



(12)发明专利

(10)授权公告号 CN 104980436 B

(45)授权公告日 2018.06.26

(21)申请号 201510319315.7

H04L 12/743(2013.01)

(22)申请日 2015.06.11

H04L 9/32(2006.01)

(65)同一申请的已公布的文献号

申请公布号 CN 104980436 A

(56)对比文件

CN 1743995 A, 2006.03.08,

WO 9733231 A1, 1997.09.12,

CN 101145906 A, 2008.03.19,

CN 104216748 A, 2014.12.17,

CN 101145911 A, 2008.03.19,

(43)申请公布日 2015.10.14

审查员 杜晓萍

(73)专利权人 努比亚技术有限公司

地址 518057 广东省深圳市南山区高新园  
北环大道9018号大族创新大厦C座9楼

(72)发明人 陈小翔

(74)专利代理机构 深圳协成知识产权代理事务  
所(普通合伙) 44458

代理人 章小燕

(51)Int.Cl.

H04L 29/06(2006.01)

权利要求书2页 说明书19页 附图3页

H04L 29/08(2006.01)

(54)发明名称

一种加密传输系统、方法、终端以及中间服  
务器

(57)摘要

本发明提出了一种加密传输系统、方法、终  
端和中间服务器，包括：发送信息时，检测施加的  
预定操作；并生成预定的第一散列值；将携带信息  
明文与第一散列值的报文发送给中间服务器。  
接收信息时，接收中间服务器发送的报文，检测  
施加在接收终端上的与发送终端上相同的操作；  
根据该操作生成第二散列值，将其与第一散列值  
相比较，两个散列值相匹配时，接收终端能够读  
取信息明文。中间服务器预先保存预定操作对应  
的散列值；接收到发送的报文后，将第一散列值  
与预存的散列值相比较，当第一散列值与预存的  
散列值中的任意一个相匹配时，将报文发送至与  
所匹配的该散列值相对应的接收终端。通过本发  
明方案能够提供一种简单、方便、易行的信息加  
密传输方案。



1. 一种加密传输系统,其特征在于,所述系统包括:发送终端和接收终端;

所述发送终端,用于当需要发送信息时,检测施加在所述发送终端上的预定的操作;根据所述操作生成预定的第一散列值;将携带有信息明文与所述第一散列值的报文发送给中间服务器;

所述接收终端,当需要接收信息时,接收所述中间服务器发送的报文,并检测施加在所述接收终端上的与施加在发送所述信息的所述发送终端上的操作相同的操作;并根据所述操作生成预定的第二散列值,将所述第二散列值与所述报文中携带的所述第一散列值相比较,当所述第二散列值与所述第一散列值相匹配时,所述接收终端能够读取所述报文中所携带的所述信息明文。

2. 如权利要求1所述的加密传输系统,其特征在于,所述系统还包括中间服务器;

所述中间服务器预先保存不同的所述发送终端和不同的所述接收终端之间在进行加密传输时预定的加密操作所对应的不同的所述预定的散列值;其中,不同的所述预定的散列值与不同的所述发送终端以及不同的所述接收终端一一对应;

所述中间服务器接收到所述发送终端发送的所述报文后,将所述报文中携带的所述第一散列值与预存的一个或多个所述预定的散列值相比较,当所述第一散列值与预存的一个或多个所述预定的散列值中的任意一个相匹配时,将所述报文发送至与所述第一散列值相匹配的所述预定的散列值相对应的所述接收终端。

3. 如权利要求2所述的加密传输系统,其特征在于,所述发送终端和所述接收终端均预存有所述预定的操作与所述预定的散列值之间的映射关系,并且所述发送终端中预存的加密操作所对应的散列值与所述接收终端中预存的相同的操作所对应的散列值相同。

4. 如权利要求1-3任意一项所述的加密传输系统,其特征在于,所述预定的加密操作包括以下形式的一种或多种:对所述发送终端和所述接收终端的用力握持、挤压、按压、滑动以及密码输入。

5. 一种加密传输终端,其特征在于,所述终端用于:

当需要发送信息时,检测施加在所述终端上的预定的操作;根据所述操作生成预定的第一散列值;将携带有信息明文与所述第一散列值的报文发送给中间服务器;

当需要接收信息时,接收所述中间服务器发送的报文,并检测施加在所述终端上的与施加在发送所述信息的终端上的操作相同的操作;并根据所述操作生成预定的第二散列值,将所述第二散列值与所述报文中携带的所述第一散列值相比较,当所述第二散列值与所述第一散列值相匹配时,所述终端能够读取所述报文中所携带的所述信息明文。

6. 如权利要求5所述的终端,其特征在于,所述预定的操作包括以下形式的一种或多种:对所述终端的用力握持、挤压、按压、滑动以及密码输入。

7. 一种中间服务器,其特征在于,所述中间服务器用于:

预先保存不同的发送终端和不同的接收终端之间在进行加密传输时预定的操作所对应的不同的预定的散列值;其中,不同的所述预定的散列值与不同的所述发送终端以及不同的所述接收终端一一对应;

接收到所述发送终端发送的报文后,将所述报文中携带的第一散列值与预存的一个或多个所述预定的散列值相比较,当所述第一散列值与预存的一个或多个所述预定的散列值中的任意一个相匹配时,将所述报文发送至与所述第一散列值相匹配的所述预定的散列值

相对应的接收终端。

8. 如权利要求7所述的中间服务器,其特征在于,所述预定的操作包括以下形式的一种或多种:对所述发送终端和所述接收终端的用力握持、挤压、按压、滑动以及密码输入。

9. 一种加密传输方法,其特征在于,所述方法包括:

当需要发送信息时,检测施加在发送终端上的预定的操作;根据所述操作生成预定的第一散列值;将携带有信息明文与所述第一散列值的报文发送给中间服务器;

当需要接收信息时,接收所述中间服务器发送的报文,并检测施加在所述接收终端上的与施加在发送所述信息的所述发送终端上的操作相同的操作;并根据所述操作生成预定的第二散列值,将所述第二散列值与所述报文中携带的所述第一散列值相比较,当所述第二散列值与所述第一散列值相匹配时,所述接收终端能够读取所述报文中所携带的所述信息明文。

