



(12)发明专利

(10)授权公告号 CN 104915584 B

(45)授权公告日 2018.01.05

(21)申请号 201510298775.6

G06F 21/32(2013.01)

(22)申请日 2015.06.03

G06Q 20/38(2012.01)

(65)同一申请的已公布的文献号

G06Q 20/40(2012.01)

申请公布号 CN 104915584 A

(56)对比文件

CN 104408356 A, 2015.03.11, Y1.

(43)申请公布日 2015.09.16

CN 104574088 A, 2015.04.29, Y2.

(73)专利权人 深圳市沃特沃德股份有限公司

CN 104462911 A, 2015.03.25, 全文.

地址 518000 广东省深圳市南山区蛇口南海大道1079号花园城数码大厦B座503、602

CN 103618611 A, 2014.03.05, 全文.

(72)发明人 谢恩 郑勇 张立新

US 2011/0126024 A1, 2011.05.26, 全文.

(74)专利代理机构 深圳市恒申知识产权事务所
(普通合伙) 44312

CN 102387161 A, 2012.03.21, 全文.

代理人 陈健

审查员 贾东曜

(51)Int.Cl.

G06F 21/31(2013.01)

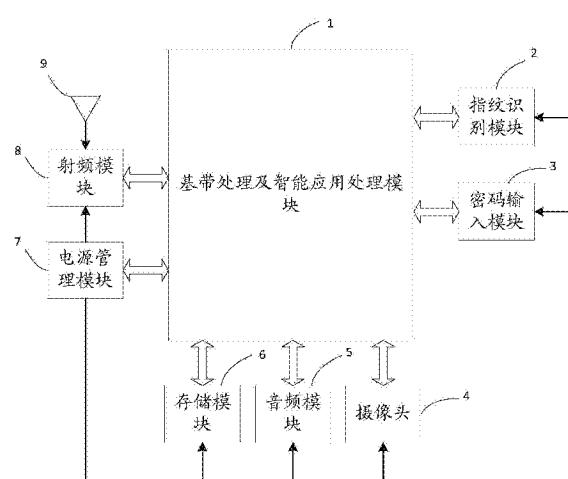
权利要求书1页 说明书4页 附图1页

(54)发明名称

基于指纹特征的智能移动终端随机加解密系统

(57)摘要

本发明涉及一种基于指纹特征的智能移动终端随机加解密系统。本发明利用初始密码对初始指纹进行对称加密得到加密指纹，并利用初始密码和加密指纹对智能移动终端进行双重加密。解密时，需输入密码与初始密码匹配才能对加密指纹进行解密得出解密指纹，同时还需解密指纹与输入指纹匹配才能完成对智能移动终端的解密。同时，由于加密指纹是利用初始密码对初始指纹进行对称加密得到，输入不同的初始密码可得到不同的加密指纹，可实现对初始指纹的随机加密。再者，由于加解密都在trust zone安全模式下执行，未授权软件无法获取加解密算法，即使获得初始密码与加密指纹，也无法得出正确的解密指纹以实现指纹匹配，大幅提升了智能移动终端的安全性。



1. 一种基于指纹特征的智能移动终端随机加解密系统，其特征在于，包括：

指纹识别模块，用于采集用户输入的初始指纹；

密码输入模块，用于接收所述用户输入的初始密码；

基带处理及智能应用处理模块，其支持trust zone架构，用于接收所述初始指纹及所述初始密码，并在trust zone安全模式下利用所述初始密码对所述初始指纹进行对称加密运算，得到加密指纹，并将该加密指纹与所述初始密码一起存储到其trust zone区域，实现对所述智能移动终端的加密；

在对所述智能移动终端解密时：

所述指纹识别模块还用于采集输入指纹；

所述密码输入模块还用于接收输入密码；

所述基带处理及智能应用处理模块还用于将所述输入密码与trust zone区域中存储的初始密码进行比对，并在比对一致时利用所述输入密码对所述加密指纹进行对称解密运算，得到解密指纹，并将该解密指纹与所述输入指纹匹配，并在匹配成功时将所述智能移动终端解锁。

