(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 103514390 A
(43)申请公布日 2014.01.15

(21)申请号 201310430771.X

(22)申请日 2013.09.18

(71)申请人 吴先洪
地址 518052 广东省深圳市南山区学府路198号华府花园2栋408室

(72)发明人 吴先洪

(74)专利代理机构 北京风雅颂专利代理有限公司 11403
代理人 李弘 李翔

(51)Int.Cl.
G06F 21/32(2013.01)

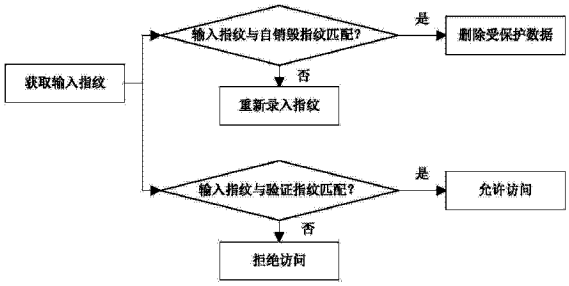
权利要求书1页 说明书3页 附图1页

(54)发明名称

数据自销毁方法、装置和数码设备

(57)摘要

本发明涉及一种数据自销毁方法、装置和数码设备。数据自销毁方法，包括：获取输入指纹；比较输入指纹与自销毁指纹是否匹配，如果匹配，则在不给出任何提示信息的情况下删除受保护数据。当所有人受到胁迫而必须打开存储设备时，由于已经预先注册了用于自动销毁存储设备中的数据的自销毁指纹，因此，只需要利用与该自销毁指纹相对应的手指进行指纹录入，即可在胁迫人毫不知情的情况下，自动删除其已获取的秘密数据，而此时胁迫人还认为所有人是在配合的情况下进行的操作，因而不会认为所有人曾经获取过秘密数据，可能从一定程度上保护所有人的人身安全。



CN 103514390 A

1. 一种数据自销毁方法，其特征在于，包括：

获取输入指纹；

比较所述输入指纹与自销毁指纹是否匹配，如果匹配，则在不给出任何提示信息的情况下删除受保护数据。

2. 根据权利要求 1 所述的数据自销毁方法，其特征在于，如果不匹配，则提示用户重新录入指纹。

3. 根据权利要求 1 所述的数据自销毁方法，其特征在于，还包括：

比较所述输入指纹与验证指纹是否匹配，如果匹配，则允许访问所述受保护数据。

4. 根据权利要求 1 所述的数据自销毁方法，其特征在于，还包括：如果不匹配，则提示用户重新录入指纹。

5. 一种数据自销毁装置，其特征在于，包括：

指纹获取模块，用于获取输入指纹；

自销毁处理模块，用于比较所述输入指纹与自销毁指纹是否匹配，如果匹配，则在不给出任何提示信息的情况下删除受保护数据。

6. 根据权利要求 5 所述的数据自销毁装置，其特征在于，所述自销毁处理模块还包括：

第一提示单元，用于在不匹配的情况下，提示用户重新录入指纹。

7. 根据权利要求 5 所述的数据自销毁装置，其特征在于，还包括：

验证处理模块，有于比较所述输入指纹与验证指纹是否匹配，如果匹配，则允许访问所述受保护数据。

8. 根据权利要求 5 所述的数据自销毁装置，其特征在于，所述验证处理模块还包括：

第二提示单元，用于在不匹配的情况下，提示用户重新录入指纹。

9. 一种数码设备，其特征在于，包括：存储单元，用于存储数据和用于对所述数据进行自销毁的自销毁指纹；还包括权利要求 5 至 8 中任一项所述的数据自销毁装置，其获取所述存储单元中存储的所述自销毁指纹。

数据自销毁方法、装置和数码设备

技术领域

[0001] 本发明涉及加密领域，特别是涉及一种数据自销毁方法、装置和数码设备。

背景技术

[0002] 数码相机、数码摄像机等的数据加密是已经很常见的功能，从而在设备遗失或未经许可的情况下，被他人非法访问。

[0003] 但是，对于某些情况来说，例如在受到胁迫时，设备所有人还是需要将密码告诉胁迫者，这样，胁迫者仍然能够顺利读取设备中的数据，给设备所有人的人身安全带来很大威胁。