10. 如权利要求9所述的加密传输方法,其特征在于,所述方法还包括:

在所述中间服务器中预先保存不同的所述发送终端和不同的所述接收终端之间在进行加密传输时预定的加密操作所对应的不同的所述预定的散列值;其中,不同的所述预定的散列值与不同的所述发送终端以及不同的所述接收终端一一对应;

在所述中间服务器接收到所述发送终端发送的所述报文后,将所述报文中携带的所述第一散列值与预存的一个或多个所述预定的散列值相比较,当所述第一散列值与预存的一个或多个所述预定的散列值中的任意一个相匹配时,将所述报文发送至与所述第一散列值相匹配的所述预定的散列值相对应的所述接收终端。

## 一种加密传输系统、方法、终端以及中间服务器

### 技术领域

[0001] 本发明涉及加密技术领域，尤其涉及一种加密传输系统、方法、终端以及中间服务器。

### 背景技术

[0002] 基于移动互联网的智能终端其应用广泛，如何保证隐私安全是需要重点考虑的问题。目前加密信息中，主流做法是采用非对称密码进行加密，常用的公钥密码算法包括RSA，ECC，Robin等。

[0003] 现有的加密方法中，大多数是固化解决方案，其流程较为复杂，且更多的是针对PC端到端的解决方案，典型的诸如网页浏览，网页支付等。对于智能终端而言，普通的信息可采用一种轻量级的加密方法来实现。因此，如何在接收方和发送方两端都做到一个简单方便的加密方案，是一个急需解决的问题。

### 发明内容

[0004] 本发明的主要目的在于提出了一种加密传输系统、方法、终端以及中间服务器，旨在提供一种简单、方便、易行的信息加密传输方案。

[0005] 此外，为实现上述目的，本发明提出了一种加密传输系统，其特征在于，该系统包括：发送终端和接收终端。

[0006] 发送终端，用于当需要发送信息时，检测施加在发送终端上的预定的操作；根据该操作生成预定的第一散列值；将携带有信息明文与第一散列值的报文发送给中间服务器。

[0007] 接收终端，当需要接收信息时，接收中间服务器发送的报文，并检测施加在该终端上的与施加在发送该信息的终端上的操作相同的操作；并根据该操作生成预定的第二散列值，将第二散列值与报文中携带的第一散列值相比较，当第二散列值与第一散列值相匹配时，终端能够读取报文中所携带的信息明文。

[0008] 优选地，该系统还包括中间服务器。

[0009] 中间服务器预先保存不同的发送终端和不同的接收终端之间在进行加密传输时预定的操作所对应的不同的预定的散列值；其中，不同的预定的散列值与不同的发送客户端以及不同的接收客户端一一对应。

[0010] 中间服务器接收到发送终端发送的报文后，将报文中携带的第一散列值与预存的一个或多个预定的散列值相比较，当第一散列值与预存的一个或多个预定的散列值中的任意一个相匹配时，将报文发送至与第一散列值相匹配的预定的散列值相对应的接收终端。

[0011] 优选地，发送终端和接收终端均预存有预定的操作与预定的散列值之间的映射关系，并且发送终端中预存的加密操作所对应的散列值与接收终端中预存的相同的操作所对应的散列值相同。

[0012] 优选地，预定的加密操作包括以下形式的一种或多种：对发送终端和接收终端的用力握持、挤压、按压、滑动以及密码输入。

[0013] 此外,为实现上述目的,本发明还提供了一种加密传输终端,该终端用于:

[0014] 当需要发送信息时,检测施加在终端上的预定的操作;根据该操作生成预定的第一散列值;将携带有信息明文与第一散列值的报文发送给中间服务器。

[0015] 当需要接收信息时,接收中间服务器发送的报文,并检测施加在该终端上的与施加在发送该信息的终端上的操作相同的操作;并根据该操作生成预定的第二散列值,将第二散列值与报文中携带的第一散列值相比较,当第二散列值与第一散列值相匹配时,终端能够读取报文中所携带的信息明文。

[0016] 优选地,预定的操作包括以下形式的一种或多种:对终端的用力握持、挤压、按压、滑动以及密码输入。

[0017] 此外,为实现上述目的,本发明还提出一种中间服务器,该中间服务器用于:

[0018] 预先保存不同的发送终端和不同的接收终端之间在进行加密传输时预定的操作所对应的不同的预定的散列值;其中,不同的预定的散列值与不同的发送终端以及不同的接收终端一一对应。

[0019] 接收到发送终端发送的报文后,将报文中携带的第一散列值与预存的一个或多个预定的散列值相比较,当第一散列值与预存的一个或多个预定的散列值中的任意一个相匹配时,将报文发送至与第一散列值相匹配的该预定的散列值相对应的接收终端。

[0020] 优选地,预定的操作包括以下形式的一种或多种:对发送终端和接收终端的用力握持、挤压、按压、滑动以及密码输入。

[0021] 此外,为实现上述目的,本发明还提出一种加密传输方法,该方法包括:

[0022] 当需要发送信息时,检测施加在发送终端上的预定的操作;根据该操作生成预定的第一散列值;将携带有信息明文与所述第一散列值的报文发送给中间服务器。

[0023] 当需要接收信息时,接收所述中间服务器发送的报文,并检测施加在接收终端上的与施加在发送该信息的发送终端上的操作相同的操作;并根据该操作生成预定的第二散列值,将第二散列值与报文中携带的第一散列值相比较,当第二散列值与第一散列值相匹配时,接收终端能够读取所述报文中所携带的信息明文。

[0024] 优选地,该方法还包括:

[0025] 在中间服务器中预先保存不同的发送终端和不同的接收终端之间在进行加密传输时预定的加密操作所对应的不同的预定的散列值;其中,不同的预定的散列值与不同的发送客户端以及不同的接收客户端一一对应。

[0026] 在中间服务器接收到发送终端发送的报文后,将报文中携带的第一散列值与预存的一个或多个预定的散列值相比较,当第一散列值与预存的一个或多个预定的散列值中的任意一个相匹配时,将报文发送至与第一散列值相匹配的预定的散列值相对应的接收终端。