2. 如权利要求1所述的基于指纹特征的智能移动终端随机加解密系统，其特征在于，所述基带处理及智能应用处理模块还具有修改密码模式；在修改密码模式中：

所述密码输入模块还用于接收所述用户输入的旧密码；

所述基带处理及智能应用处理模块还用于接收所述旧密码，并将所述旧密码与trust zone区域中存储的初始密码进行比对，并在比对一致时利用所述旧密码对所述加密指纹进行对称解密运算，得到解密指纹，同时，通过所述密码输入模块接收所述用户输入的新密码，并利用该新密码对该解密指纹重新进行对称加密，得到新的加密指纹，并将该新的加密指纹与该新密码一起存储到trust zone区域。

3. 如权利要求1所述的基于指纹特征的智能移动终端随机加解密系统，其特征在于，所述对称加密运算为异或/可逆矩阵相乘/循环移位或DES对称加密算法。

4. 如权利要求1所述的基于指纹特征的智能移动终端随机加解密系统，其特征在于，所述指纹识别模块为电容式指纹传感器。

5. 如权利要求1所述的基于指纹特征的智能移动终端随机加解密系统，其特征在于，所述密码输入模块为触摸显示屏。

6. 如权利要求1所述的基于指纹特征的智能移动终端随机加解密系统，其特征在于，所述基带处理及智能应用处理模块连接有射频模块；该射频模块连接有天线。

7. 如权利要求1所述的基于指纹特征的智能移动终端随机加解密系统，其特征在于，所述基带处理及智能应用处理模块连接有存储模块。

8. 如权利要求1所述的基于指纹特征的智能移动终端随机加解密系统，其特征在于，所述基带处理及智能应用处理模块连接有音频模块；所述音频模块连接有传声器及扬声器，用于驱动所述传声器及扬声器。

9. 如权利要求1所述的基于指纹特征的智能移动终端随机加解密系统，其特征在于，所述基带处理及智能应用处理模块连接有摄像头。

10. 如权利要求1所述的基于指纹特征的智能移动终端随机加解密系统，其特征在于，所述基带处理及智能应用处理模块的内核为ARM Cortex A系列多核处理器。

基于指纹特征的智能移动终端随机加解密系统

技术领域

[0001] 本发明涉及指纹加密技术领域,尤其涉及一种基于指纹特征的智能移动终端随机加解密系统。

背景技术

[0002] 随着支付向移动端迁移,安全风险也正不断加剧。手机丢失、木马软件盗取等都让手机等移动介质变为不设防的移动金库。指纹识别即指通过比较不同指纹的细节特征点来进行鉴别,由于指纹识别具有快速、便利、安全、独有、不会丢失等优势,特别是用户与生俱来的特点,指纹识别将让其在移动终端安全和移动支付业务方面得到普遍应用。但指纹识别也存在安全风险,移动智能终端尺寸限制导致指纹传感器的接触面积小,特征点的取样有限,基于指纹图像匹配的算法是通过相似度模糊比较,对图像匹配算法依赖大,所以通过一些特殊的手段也能破解,破解的概率大约是 $1/50000$,给移动支付和移动终端信息安全带来隐患。传统的密码在移动支付现在是主流,方便实用,符合用户习惯,6位数字密码被破解的概率为 $1/1000000$ 。将指纹识别与密码结合起来,将密码作为密钥,即可实现指纹特征特有的加密,其破解的概率为 $1/50000000000$,能够极大增加移动支付的安全。

发明内容

[0003] 本发明所要解决的技术问题是,提供一种基于指纹特征的智能移动终端随机加解密系统,利用密码与指纹结合对智能移动终端进行加解密。本发明是这样实现的:

[0004] 一种基于指纹特征的智能移动终端随机加解密系统,包括:

[0005] 指纹识别模块,用于采集用户输入的初始指纹;

[0006] 密码输入模块,用于接收所述用户输入的初始密码;

