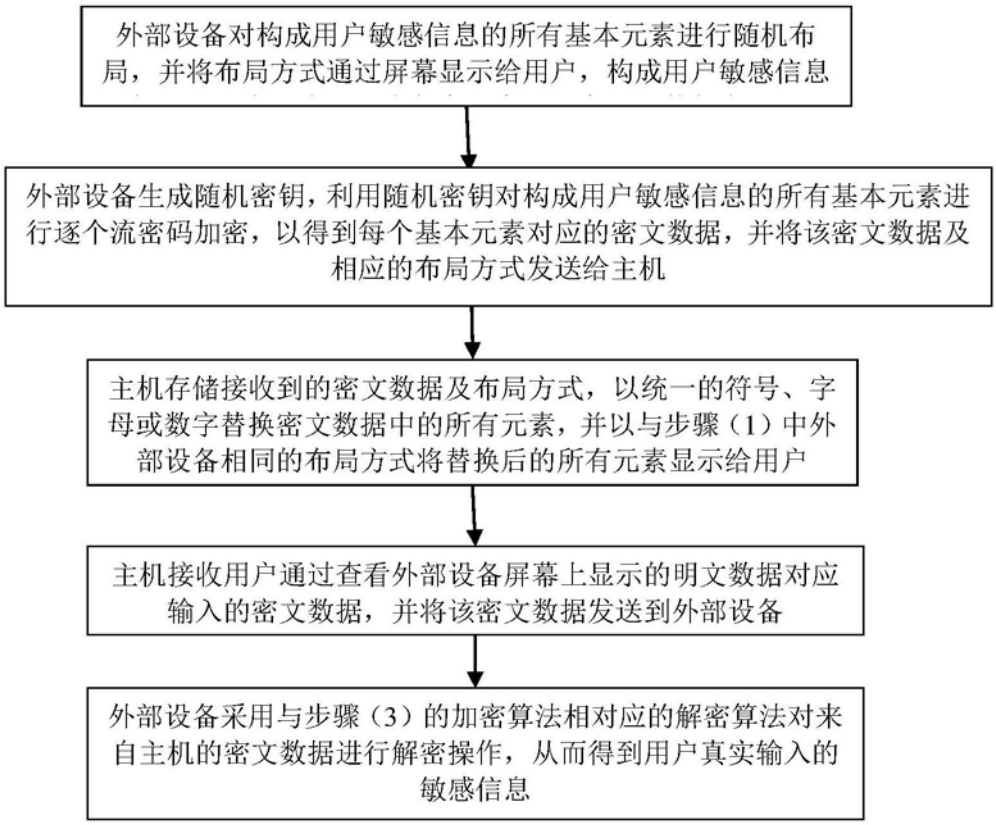

外部设备对构成用户敏感信息的所有基本元素进行随机布局，并将布局方式通过屏幕显示给用户，构成用户敏感信息
外部设备生成随机密钥，利用随机密钥对构成用户敏感信息的所有基本元素进行逐个流密码加密，以得到每个基本元素对应的密文数据，并将该密文数据及相应的布局方式发送给主机
主机存储接收到的密文数据及布局方式，以统一的符号、字母或数字替换密文数据中的所有元素，并以与步骤（1）中外部设备相同的布局方式将替换后的所有元素显示给用户
主机接收用户通过查看外部设备屏幕上显示的明文数据对应输入的密文数据，并将该密文数据发送到外部设备
外部设备采用与步骤（3）的加密算法相对应的解密算法对来自主机的密文数据进行解密操作，从而得到用户真实输入的敏感信息

图2