[0027] 优选地,发送终端和接收终端均预存有预定的操作与预定的散列值之间的映射关系,并且发送终端中预存的加密操作所对应的散列值与接收终端中预存的相同的操作所对应的散列值相同。

[0028] 优选地,预定的加密操作包括以下形式的一种或多种:对发送终端和接收终端的用力握持、挤压、按压、滑动以及密码输入。

[0029] 本发明提出的加密传输系统、方法和终端,包括:当需要发送信息时,检测施加在

终端上的预定的操作；根据该操作生成预定的第一散列值；将携带有信息明文与第一散列值的报文发送给中间服务器。当需要接收信息时，接收中间服务器发送的报文，并检测施加在终端上的与施加在发送该信息的终端上的操作相同的操作；并根据该操作生成预定的第二散列值，将第二散列值与报文中携带的第一散列值相比较，当第二散列值与第一散列值相匹配时，终端能够读取报文中所携带的信息明文。本发明提出的中间服务器包括：预先保存不同的发送终端和不同的接收终端之间在进行加密传输时预定的操作所对应的不同的预定的散列值；其中，不同的预定的散列值与不同的发送终端以及不同的接收终端一一对应。接收到发送终端发送的报文后，将报文中携带的第一散列值与预存的一个或多个预定的散列值相比较，当第一散列值与预存的一个或多个预定的散列值中的任意一个相匹配时，将报文发送至与第一散列值相匹配的该预定的散列值相对应的接收终端。通过本发明的方案能够提供一种简单、方便、易行的信息加密传输方案。

## 附图说明

- [0030] 图1为实现本发明各个实施例的移动终端的硬件结构示意图；
- [0031] 图2为如图1所示的移动终端的无线通信系统示意图；
- [0032] 图3为本发明的加密传输系统框图；
- [0033] 图4为本发明实施例中以接收终端进行鉴权的实施方法流程图；
- [0034] 图5为本发明实施例中以中间服务器进行鉴权的实施方法流程图。
- [0035] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

## 具体实施方式

- [0036] 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。
- [0037] 现在将参考附图描述实现本发明各个实施例的移动终端。在后续的描述中，使用用于表示元件的诸如“模块”、“部件”或“单元”的后缀仅为了有利于本发明的说明，其本身并没有特定的意义。因此，“模块”与“部件”可以混合地使用。
- [0038] 移动终端可以以各种形式来实施。例如，本发明中描述的终端可以包括诸如移动电话、智能电话、笔记本电脑、数字广播接收器、PDA（个人数字助理）、PAD（平板电脑）、PMP（便携式多媒体播放器）、导航装置等等的移动终端以及诸如数字TV、台式计算机等等的固定终端。下面，假设终端是移动终端。然而，本领域技术人员将理解的是，除了特别用于移动目的的元件之外，根据本发明的实施方式的构造也能够应用于固定类型的终端。
- [0039] 图1为实现本发明各个实施例的移动终端的硬件结构示意。
- [0040] 移动终端100可以包括无线通信单元110、A/V（音频/视频）输入单元120、用户输入单元130、感测单元140、输出单元150、存储器160、接口单元170、控制器180和电源单元190等等。图1示出了具有各种组件的移动终端，但是应理解的是，并不要求实施所有示出的组件。可以替代地实施更多或更少的组件。将在下面详细描述移动终端的元件。
- [0041] 无线通信单元110通常包括一个或多个组件，其允许移动终端100与无线通信系统或网络之间的无线电通信。例如，无线通信单元可以包括广播接收模块111、移动通信模块112、无线互联网模块113、短程通信模块114和位置信息模块115中的至少一个。
- [0042] 广播接收模块111经由广播信道从外部广播管理服务器接收广播信号和/或广播

相关信息。广播信道可以包括卫星信道和/或地面信道。广播管理服务器可以是生成并发送广播信号和/或广播相关信息的服务器或者接收之前生成的广播信号和/或广播相关信息并且将其发送给终端的服务器。广播信号可以包括TV广播信号、无线电广播信号、数据广播信号等等。而且，广播信号可以进一步包括与TV或无线电广播信号组合的广播信号。广播相关信息也可以经由移动通信网络提供，并且在该情况下，广播相关信息可以由移动通信模块112来接收。广播信号可以以各种形式存在，例如，其可以以数字多媒体广播(DMB)的电子节目指南(EPG)、数字视频广播手持(DVB-H)的电子服务指南(ESG)等等的形式而存在。广播接收模块111可以通过使用各种类型的广播系统接收信号广播。特别地，广播接收模块111可以通过使用诸如多媒体广播-地面(DMB-T)、数字多媒体广播-卫星(DMB-S)、数字视频广播-手持(DVB-H)，前向链路媒体(MediaFL0<sup>®</sup>)的数据广播系统、地面数字广播综合服务(ISDB-T)等等的数字广播系统接收数字广播。广播接收模块111可以被构造为适合提供广播信号的各种广播系统以及上述数字广播系统。经由广播接收模块111接收的广播信号和/或广播相关信息可以存储在存储器160(或者其它类型的存储介质)中。

[0043] 移动通信模块112将无线电信号发送到基站(例如，接入点、节点B等等)、外部终端以及服务器中的至少一个和/或从其接收无线电信号。这样的无线电信号可以包括语音通话信号、视频通话信号、或者根据文本和/或多媒体消息发送和/或接收的各种类型的数据。

[0044] 无线互联网模块113支持移动终端的无线互联网接入。该模块可以内部或外部地耦接到终端。该模块所涉及的无线互联网接入技术可以包括WLAN(无线LAN)(Wi-Fi)、Wibro(无线宽带)、Wimax(全球微波互联接入)、HSDPA(高速下行链路分组接入)等等。

[0045] 短程通信模块114是用于支持短程通信的模块。短程通信技术的一些示例包括蓝牙<sup>TM</sup>、射频识别(RFID)、红外数据协会(IrDA)、超宽带(UWB)、紫蜂<sup>TM</sup>等等。