[0007] 基带处理及智能应用处理模块,其支持trust zone架构,用于接收所述初始指纹及所述初始密码,并在trust zone安全模式下利用所述初始密码对所述初始指纹进行对称加密运算,得到加密指纹,并将该加密指纹与所述初始密码一起存储到其trust zone区域,实现对所述智能移动终端的加密;

[0008] 在对所述智能移动终端解密时:

[0009] 所述指纹识别模块还用于采集输入指纹;

[0010] 所述密码输入模块还用于接收输入密码;

[0011] 所述基带处理及智能应用处理模块还用于将所述输入密码与trust zone区域中存储的初始密码进行比对,并在比对一致时利用所述输入密码对所述加密指纹进行对称解密运算,得到解密指纹,并将该解密指纹与所述输入指纹匹配,并在匹配成功时将所述智能移动终端解锁。

[0012] 进一步地,所述基带处理及智能应用处理模块还具有修改密码模式;在修改密码模式中:

[0013] 所述密码输入模块还用于接收所述用户输入的旧密码;

[0014] 所述基带处理及智能应用处理模块还用于接收所述旧密码，并将所述旧密码与 trust zone 区域中存储的初始密码进行比对，并在比对一致时利用所述旧密码对所述加密指纹进行对称解密运算，得到解密指纹，同时，通过所述密码输入模块接收所述用户输入的新密码，并利用该新密码对该解密指纹重新进行对称加密，得到新的加密指纹，并将该新的加密指纹与该新密码一起存储到 trust zone 区域。

[0015] 进一步地，所述对称加密运算为异或/可逆矩阵相乘/循环移位或DES对称加密算法。

[0016] 进一步地，所述指纹识别模块为电容式指纹传感器。

[0017] 进一步地，所述密码输入模块为触摸显示屏。

[0018] 进一步地，所述基带处理及智能应用处理模块连接有射频模块；该射频模块连接有天线。

[0019] 进一步地，所述基带处理及智能应用处理模块连接有存储模块。

[0020] 进一步地，所述基带处理及智能应用处理模块连接有音频模块；所述音频模块连接有传声器及扬声器，用于驱动所述传声器及扬声器。

[0021] 进一步地，所述基带处理及智能应用处理模块连接有摄像头。

[0022] 进一步地，所述基带处理及智能应用处理模块的内核为ARM Cortex A53四核64位处理器。

[0023] 与现有技术相比，本发明利用初始密码对初始指纹进行对称加密得到加密指纹，并利用初始密码和加密指纹对智能移动终端进行双重加密。解密时，需输入密码与初始密码匹配才能对加密指纹进行解密得出解密指纹，同时还需解密指纹与输入指纹匹配才能完成对智能移动终端的解密。同时，由于加密指纹是利用初始密码对初始指纹进行对称加密得到，输入不同的初始密码可得到不同的加密指纹，可实现对初始指纹的随机加密。再者，由于加解密都在 trust zone 安全模式下执行，未授权软件无法获取加解密算法，即使获得初始密码与加密指纹，也无法得出正确的解密指纹以实现指纹匹配，大幅提升了智能移动终端的安全性。

附图说明

[0024] 图1：本发明实施例提供的基于指纹特征的智能移动终端随机加解密系统组成示意图。

具体实施方式

[0025] 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。

[0026] 如图1所示，本发明实施例提供的基于指纹特征的智能移动终端随机加解密系统包括指纹识别模块2、密码输入模块3及基带处理及智能应用处理模块1。

[0027] 指纹识别模块2用于采集用户输入的初始指纹。指纹识别模块2由芯片、蓝宝石、金属环、软板、载板等组成，与基带处理及智能应用处理模块1之间采用SPI高速总线接口连接。指纹识别模块2采用电容式指纹传感器，可采用划擦式或者按压式的指纹传感器。当手指指端划擦或者按压感测指纹的电容式指纹传感器，该电容式指纹传感器就可根据指纹的

指纹脊和指纹谷而产生电容信号变化以提供指纹图像。获取的指纹图像是一幅含有较多噪声的灰度图像,可通过智能应用处理器对该指纹图像进行预处理以改善指纹图像的质量,增强指纹脊和指纹谷的对比度,将指纹图像变成一幅清晰的点线图,以便于进行特征提取。

