(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 102419805 B
(45)授权公告日 2015.05.20

(21)申请号 201110373961.3
(22)申请日 2011.11.22
(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部
(72)发明人 唐贵杰 韩辰 雷春雪 李春雨 谢群
(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国
(51)Int.Cl.
G06F 21/32(2013.01)

(56)对比文件
CN 102123027 A,2011.07.13,
CN 101236591 A,2008.08.06,
US 2003/0051138 A1,2003.03.13,
CN 1893713 A,2007.01.10,

审查员 吴琼

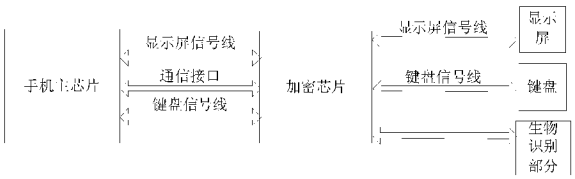
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种终端设备及其用户信息加密方法

(57)摘要

一种终端设备及其用户信息加密方法。所述终端设备包括加密芯片和终端主体；所述终端主体采集用户生物信息和用户私密信息；所述加密芯片对所述用户私密信息以所述生物识别信息为密钥通过加密算法加密，并将加密后的信息发送给终端主体存储。采用本发明的技术方案，MID可以根据不同的外界光照环境，更改显示策略，从而增加用户的视觉感官满意度，提高产品性能。采用加密芯片的硬件解决方案，速度和性能都优于软件方法；采用生物识别技术，不需要用户记忆任何密码；所有加密，解密，显示，输入等操作过程都在加密芯片内部完成，不需要通过手机，避免了手机中病毒或者木马导致的信息泄露。



CN 102419805 B

1. 一种终端设备，其特征在于，所述终端设备包括加密芯片和终端主体；

所述终端主体提示用户输入需加密的用户私密信息对应的明细信息，其中，所述终端主体包括终端主芯片和键盘；

所述终端主体通知所述加密芯片进入加密状态，并提示用户输入用户生物信息；

所述加密芯片断开终端主芯片与键盘的连接；

所述加密芯片采集用户输入的用户生物信息；

所述终端主体提示用户输入需加密的用户私密信息，所述加密芯片采集用户输入的所述用户私密信息；

所述加密芯片对所述用户私密信息以用户生物信息为密钥通过加密算法加密，并将加密后的信息发送给终端主体存储。

2. 如权利要求 1 所述的终端设备，其特征在于，当用户需要解密其用户私密信息时，再次输入相同的用户生物信息，加密芯片以该用户生物信息为密钥解密所述加密后的信息并解密出用户私密信息。

3. 如权利要求 1 所述的终端设备，其特征在于，所述加密芯片包含终端屏幕控制模块、加密算法模块、与终端主芯片通信的模块、输入控制模块和生物识别信息输入模块；

所述终端屏幕控制模块用于将用户私密信息输出到终端显示屏上；

所述加密算法模块用于对用户私密信息加密；

所述与终端主芯片通信的模块用于和终端主芯片通信；

所述输入控制模块用于控制信息输入和接收信息输入；

所述生物识别信息输入模块用于采集用户生物信息并识别用户生物信息。

4. 如权利要求 1 所述的终端设备，其特征在于，所述加密算法是 AES、DES、RSA、MD5 之一种或组合。

5. 如权利要求 1 所述的终端设备，其特征在于，所述用户生物信息是指纹信息、虹膜信息、面部信息、静脉信息、耳纹信息之一种或组合。

6. 一种用户信息加密方法，其特征在于，所述加密方法包括：

终端主体提示用户输入需加密的用户私密信息对应的明细信息，其中，所述终端主体包括终端主芯片和键盘；

所述终端主体通知加密芯片进入加密状态，并提示用户输入用户生物信息；

所述加密芯片断开终端主芯片与键盘的连接；

所述加密芯片采集用户输入的用户生物信息；

所述终端主体提示用户输入需加密的用户私密信息，所述加密芯片采集用户输入的所述用户私密信息；

通过加密芯片对所述用户私密信息以用户生物信息为密钥采用加密算法加密，并将加密后的信息发送给终端主体存储。

7. 如权利要求 6 所述的方法，其特征在于，当用户需要解密其用户私密信息时，再次输入相同的用户生物信息，加密芯片以该用户生物信息作为密钥解密所述加密后的信息并解密出用户私密信息。