[0046] 位置信息模块115是用于检查或获取移动终端的位置信息的模块。位置信息模块的典型示例是GPS(全球定位系统)。根据当前的技术，GPS模块115计算来自三个或更多卫星的距离信息和准确的时间信息并且对于计算的信息应用三角测量法，从而根据经度、纬度和高度准确地计算三维当前位置信息。当前，用于计算位置和时间信息的方法使用三颗卫星并且通过使用另外的一颗卫星校正计算出的位置和时间信息的误差。此外，GPS模块115能够通过实时地连续计算当前位置信息来计算速度信息。

[0047] A/V输入单元120用于接收音频或视频信号。A/V输入单元120可以包括相机121和麦克风1220，相机121对在视频捕获模式或图像捕获模式中由图像捕获装置获得的静态图片或视频的图像数据进行处理。处理后的图像帧可以显示在显示单元151上。经相机121处理后的图像帧可以存储在存储器160(或其它存储介质)中或者经由无线通信单元110进行发送，可以根据移动终端的构造提供两个或更多相机1210。麦克风122可以在电话通话模式、记录模式、语音识别模式等等运行模式中经由麦克风接收声音(音频数据)，并且能够将这样的声音处理为音频数据。处理后的音频(语音)数据可以在电话通话模式的情况下转换为可经由移动通信模块112发送到移动通信基站的格式输出。麦克风122可以实施各种类型的噪声消除(或抑制)算法以消除(或抑制)在接收和发送音频信号的过程中产生的噪声或者干扰。

[0048] 用户输入单元130可以根据用户输入的命令生成键输入数据以控制移动终端的各种操作。用户输入单元130允许用户输入各种类型的信息，并且可以包括键盘、锅仔片、触摸

板(例如,检测由于被接触而导致的电阻、压力、电容等等的变化的触敏组件)、滚轮、摇杆等等。特别地,当触摸板以层的形式叠加在显示单元151上时,可以形成触摸屏。

[0049] 感测单元140检测移动终端100的当前状态,(例如,移动终端100的打开或关闭状态)、移动终端100的位置、用户对于移动终端100的接触(即,触摸输入)的有无、移动终端100的取向、移动终端100的加速或减速移动和方向等等,并且生成用于控制移动终端100的操作的命令或信号。例如,当移动终端100实施为滑动型移动电话时,感测单元140可以感测该滑动型电话是打开还是关闭。另外,感测单元140能够检测电源单元190是否提供电力或者接口单元170是否与外部装置耦接。感测单元140可以包括接近传感器1410将在下面结合触摸屏来对此进行描述。

[0050] 接口单元170用作至少一个外部装置与移动终端100连接可以通过的接口。例如,外部装置可以包括有线或无线头戴式耳机端口、外部电源(或电池充电器)端口、有线或无线数据端口、存储卡端口、用于连接具有识别模块的装置的端口、音频输入/输出(I/O)端口、视频I/O端口、耳机端口等等。识别模块可以是存储用于验证用户使用移动终端100的各种信息并且可以包括用户识别模块(UIM)、客户识别模块(SIM)、通用客户识别模块(USIM)等等。另外,具有识别模块的装置(下面称为“识别装置”)可以采取智能卡的形式,因此,识别装置可以经由端口或其它连接装置与移动终端100连接。接口单元170可以用于接收来自外部装置的输入(例如,数据信息、电力等等)并且将接收到的输入传输到移动终端100内的一个或多个元件或者可以用于在移动终端和外部装置之间传输数据。

[0051] 另外,当移动终端100与外部底座连接时,接口单元170可以用作允许通过其将电力从底座提供到移动终端100的路径或者可以用作允许从底座输入的各种命令信号通过其传输到移动终端的路径。从底座输入的各种命令信号或电力可以用作用于识别移动终端是否准确地安装在底座上的信号。输出单元150被构造为以视觉、音频和/或触觉方式提供输出信号(例如,音频信号、视频信号、警报信号、振动信号等等)。输出单元150可以包括显示单元151、音频输出模块152、警报单元153等等。

[0052] 显示单元151可以显示在移动终端100中处理的信息。例如,当移动终端100处于电话通话模式时,显示单元151可以显示与通话或其它通信(例如,文本消息收发、多媒体文件下载等等)相关的用户界面(UI)或图形用户界面(GUI)。当移动终端100处于视频通话模式或者图像捕获模式时,显示单元151可以显示捕获的图像和/或接收的图像、示出视频或图像以及相关功能的UI或GUI等等。

[0053] 同时,当显示单元151和触摸板以层的形式彼此叠加以形成触摸屏时,显示单元151可以用作输入装置和输出装置。显示单元151可以包括液晶显示器(LCD)、薄膜晶体管LCD(TFT-LCD)、有机发光二极管(OLED)显示器、柔性显示器、三维(3D)显示器等等中的至少一种。这些显示器中的一些可以被构造为透明状以允许用户从外部观看,这可以称为透明显示器,典型的透明显示器可以例如为TOLED(透明有机发光二极管)显示器等等。根据特定想要的实施方式,移动终端100可以包括两个或更多显示单元(或其它显示装置),例如,移动终端可以包括外部显示单元(未示出)和内部显示单元(未示出)。触摸屏可用于检测触摸输入压力以及触摸输入位置和触摸输入面积。

[0054] 音频输出模块152可以在移动终端处于呼叫信号接收模式、通话模式、记录模式、语音识别模式、广播接收模式等等模式下时,将无线通信单元110接收的或者在存储器160

中存储的音频数据转换音频信号并且输出为声音。而且，音频输出模块152可以提供与移动终端100执行的特定功能相关的音频输出(例如，呼叫信号接收声音、消息接收声音等等)。音频输出模块152可以包括扬声器、蜂鸣器等等。

[0055] 警报单元153可以提供输出以将事件的发生通知给移动终端100。典型的事件可以包括呼叫接收、消息接收、键信号输入、触摸输入等等。除了音频或视频输出之外，警报单元153可以以不同的方式提供输出以通知事件的发生。例如，警报单元153可以以振动的形式提供输出，当接收到呼叫、消息或一些其它进入通信(incoming communication)时，警报单元153可以提供触觉输出(即，振动)以将其通知给用户。通过提供这样的触觉输出，即使在用户的移动电话处于用户的口袋中时，用户也能够识别出各种事件的发生。警报单元153也可以经由显示单元151或音频输出模块152提供通知事件的发生的输出。