发明内容

[0004] 本发明的目的是提供一种可自动销毁数据的数据自销毁方法、装置和数码设备。

[0005] 为解决上述技术问题，作为本发明的第一个方面，提供了一种数据自销毁方法，包括：获取输入指纹；比较输入指纹与自销毁指纹是否匹配，如果匹配，则在不给出任何提示信息的情况下删除受保护数据。

[0006] 进一步地，如果不匹配，则提示用户重新录入指纹。

[0007] 进一步地，还包括：比较输入指纹与验证指纹是否匹配，如果匹配，则允许访问受保护数据。

[0008] 进一步地，还包括：如果不匹配，则提示用户重新录入指纹。

[0009] 作为本发明的第二个方面，提供了一种数据自销毁装置，包括：指纹获取模块，用于获取输入指纹；自销毁处理模块，用于比较输入指纹与自销毁指纹是否匹配，如果匹配，则在不给出任何提示信息的情况下删除受保护数据。

[0010] 进一步地，自销毁处理模块还包括：第一提示单元，用于在不匹配的情况下，提示用户重新录入指纹。

[0011] 进一步地，还包括：验证处理模块，有于比较输入指纹与验证指纹是否匹配，如果匹配，则允许访问受保护数据。

[0012] 进一步地，验证处理模块还包括：第二提示单元，用于在不匹配的情况下，提示用户重新录入指纹。

[0013] 作为本发明的第三个方面，提供了一种数码设备，包括：存储单元，用于存储数据和用于对数据进行自销毁的自销毁指纹；还包括上述的数据自销毁装置，其获取存储单元中存储的自销毁指纹。

[0014] 当所有人受到胁迫而必须打开存储设备时，由于已经预先注册了用于自动销毁存储设备中的数据的自销毁指纹，因此，只需要利用与该自销毁指纹相对应的手指进行指纹录入，即可在胁迫人毫不知情的情况下，自动删除其已获取的秘密数据，而此时胁迫人还认为所有人是在配合的情况下进行的操作，因而不会认为所有人曾经获取过秘密数据，可能从一定程度上保护所有人的人身安全。

附图说明

[0015] 图 1 示意性示出了本发明的流程图。

具体实施方式

[0016] 以下对本发明的实施例进行详细说明，但是本发明可以由权利要求限定和覆盖的多种不同方式实施。

[0017] 作为本发明的第一方面，提供了一种数据自销毁方法，包括：获取输入指纹；比较输入指纹与自销毁指纹是否匹配，如果匹配，则在不给出任何提示信息的情况下删除受保护数据。优选地，如果不匹配，则提示用户重新录入指纹。

[0018] 当所有人受到胁迫而必须打开存储设备时，由于已经预先注册了用于自动销毁存储设备中的数据的自销毁指纹，因此，只需要利用与该自销毁指纹相对应的手指进行指纹录入，即可在胁迫人毫不知情的情况下，自动删除其已获取的秘密数据，而此时胁迫人还认为所有人是在配合的情况下进行的操作，因而不会认为所有人曾经获取过秘密数据，可能从一定程度上保护所有人的人身安全。

[0019] 优选地，还包括：比较输入指纹与验证指纹是否匹配，如果匹配，则允许访问受保护数据。优选地，还包括：如果不匹配，则提示用户重新录入指纹。

[0020] 当需要正常访问存储设备时，可以使用已经注册的验证指纹，当验证指纹通过验证后，即可正常访问数据设备。如果未通道，则可拒绝访问，但仍可保留存储设备中的秘密数据。

[0021] 作为本发明的第二方面，提供了一种数据自销毁装置，包括：指纹获取模块，用于获取输入指纹；自销毁处理模块，用于比较输入指纹与自销毁指纹是否匹配，如果匹配，则在不给出任何提示信息的情况下删除受保护数据。