8. 如权利要求 6 所述的方法，其特征在于，所述加密芯片包含终端屏幕控制模块、加密算法模块、与终端主芯片通信的模块、输入控制模块和生物识别信息输入模块；

所述终端屏幕控制模块用于将用户私密信息输出到终端显示屏上；

所述加密算法模块用于对用户私密信息加密；

所述与终端主芯片通信的模块用于和终端主芯片通信；

所述输入控制模块用于控制信息输入和接受信息输入；

所述生物识别信息输入模块用于采集用户生物信息并识别用户生物信息。

9. 如权利要求 6 所述的方法，其特征在于，所述加密算法是 AES、DES、RSA、MD5 之一种或组合。

10. 如权利要求 6 所述的方法，其特征在于，所述用户生物信息是指纹信息、虹膜信息、面部信息、静脉信息、耳纹信息之一种或组合。

一种终端设备及其用户信息加密方法

技术领域

[0001] 本发明涉及通信技术领域，更具体地，涉及一种终端设备及其用户信息加密方法。

背景技术

[0002] 人们生活在现代社会，每天都会和不同类型的密码打交道，工作电脑的开机密码，银行信用卡的密码，个人电子邮箱的登录密码，各种注册网站的密码，网络银行的密码，证券交易密码等等，可以说我们生活在一个被密码包围的环境。虽然每种密码的长度、位数、种类各不相同。但是任何一种密码泄露或丢失都会造成用户的巨大损失。

[0003] 目前大部分用户都采用一些对自己比较特别的数字或名称作为密码，例如生日、电话号码、身份证号、名字等。而且很多人为了使密码简单容易记忆，都会采用同一密码来应对不同的应用，例如多张银行卡共用一个密码等等。从密码学的角度，以上种种建立密码的方式都会带来巨大的隐患。别有用心的人很容易通过穷举，字典攻击的方法破解强度较弱的密码，获得用户的机密信息，窃取用户的财产和个人隐私。因此，用户密码最好采用不易被破解和猜测到的数字或名称，且各种密码最好不要相同或相近似，如此，才能更有效的保护用户密码，但这样，又带来一个问题，那就是用户面对如此繁杂且多的密码往往可能会忘记。