[0056] 存储器160可以存储由控制器180执行的处理和控制操作的软件程序等等，或者可以暂时地存储已经输出或将要输出的数据(例如，电话簿、消息、静态图像、视频等等)。而且，存储器160可以存储关于当触摸施加到触摸屏时输出的各种方式的振动和音频信号的数据。

[0057] 存储器160可以包括至少一种类型的存储介质，所述存储介质包括闪存、硬盘、多媒体卡、卡型存储器(例如，SD或DX存储器等等)、随机访问存储器(RAM)、静态随机访问存储器(SRAM)、只读存储器(ROM)、电可擦除可编程只读存储器 EEPROM)、可编程只读存储器(PROM)、磁性存储器、磁盘、光盘等等。而且，移动终端100可以与通过网络连接执行存储器160的存储功能的网络存储装置协作。

[0058] 控制器180通常控制移动终端的总体操作。例如，控制器180执行与语音通话、数据通信、视频通话等等相关的控制和处理。另外，控制器180可以包括用于再现(或回放)多媒体数据的多媒体模块1810，多媒体模块1810可以构造在控制器180内，或者可以构造为与控制器180分离。控制器180可以执行模式识别处理，以将在触摸屏上执行的手写输入或者图片绘制输入识别为字符或图像。

[0059] 电源单元190在控制器180的控制下接收外部电力或内部电力并且提供操作各元件和组件所需的适当的电力。

[0060] 这里描述的各种实施方式可以以使用例如计算机软件、硬件或其任何组合的计算机可读介质来实施。对于硬件实施，这里描述的实施方式可以通过使用特定用途集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理装置(DSPD)、可编程逻辑装置(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器、被设计为执行这里描述的功能的电子单元中的至少一种来实施，在一些情况下，这样的实施方式可以在控制器180中实施。对于软件实施，诸如过程或功能的实施方式可以与允许执行至少一种功能或操作的单独的软件模块来实施。软件代码可以由以任何适当的编程语言编写的软件应用程序(或程序)来实施，软件代码可以存储在存储器160中并且由控制器180执行。

[0061] 至此，已经按照其功能描述了移动终端。下面，为了简要起见，将描述诸如折叠型、直板型、摆动型、滑动型移动终端等等的各种类型的移动终端中的滑动型移动终端作为示例。因此，本发明能够应用于任何类型的移动终端，并且不限于滑动型移动终端。

[0062] 如图1中所示的移动终端100可以被构造为利用经由帧或分组发送数据的诸如有线和无线通信系统以及基于卫星的通信系统来操作。

[0063] 现在将参考图2描述其中根据本发明的移动终端能够操作的通信系统。

[0064] 这样的通信系统可以使用不同的空中接口和/或物理层。例如,由通信系统使用的空中接口包括例如频分多址(FDMA)、时分多址(TDMA)、码分多址(CDMA)和通用移动通信系统(UMTS)(特别地,长期演进(LTE))、全球移动通信系统(GSM)等等。作为非限制性示例,下面的描述涉及CDMA通信系统,但是这样的教导同样适用于其它类型的系统。

[0065] 参考图2,CDMA无线通信系统可以包括多个移动终端100、多个基站(BS)270、基站控制器(BSC)275和移动交换中心(MSC)280。MSC280被构造为与公共电话交换网络(PSTN)290形成接口。MSC280还被构造为与可以经由回程线路耦接到基站270的BSC275形成接口。回程线路可以根据若干已知的接口中的任一种来构造,所述接口包括例如E1/T1、ATM、IP、PPP、帧中继、HDSL、ADSL或xDSL。将理解的是,如图2中所示的系统可以包括多个BSC2750。

[0066] 每个BS270可以服务一个或多个分区(或区域),由多向天线或指向特定方向的天线覆盖的每个分区放射状地远离BS270。或者,每个分区可以由用于分集接收的两个或更多天线覆盖。每个BS270可以被构造为支持多个频率分配,并且每个频率分配具有特定频谱(例如,1.25MHz,5MHz等等)。

[0067] 分区与频率分配的交叉可以被称为CDMA信道。BS270也可以被称为基站收发器子系统(BTS)或者其它等效术语。在这样的情况下,术语“基站”可以用于笼统地表示单个BSC275和至少一个BS270。基站也可以被称为“蜂窝站”。或者,特定BS270的各分区可以被称为多个蜂窝站。

[0068] 如图2中所示,广播发射器(BT)295将广播信号发送给在系统内操作的移动终端100。如图1中所示的广播接收模块111被设置在移动终端100处以接收由BT295发送的广播信号。在图2中,示出了几个全球定位系统(GPS)卫星300。卫星300帮助定位多个移动终端100中的至少一个。

[0069] 在图2中,描绘了多个卫星300,但是理解的是,可以利用任何数目的卫星获得有用的定位信息。如图1中所示的GPS模块115通常被构造为与卫星300配合以获得想要的定位信息。替代GPS跟踪技术或者在GPS跟踪技术之外,可以使用可以跟踪移动终端的位置的其它技术。另外,至少一个GPS卫星300可以选择性地或者额外地处理卫星DMB传输。

[0070] 作为无线通信系统的一个典型操作,BS270接收来自各种移动终端100的反向链路信号。移动终端100通常参与通话、消息收发和其它类型的通信。特定基站270接收的每个反向链路信号被在特定BS270内进行处理。获得的数据被转发给相关的BSC275。BSC提供通话资源分配和包括BS270之间的软切换过程的协调的移动管理功能。BSC275还将接收到的数据路由到MSC280,其提供用于与PSTN290形成接口的额外的路由服务。类似地,PSTN290与MSC280形成接口,MS与BSC275形成接口,并且BSC275相应地控制BS270以将正向链路信号发送到移动终端100。

[0071] 基于上述移动终端硬件结构以及通信系统,提出本发明方法各个实施例。

[0072] 本发明提出了一种针对普通信息(短信/微信)的轻量级加密方式。采用C-S-C架构,在客户端进行特定操作(用力握持/挤压/),生成一散列值,在接收端需要进行同样的特定操作,生成同样的散列值,对比相同后才能阅读原报文,否则失败。