[0028] 基带处理及智能应用处理模块1支持trust zone架构。TrustZone是ARM公司开发的针对移动智能终端的安全技术,TrustZone技术与Cortex™-A处理器紧密集成,并通过AMBA® AXI总线和特定的TrustZone系统IP块在系统中进行扩展。此系统可以保护安全内存、加密块、键盘和屏幕等外设,从而可确保它们免遭软件攻击。按照TrustZone Ready Program建议开发并利用TrustZone技术的设备提供了能够支持完全可信执行环境(TEE)、安全感知应用程序及安全服务的平台,在高性能ARM处理器平台上可将三者结合起来。基带处理及智能应用处理模块1的内核可采用ARM Cortex A系列多核处理器,该系列处理器支持TrustZone技术。如ARM Cortex A53四核64位处理器,具有1.5GHz的处理速度,可用于指纹特征提取、密码匹配、智能移动终端的加解密运算等。该处理器的指纹特征提取时间<20ms,指纹匹配运算时间<200ms,可满足支付实时性需求。基带处理及智能应用处理模块1具有普通模式和Trust Zone安全模式,可在两种模式之间切换。基带处理及智能应用处理模块1可在trust zone安全模式下对指纹识别模块2采集到的指纹图像进行预处理以提高处理过程中的安全性,预处理包括归一化、图像分割、增强、二值化和细化等。初始指纹中包含指纹特征点和纹理等信息。基带处理及智能应用处理模块1可对这些指纹特征点和纹理等信息进行提取,用于后续对初始指纹的加密计算。

[0029] 密码输入模块3用于接收用户输入的初始密码。密码输入模块3采用触摸显示屏,可通过触摸显示屏上的虚拟键盘输入密码。

[0030] 基带处理及智能应用处理模块1接收初始指纹及初始密码,并在trust zone安全模式下利用初始密码对初始指纹进行对称加密运算,得到加密指纹,并将该加密指纹与初始密码一起存储到其trust zone区域,实现对智能移动终端的加密。由于加密指纹是利用初始密码对初始指纹进行对称加密得到,输入不同的初始密码可得到不同的加密指纹,可实现对初始指纹的随机加密,提升智能移动终端的安全性。

[0031] 在对智能移动终端解密时,指纹识别模块2采集输入指纹,密码输入模块3接收输入密码。基带处理及智能应用处理模块1将输入密码与trust zone区域中存储的初始密码进行比对,密码比对是精确比对,如果比对不一致,则终止解密进程,如果比对一致,则利用输入密码对加密指纹进行对称解密运算,得到解密指纹。

[0032] 对称加密是一种采用单钥密码系统的加密方法,同一个密钥可以同时用作信息的加密和解密,发收信双方都使用这个密钥对数据进行加密和解密,收信方收到密文后,若想解读原文,则需要使用加密用过的密钥及相同算法的逆算法对密文进行解密,才能使其恢复成可读明文。这种加密方法也称为单密钥加密。对称加密运算可采用异或/可逆矩阵相乘/循环移位或DES对称加密算法。

[0033] 基于对称加密的原理,如果输入密码与trust zone区域中存储的初始密码一致,则对加密指纹进行对称解密运算得到的解密指纹将与初始指纹具有相同的指纹特征。此时,可将该解密指纹与输入指纹匹配。指纹匹配是模糊匹配,具体而言,是几何域模糊识别匹配,主要是指纹特征点定位和纹理类型的匹配。如果匹配不成功,则再次终止解密进程,如果匹配成功,则说明输入的密码及指纹均通过验证,此时则将智能移动终端解锁。

[0034] 基带处理及智能应用处理模块1还具有修改密码模式，在修改密码模式中，密码输入模块3接收用户输入的旧密码，基带处理及智能应用处理模块1接收旧密码，并将旧密码与trust zone区域中存储的初始密码进行比对，并在比对一致时利用旧密码对加密指纹进行对称解密运算，得到解密指纹，同时，通过密码输入模块3接收用户输入的新密码，并利用该新密码对该解密指纹重新进行对称加密，得到新的加密指纹，并将该新的加密指纹与该新密码一起存储到trust zone区域。