发明内容

[0004] 为弥补上述不足，本发明提出一种终端设备，所述终端设备包括加密芯片和终端主体；

[0005] 所述终端主体采集用户生物信息和用户私密信息；

[0006] 所述加密芯片对所述用户私密信息以所述生物识别信息为密钥通过加密算法加密，并将加密后的信息发送给终端主体存储。

[0007] 进一步地，当用户需要解密其用户私密信息时，可再次输入相同的用户生物信息，加密芯片以该用户生物信息为密钥解密所述加密信息并解密出用户私密信息。

[0008] 进一步地，所述加密芯片包含终端屏幕控制模块、加密算法模块、与终端主芯片通信的模块、输入控制模块和生物识别信息输入模块；

[0009] 所述终端屏幕控制模块用于将私密信息输出到终端显示屏上；

[0010] 所述加密算法模块用于对用户私密信息加密；

[0011] 所述与终端主芯片通信的模块用于和终端主芯片通信；

[0012] 所述输入控制模块用于控制信息输入和接收信息输入；

[0013] 所述生物识别信息输入模块用于采集生物信息并识别生物信息。

[0014] 进一步地，所述加密算法是 AES、DES、RSA、MD5 之一种或组合。

[0015] 进一步地，所述用户生物信息是指纹信息、虹膜信息、面部信息、静脉信息、耳纹信息之一种或组合。

[0016] 本发明提出一种用户信息加密方法，所述加密方法包括：用户终端主体采集用户

生物信息和用户私密信息；通过加密芯片对所述用户私密信息以所述生物识别信息为密钥采用加密算法加密，并将加密后的信息发送给终端主体存储。

[0017] 进一步地，当用户需要解密其用户私密信息时，可再次输入相同的用户生物信息，加密芯片以该用户生物信息作为密钥解密所述加密信息并解密出用户私密信息。

[0018] 进一步地，所述加密芯片包含终端屏幕控制模块、加密算法模块、与终端主芯片通信的模块、输入控制模块和生物识别信息输入模块；

[0019] 所述终端屏幕控制模块用于将私密信息输出到终端显示屏上；

[0020] 所述加密算法模块用于对用户私密信息加密；

[0021] 所述与终端芯片的通信模块用于和终端主芯片通信；

[0022] 所述输入控制模块用于控制信息输入和接受信息输入；

[0023] 所述生物识别信息输入模块用于采集生物信息并识别生物信息。

[0024] 进一步地，所述加密算法是 AES、DES、RSA、MD5 之一种或组合。

[0025] 进一步地，所述用户生物信息是指纹信息、虹膜信息、面部信息、静脉信息、耳纹信息之一种或组合。

[0026] 综上所述，采用本发明具有如下有益效果：

[0027] 采用加密芯片的硬件解决方案，速度和性能都优于软件方法；采用生物识别技术，不需要用户记忆任何密码；所有加密，解密，显示，输入等操作过程的都在加密芯片内部完成，不需要通过手机，避免了手机中病毒或者木马导致的信息泄露。

附图说明

[0028] 图 1 是本发明实施例终端设备结构示意图；

[0029] 图 2 是本发明实施例用户信息加密方法流程图；

[0030] 图 3 是本发明实施例用户信息解密方法流程图。

具体实施方式

[0031] 本发明克服现有技术中存在的加密和解密过程都依赖于手机中的软件运行，如果用户的手机被植入病毒和木马程序，就可以监视用户手机内存中的信息，窃取用户输入的密码（密钥）或者解密后输出的密码，给用户造成重大的财产经济损失。

[0032] 本发明包含加密芯片和终端主体两部分。加密芯片内置的加密算法可以是 AES(Advanced Encryption Standard)、DES(Data Encryption Standard)、RSA(Rivest Shamir and Adleman)、MD5(Message Digest Algorithm) 等多种加密方法之一种或组合，本发明只是以 AES128 算法为例进行说明。

[0033] AES 加密算法的密钥为生物信息识别模块提取的，与用户身份构成唯一识别的一段特征码。应当注意的是生物信息识别模块采用的生物信息识别方法可以是指纹识别、虹膜识别、面部识别、静脉识别、耳纹识别等多种方法之一种或组合，本发明只是以指纹识别为例进行说明。

[0034] 加密芯片目前通过 FPGA 实现，包含五个模块：手机屏幕控制模块、AES 加密算法模块、与手机主芯片通信的模块、键盘控制模块和生物识别信息输入模块。

[0035] AES 加密算法通过 FPGA 内部编程的硬件电路实现，AES 加密算法的密钥为用户输

入的唯一的生物识别信息。为了不经过手机部分，所以用户输入生物识别信息输入到加密芯片内部，同样出于安全原因，输出解密后的密码也不需要经过手机主控程序，直接通过加密芯片内的手机屏幕控制模块输出到手机显示屏上。

[0036] 下面结合附图和具体实施例对本发明技术方案做进一步详细描述。下面实施例中，本发明终端设备以手机为例进行说明。

[0037] 如图 1 所示，本发明实施例终端设备结构示意图，所述终端设备由手机主体和加密芯片两部分组成，其中显示屏和键盘属于手机主体部分，就是通常采用的显示屏和键盘，通过相应的信号线经由加密芯片连接到手机主芯片，正常工作时加密芯片相当于通路作用，不会对手机的正常输入和显示造成影响。手机主芯片通过通信接口与加密芯片进行信息交换。

[0038] 加密芯片目前通过 FPGA 实现，包含五个模块：手机屏幕控制模块、AES 加密算法模块、与手机主芯片的通信模块、键盘控制模块和生物识别信息输入模块。