[0073] 所谓C-S-C即客户端-服务器-客户端,是一种比较典型的架构。两个客户端分别为发送端和接收端,发送端将明文发送给服务器,此外,将生成的散列值同时发送给服务器,

服务器作为认证中心,事先保存有发送端及接收端特定操作对应的散列值,当某一接收端的散列值与发送端发送给服务器的散列值一致时,服务器才将明文报文发送至该接收端。

[0074] 具体地,如图3所示,本发明提出了一种加密传输系统01,其特征在于,该系统包括:发送终端02和接收终端03。

[0075] 发送终端02,用于当需要发送信息时,检测施加在发送终端上的预定的操作;根据该操作生成预定的第一散列值;将携带有信息明文与第一散列值的报文发送给中间服务器。

[0076] 接收终端03,当需要接收信息时,接收中间服务器发送的报文,并检测施加在该接收终端上的与施加在发送该信息的发送终端上的操作相同的操作;并根据该操作生成预定的第二散列值,将第二散列值与报文中携带的第一散列值相比较,当第二散列值与第一散列值相匹配时,接收终端能够读取报文中所携带的信息明文。

[0077] 优选地,发送终端02和接收终端03均预存有预定的操作与预定的散列值之间的映射关系,并且发送终端02中预存的加密操作所对应的散列值与接收终端03中预存的相同的操作所对应的散列值相同。

[0078] 优选地,该系统还包括中间服务器04。

[0079] 中间服务器04预先保存不同的发送终端和不同的接收终端之间在进行加密传输时预定的操作所对应的不同的预定的散列值;其中,不同的预定的散列值与不同的发送终端以及不同的接收终端一一对应。

[0080] 中间服务器04接收到发送终端发送的报文后,将报文中携带的第一散列值与预存的一个或多个预定的散列值相比较,当第一散列值与预存的一个或多个预定的散列值中的任意一个相匹配时,将报文发送至与第一散列值相匹配的预定的散列值相对应的接收终端。

[0081] 需要说明的是,本发明实施例中的散列值可以通过对原文进行HASH运算获得(类似于报文摘要),也可以通过预设的映射关系表获得,当检测并识别该特定操作后,直接通过映射关系表获得相应的散列值。

[0082] 在本发明实施例中,采用散列技术与预定操作相结合的方法进行加密,该过程是一种轻量级的鉴权过程,通过简单的动作手势完成轻加密。在轻量级的通信方式中均可采用该加密方式,适用范围广泛,并且相对于传统的数字证书,数字签名方式,该方式更简单、更高效。

[0083] 散列方法是将值从一个大的(可能很大)定义域映射到一个较小值域的(数学)函数。散列方法不同于顺序查找、二分查找、二叉排序树及B-树上的查找。它不以关键字的比较为基本操作,采用直接寻址技术。在理想情况下,无须任何比较就可以找到待查关键字,查找的期望时间为O(1),快捷、高效。

[0084] 在实际的签名应用中,总是先将要签署的数据通过散列函数运算为固定长度的比特串,然后用私钥对该比特串进行运算,所得到的结果作为原始数据的签名,故散列函数的好坏对于数字签名应用至关重要。目前常见的散列函数如MD5、SHA-1,但在本发明实施例中不限于上述两种散列函数,任何适用于本发明的散列函数都在本发明保护范围之内。

[0085] 优选地,预定的操作包括以下形式的一种或多种:对终端的用力握持、挤压、按压、滑动以及密码输入。

[0086] 在本发明实施例中,该预定的操作不仅仅限于上述的操作形式,能够施加在终端上的任何适用于本发明的操作都在本发明的保护范围之内。

[0087] 另外,在本发明实施例中,也不限制终端中使用何种形式的操作检测方法,如,对施加的压力进行压力形式和/或压力等级的检测;对指纹进行用户指纹的图像和/或用户指纹的滑动方式的检测;对密码输入顺序和/或密码输入类型的检测。下面将分别针对不同的操作形式的检测做详细说明。

[0088] 首先,针对压力形式和/或压力等级的检测进行说明:

[0089] 优选地,

[0090] 压力形式包括:单次点击按压、持续按压、多次连续点击按压。

[0091] 压力等级包括:

[0092] 在单次点击按压时,单次点击按压的按压力度等级。

[0093] 在持续按压时,持续按压的持续按压时间等级。

[0094] 在多次连续点击按压时,多次连续点击按压的连续点击次数等级。

[0095] 在本发明实施例中,可以有三种检测方案:

[0096] 方案一、用户可以仅对压力形式进行检测,如,仅检测用户是单次点击按压还是持续按压。

[0097] 在该方案中,对压力形式进行检测,就需要对压力的压力形式进行判断,具体如何对压力的压力形式进行判断,我们可以通过以下方式:

[0098] 方式一、首先通过检测预定时间内的按压次数来检测是单次按压还是多次按压。在这里,对于一种按压操作来说,为了防止误操作等情况的发生,我们必须对该按压进行一定的限制,在限制范围内的才能算作有效按压,本发明中的预定时间就是本发明方案对所施加压力的一种限制条件,只有在该预定时间内完成的按压才算有效按压。这里的预定时间我们可以根据不同的应用场景进行不同的设置,例如,对于年轻人来说,动作比较灵活,可以将该时间定的短一些,如1秒或0.5秒,终端检测1秒或0.5秒内按压的次数,来确定是单次按压还是多次按压;对于老年人、儿童以及残障人士来说,动作不太灵活,可以将该时间定的长一些,如2秒或3秒等,终端检测2秒或3秒内的按压次数,来确定是单次按压还是多次按压。