[0035] 智能应用处理器还连接有其他功能模块，包括射频模块8、音频模块5、摄像头4及电源管理模块7等。射频模块8连接有天线9，用于射频信号的收发。存储模块6包含EMMCP芯片和TF卡，支持高速存储。音频模块5连接有传声器及扬声器，用于驱动传声器及扬声器。

[0036] 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。

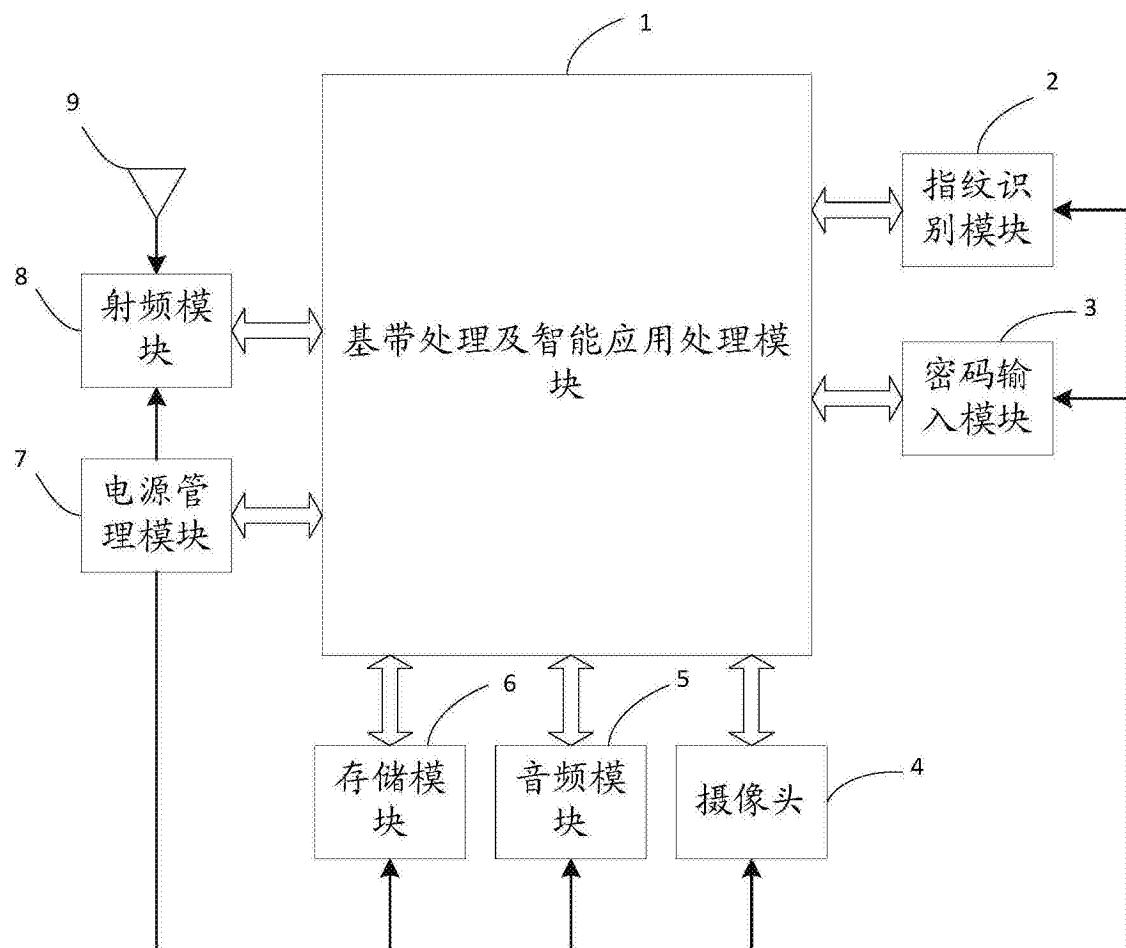


图1