[0039] 所述手机屏幕控制模块用于将输出密码输出到手机显示屏上。

[0040] 所述 AES 加密算法模块用于对用户信息加密。

[0041] 所述与手机主芯片的通信模块用于和手机主芯片通信。

[0042] 所述键盘控制模块用于控制键盘输入和接受键盘输入。

[0043] 所述生物识别信息输入模块用于采集生物信息并识别生物信息。

[0044] 请参考图 2 所示，是本发明实施例用户信息加密方法流程图，其包括如下步骤：

[0045] S201：首先提示用户输入需要建立密码的明细信息；

[0046] 例如用户需要建立一个招商银行卡的密码信息，输入“招商银行卡”。

[0047] S202：手机通过通信接口通知加密芯片进入加密状态，并提示用户输入唯一密码（密钥）；

[0048] S203：加密芯片断开手机与键盘的连接；

[0049] S204：用户输入生物识别信息，例如指纹信息；

[0050] S205：加密芯片向手机主芯片发出信息，通知手机显示屏显示提示用户输入密码；

[0051] S206：加密芯片将用户输入的密码进行加密处理；

[0052] S207：加密处理后的信息发送给手机芯片与明细信息一一对应存储。

[0053] 在上述步骤中，手机提示用户进行指纹识别信息的输入工作，同时加密芯片切断键盘等输入装置与手机的连接，通常键盘与主芯片的通信这时用户可以输入相应的密码，通常银行卡的密码为 6 位数字。每位数字占用空间为一个字节（8 比特）完成输入后 6 个数字就储存在加密芯片内部，需要用户输入两次，以便确认密码输入无误。6 个数字占有 48 比特的空间，AES 加密算法需要至少输入 128 比特数据，所以要想对 48 比特的数据进行加密，需要对密码数据进行填充。填充的方式可选为全零或其他规定好的方式。通常各类密码占用空间都小于 16 字节（128 比特），所以本发明只需要进行一次 AES 算法即可完成对一个密码的加密过程。加密芯片将加密后的数据通过通信接口发送给手机，并与用户输入的密码信息“招商银行卡”一一对应储存。需要说明的是如果用户需要输入字母数字混合的密码处理方式，首先需要说明的是手机默认的输入模式为数字方式，这时手机需要通过通信接口通知加密芯片，如果按下键盘的某个键，则输入模式切换为字母方式；然后加密芯片

对键盘输入的信息进行判定，如果切换键被键入，则加密芯片不拦截键盘输入，保证输入方式切换为字母方式，如果其他按键被输入则加密芯片截取相应的输入信息，并保存。通过鉴别切换键的方法可以控制加密芯片识别用户输入的是字母还是数字，并将其对应的信息保存在加密芯片内，每次成功输入一个密码后，加密芯片都会通过通信接口，提示手机显示应经输入了多少位密码。用户完成密码输入后，再经过 AES 算法加密后发送给手机。

[0054] 请参看图 3 所示，是本发明实施例用户信息解密方法流程图，其包括如下步骤：

[0055] S301：手机提示用户选择需要查询密码的明细信息；

[0056] S302：手机通过通信接口将与明细信息对应的加密信息发送给加密芯片，并通知其进入解密状态，并提示用户输入唯一密码（密钥）；

[0057] S303：用户输入生物识别信息；

[0058] S304：加密芯片利用用户输入的密钥和手机发送的加密信息进行解密操作；

[0059] S305：加密芯片断开手机与屏幕的连接；

[0060] S306：加密芯片将解密后的密码显示到手机屏幕。

[0061] 上述流程中，首先需要用户选择需要输出密码的明细信息，然后将与用户所选择明细信息对应的加密信息通过通信接口发送给加密芯片，同时通过手机显示屏提示用户输入指纹识别信息，在接收到用户输入的指纹识别信息后，加密芯片对从手机输入的加密信息进行解密（密钥为用户输入的指纹识别信息）。并中断手机显示屏与手机的电气信号连接，由加密芯片接管对手机显示屏的控制，将解密后的密码显示到手机显示屏上。可以设置通过显示时间，比如显示 1 分钟后，加密芯片退出对显示屏的控制，并清空相应的储存密码明文的储存器，返回到再次接收手机发送加密信息的状态。显示密码明文时，因为原始密码可能因为位数不足而经过填充处理，需要用户判断如果出现连续的零并以零收尾的部分密码明文信息，不是用户输入的密码信息。