[0099] 在上述步骤中,我们通过检测预定时间内的按压次数确定了是单次按压还是多次按压以后,如果是多次按压,可以毫无疑问的可以确定该压力为多次连续点击按压的形式,但如果是单次按压,我们还需要进一步判定该单次按压是单次点击按压形式,还是持续按压形式。这里我们设置了第二个限制条件,即第二预定时间,因为区分一个按压是点击按压还是持续按压的标准就是该压力的持续时间,这里需要说明的是,这个第二预定时间与上述的第一预定时间可以相同也可以不同,同样是可以根据不同的用户情况进行不同的设置,这种情况其实在上述的优先区分该压力是持续按压还是点击按压时已经进行了详细描述,其情况与此时的情况完全形同,这里的第二预定时间也可以根据个人的不同习惯进行不同的设置,例如,某些人行动利落,性格较急,可以将该时间定的短一些,如1秒或2秒,终端检测该压力是否持续了1秒或2秒,来确定是单次按压还是多次按压,如果持续了1秒或2秒,则可判定该压力为持续按压,如果未持续1秒或2秒,则可判定该压力为单次点击按压;对于行动缓慢或性格缓慢的人来说,可以将该时间定的长一些,如3秒或4秒等,终端检测3

秒或4秒内的按压次数,来确定是单次按压还是多次按压,如果持续了3秒或4秒,则可判定该压力为持续按压,如果未持续3秒或4秒,则可判定该压力为单次点击按压。

[0100] 方式二、也可以通过其他的检测形式首先检测其他的按压形式,如,首先通过一个压力的持续时间检测该压力是持续按压还是点击按压。这里的预定的持续时间我们可以根据个人的不同习惯进行不同的设置,例如,某些人行动利落,性格较急,可以将该时间定的短一些,如1秒或2秒,终端检测该压力是否持续了1秒或2秒,来确定是单次按压还是多次按压;对于行动缓慢或性格缓慢的人来说,可以将该时间定的长一些,如3秒或4秒等,终端检测3秒或4秒内的按压次数,来确定是单次按压还是多次按压。

[0101] 在上述步骤中,我们通过检测一个压力的持续时间确定了是持续按压还是点击按压以后,如果是持续按压,可以毫无疑问的可以确定该压力为持续按压的形式,但如果是点击按压,我们还需要进一步判定该点击按压是单次点击按压形式,还是多次连续点击按压形式。在这一判断中,方法同上述的方式一种的初始判断方式一样,可以通过检测预定时间内的按压次数来检测是单次按压还是多次按压,这里不再赘述。

[0102] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0103] 方案二、也可以在默认某一种压力形式的情况下,仅对压力等级进行检测,如,默认的压力形式为单次点击,仅对每单次按压的力度等级来实施检测,检测该压力的力度等级是否发到了预定的阈值。

[0104] 在上述的方案一种,我们确定了用户所施加压力的压力形式以后,可以仅针对某一压力形式说对应的压力等级进行检测,即,仅用某一压力形式说对应的压力等级作为激活指令。下面分别针对三种压力形式对应的三种压力等级分别说明不同形式下的压力等级的检测方式。

[0105] 方式一、在单次点击按压时,检测单次点击按压的按压力度等级。

[0106] 在单次点击按压时,对单次点击按压的按压力度等级的确定包括:

[0107] 当确定该压力的按压形式为单次点击按压时,将压力的压力值的大小与预定的不同的按压力度范围进行比较,当压力的压力值的大小属于不同的按压力度范围中的任何一个时,将该压力确定为所属的该按压力度范围所对应的按压力度等级;当压力的压力值的大小不属于该不同的按压力度范围中的任何一个时,确定该压力无效。

[0108] 在本发明实施例中,为了明确外界对终端的压力的大小,我们预先将不同的压力值定义为不同的力度等级,如力度等级1、力度等级2、力度等级3……依此类推。具体每个等级中对应的压力值的大小为多少可以依据不同的用户进行不同的定义,如,对于年轻人来说,力量较大,在力度等级设置中每一个等级中可以设置为对应较大的压力值,如,50g-60g属于力度等级1、60g-70g属于力度等级2、70g-80g属于力度等级3(需要说明的是,由于重力加速度恒定,这里以重量来表示压力的大小,以下描述同理。);对于老年人和儿童来说,力量较小,在力度等级设置中每一个等级中可以设置为对应较小的压力值,如,20g-35g属于力度等级1、35g-50g属于力度等级2、50g-65g属于力度等级3。上述内容仅是本发明的一个具体实施例,在其它实施例中,我们也可以根据不同的应用场景对力度等级及每个力度等级对应的压力值的大小做相应的调整。

[0109] 在上述内容中,我们详细介绍了如何对压力的力度等级进行了预定义。下面通过具体实施例详细介绍如何通过预定的压力力度等级范围确定施加在终端上的压力的力度等级。这里继续以上述实施例中定义的年轻人的力度等级范围为例来进行说明,在上述实施例中,我们提到,对于年轻人来说,力量较大,在力度等级设置中每一个等级中可以设置为对应较大的压力值,如,50g-60g属于力度等级1、60g-70g属于力度等级2、70g-80g属于力度等级3(需要说明的是,由于重力加速度恒定,这里以重量来表示压力的大小,以下描述同理。);仍以此范围为例,如果外界对终端施加了一个压力,检测到该压力的压力大小为75g,这时将这个75g的力分别与上述的压力范围50g-60g、60g-70g、70g-80g进行比较,比较结果可知,这个75g的力属于70g-80g的力度范围内,并且该70g-80g的力度范围对应预先设置的力度等级3,因此将外界对终端施加的这个75g的力确定为力度等级3。

[0110] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0111] 方式二、在持续按压时,持续按压的持续按压时间等级。

[0112] 在持续按压时,对持续按压的持续按压时间等级的确定包括:

[0113] 当确定该压力的按压形式为持续按压时,将压力的持续时间与预定的不同的持续按压时间范围进行比较,当压力的持续时间属于不同的持续按压时间范围中的任何一个时,将该压力确定为所属的该持续按压时间范围所对应的持续按压时间等级;当压力的持续时间不属于该不同的持续按压时间范围中的任何一个时,确定该压力无效。