[0022] 优选地，自销毁处理模块还包括：第一提示单元，用于在不匹配的情况下，提示用户重新录入指纹。

[0023] 优选地，还包括：验证处理模块，有于比较输入指纹与验证指纹是否匹配，如果匹配，则允许访问受保护数据。

[0024] 优选地，验证处理模块还包括：第二提示单元，用于在不匹配的情况下，提示用户重新录入指纹。

[0025] 作为本发明的第三方面，提供了一种数码设备，包括：存储单元，用于存储数据和用于对数据进行自销毁的自销毁指纹；还包括上述的数据自销毁装置，其获取存储单元中存储的自销毁指纹。

[0026] 例如，数码设备可以是指数码相机、摄像机、录音笔、平板电脑、手机、笔记本电脑、视频播放设备(例如 MP4 等)等现有技术中的各种便携式数码设备。

[0027] 显然，本发明中的数码设备，还可以是指现有技术中的各种便携式设备(例如数码相机、摄像机、录音笔、平板电脑、手机、笔记本电脑、视频播放设备(例如 MP4 等))及与该设备配合使用的电脑所构成的系统。此时，存储单元位于便携式设备中，而数据自销毁装置则位于电脑中。

[0028] 本领域技术人员还将明白的是，结合这里的公开所描述的各种示例性逻辑块、单

元、电路和算法步骤可以被实现为电子硬件、计算机软件或两者的组合。为了清楚地说明硬件和软件的这种可互换性，已经就各种示意性组件、方块、单元、电路和步骤的功能对其进行了一般性的描述。这种功能是被实现为软件还是被实现为硬件取决于具体应用以及施加给整个系统的设计约束。本领域技术人员可以针对每种具体应用以各种方式来实现所述的功能，但是这种实现决定不应被解释为导致脱离本发明的范围。

[0029] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

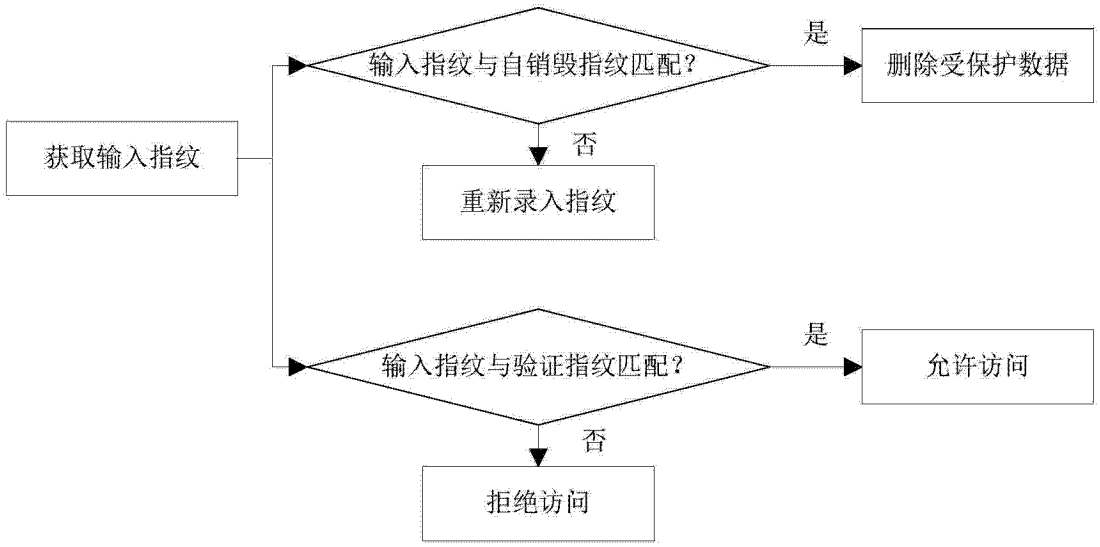

获取输入指纹
输入指纹与自销毁指纹匹配？
是
删除受保护数据
否
重新录入指纹
输入指纹与验证指纹匹配？
是
允许访问
否
拒绝访问

图 1