[0062] 需要注意的是前面举例说明都是以带有全键盘输入的手机为例，如果用户使用的是触控屏手机，则触控屏与手机的连接类似键盘与手机的连接，实现原理也类似，只不过需要加密芯片对触控屏的数据进行解析，如果按下触控屏的某个区域，则输入模式切换为字母方式；加密芯片通过对输入的触控屏区域信息进行判定，如果切换键区域被触发，则加密芯片不拦截键盘输入，保证输入方式切换为字母方式，如果其他按键被输入则加密芯片截取相应的输入信息，并保存。通过鉴别切换键触发区域的方法可以控制加密芯片识别用户输入的是字母还是数字，并将其对应的信息保存在加密芯片内，完成密码输入后，再经过 AES 算法加密后发送给手机。

[0063] 该设计方案综合使用指纹识别技术，AES 加密算法提供了很高的安全标准，加密解密过程依赖于硬件加密芯片实现，没有通过手机软件进行，保证了所有密码信息明文不进入手机内存或相关外部存储器，不会被手机植入的木马程序或病毒窃取。

[0064] 本发明还可有多种实施方式，在不背离本发明精神及其实质的情况，熟悉本领域的技术人员当然可根据本发明做出各种相应的更改或变化，但凡在本发明的精神和原则之内所作的任何修改、等同替换、改进，均应包含在本发明的保护范围之内。

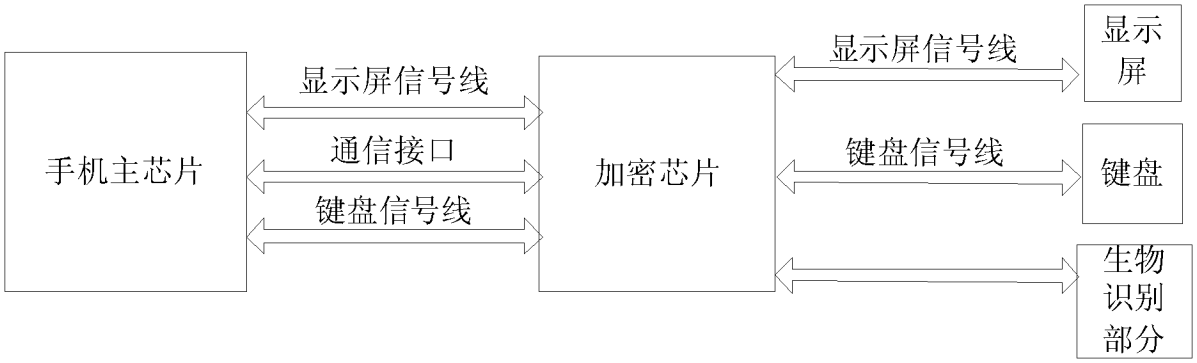

手机主芯片
显示屏信号线
通信接口
键盘信号线
加密芯片
显示屏信号线
显示屏
键盘信号线
键盘
生物识别部分

图 1

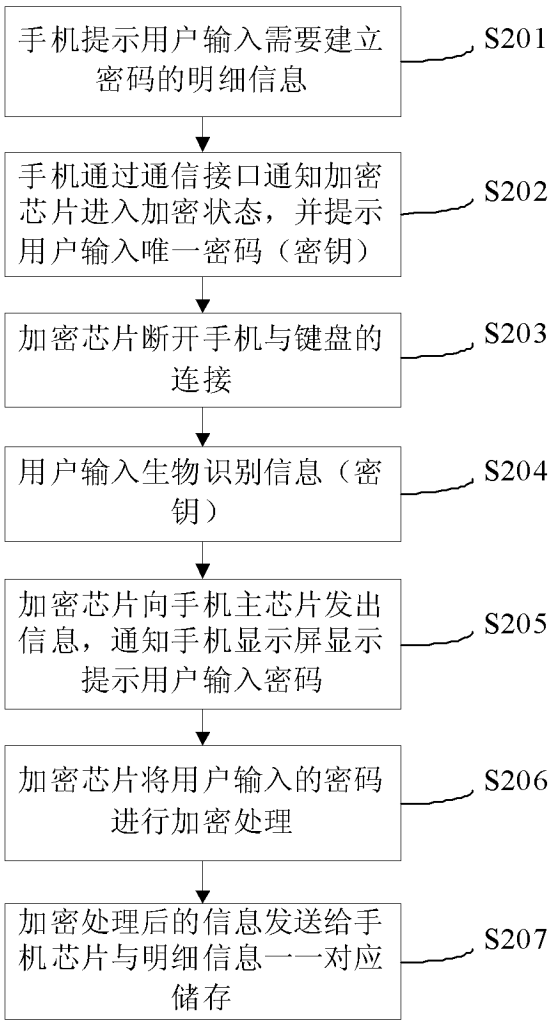

手机提示用户输入需要建立密码的明细信息
S201
手机通过通信接口通知加密芯片进入加密状态，并提示用户输入唯一密码（密钥）
S202
加密芯片断开手机与键盘的连接
S203
用户输入生物识别信息（密钥）
S204
加密芯片向手机主芯片发出信息，通知手机显示屏显示提示用户输入密码
S205
加密芯片将用户输入的密码进行加密处理
S206
加密处理后的信息发送给手机芯片与明细信息一一对应储存
S207

图 2

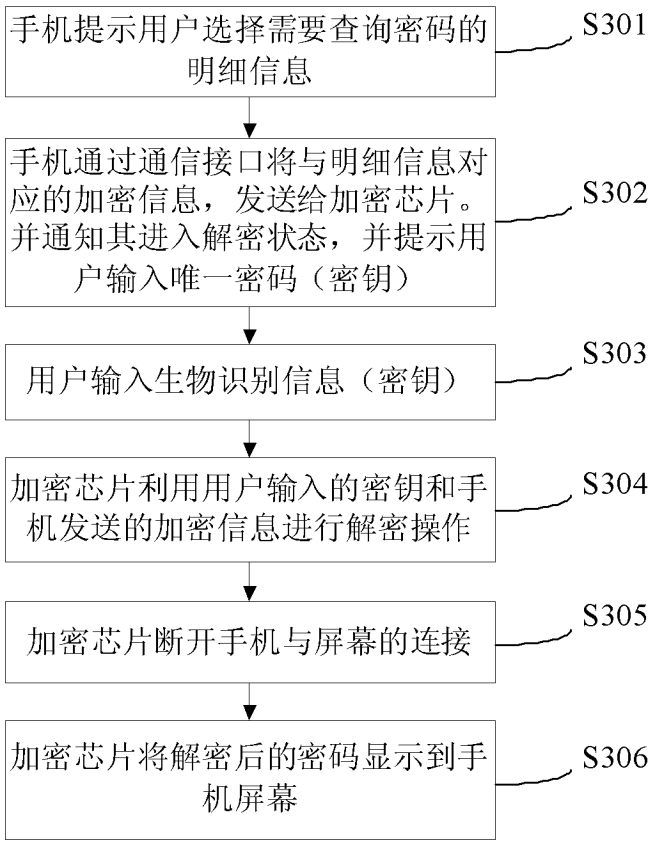

手机提示用户选择需要查询密码的明细信息
S301
手机通过通信接口将与明细信息对应的加密信息，发送给加密芯片。并通知其进入解密状态，并提示用户输入唯一密码（密钥）
S302
用户输入生物识别信息（密钥）
S303
加密芯片利用用户输入的密钥和手机发送的加密信息进行解密操作
S304
加密芯片断开手机与屏幕的连接
S305
加密芯片将解密后的密码显示到手机屏幕
S306

图 3