[0114] 在本发明实施例中,为了明确外界对终端的压力的持续时间的长短,我们预先将不同的持续时间定义为不同的持续时间等级,如持续时间等级1、持续时间等级2、持续时间等级3……依此类推。如,持续1秒代表到了持续时间等级1,持续2秒代表到了持续时间等级2,持续3秒代表到了持续时间等级3,……依此类推,并且每个等级中对应的压力持续时间可以依据不同的用户进行不同的定义,如,可以根据个人的不同习惯进行不同的设置,例如,某些人行动利落,性格较急,可以将该持续时间定的短一些,如,持续1秒代表到了持续时间等级1,持续1.5秒代表到了持续时间等级2,持续2秒代表到了持续时间等级3,……依此类推;即,1-1.5秒代表持续时间等级1,1.5-2秒代表持续时间等级2,2秒以上范围代表持续时间等级3。

[0115] 对于行动缓慢或性格缓慢的人来说,可以将该持续时间定的长一些,如,持续1秒代表到了持续时间等级1,持续2秒代表到了持续时间等级2,持续3秒代表到了持续时间等级3,……依此类推;即,1-2秒代表持续时间等级1,2-3秒代表持续时间等级2,3秒以上范围代表持续时间等级3。上述内容仅是本发明的一个具体实施例,在其它实施例中,我们也可以根据不同的应用场景对持续时间等级及每个持续时间等级对应的持续时间的长短做相应的调整。

[0116] 在上述内容中,我们详细介绍了如何对压力的持续时间等级进行了预定义。下面通过具体实施例详细介绍如何通过预定的压力持续时间等级范围确定施加在终端上的压力的持续时间等级。这里继续以上述实施例中定义的行动利落,性格较急的人的持续时间等级范围为例来进行说明,在上述实施例中,我们提到,对于行动利落,性格较急的人来说,可以将该持续时间定的短一些,如,持续1秒代表到了持续时间等级1,持续1.5秒代表

到了持续时间等级2,持续2秒代表达到了持续时间等级3,……依此类推;即,1-1.5秒代表持续时间等级1,1.5-2秒代表持续时间等级2,2秒以上范围代表持续时间等级3。仍以此范围为例,如果外界对终端施加了一个压力,检测到该压力的持续时间为1.3秒,这时将这个持续了1.3秒的力分别与上述的压力范围1-1.5秒、1.5-2、2秒以上进行比较,比较结果可知,这个持续了1.3秒的力属于1-1.5秒的持续时间范围内,并且该1-1.5秒的持续时间范围对应预先设置的持续时间等级1,因此将外界对终端施加的这个持续了1.3秒的力确定为持续时间等级1。

[0117] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0118] 方式三、在多次连续点击按压时,多次连续点击按压的连续点击次数等级。

[0119] 在多次连续点击按压时,对多次连续点击按压的连续点击次数等级的确定包括:

[0120] 当确定该压力的按压形式为多次连续点击按压时,将压力的连续点击次数与预定的不同的连续点击次数阈值进行比较,当压力的连续点击次数符合不同的连续点击次数阈值中的任何一个时,将该压力确定为所符合的该连续点击次数阈值所对应的连续点击次数等级;当压力的连续点击次数不符合该不同的连续点击次数阈值中的任何一个时,确定该压力无效。

[0121] 在本发明实施例中,为了明确外界对终端的按压的连续点击次数,我们预先将不同的连续点击次数定义为不同的连续点击次数等级,如连续点击次数等级1、连续点击次数等级2、连续点击次数等级3……依此类推。如,连续点击1次代表到了连续点击次数等级1,连续点击2次代表到了连续点击次数等级2,连续点击3次代表到了连续点击次数等级3,……依此类推,并且每个等级中对应的连续点击次数可以依据不同的用户进行不同的定义,如,可以根据个人的不同习惯进行不同的设置,例如,某些人行动利落,性格较急,可以将该连续点击次数定的少一些,如,连续点击1次代表到了连续点击次数等级1,连续点击2次代表到了连续点击次数等级2,连续点击3次代表到了连续点击次数等级3,……依此类推。

[0122] 对于行动缓慢或性格缓慢的人来说,可以将该连续点击次数定的多一些,如,连续点击2次代表到了连续点击次数等级1,连续点击3次代表到了连续点击次数等级2,连续点击4次代表到了连续点击次数等级3,……依此类推。上述内容仅是本发明的一个具体实施例,在其它实施例中,我们也可以根据不同的应用场景对持续时间等级及每个持续时间等级对应的持续时间的长短做相应的调整。

[0123] 在上述内容中,我们详细介绍了如何对按压的连续点击次数等级进行预定义。下面通过具体实施例详细介绍如何通过预定的连续点击次数等级确定施加在终端上的连续点击次数的等级。这里继续以上述实施例中定义的行动利落,性格较急的人的连续点击次数等级为例来进行说明,在上述实施例中,我们提到,对于行动利落,性格较急的人来说,可以将该连续点击次数定的少一些,如,连续点击1次代表到了连续点击次数等级1,连续点击2次代表到了连续点击次数等级2,连续点击3次代表到了连续点击次数等级3,……依此类推。仍以此等级为例,如果外界对终端施加了一个按压压力,检测到该按压压力的连续点击次数为2次,这时将这个连续点击次数为2次的力分别与上述的压力等级进行比较,

比较结果可知,这个连续点击次数为2次的力属于连续点击次数等级2,因此将外界对终端施加的这个连续点击次数为2次的力确定为连续点击次数等级2。

[0124] 在这里,对于检测一个按压的按压次数来说,必须是在一定时间内完成的按压次数,不能无限延时来确定一个按压的按压次数,这是毫无意义的,因此,我们必须对该按压进行一定的限制,在限制范围内达到的按压次数才能算作有效按压,本发明中对该按压次数设置的预定时间就是本发明方案对所施加压力的一种限制条件,只有在该预定时间内完成的按压次数才算有效按压。这里的预定时间我们可以根据不同的应用场景进行不同的设置,例如,对于年轻人来说,动作比较灵活,可以将该时间定的短一些,如1秒或0.5秒,终端检测1秒或0.5秒内按压的次数来确定是都为有效按压;对于老年人、儿童以及残障人士来说,动作不太灵活,可以将该时间定的长一些,如2秒或3秒等,终端检测2秒或3秒内的按压次数来确定是都为有效按压。

[0125] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0126] 方案三、用户还可将不同的压力形式和不同的按压等级相结合进行检测,如,先检测用户的压力形式是单次点击按压、持续按压还是多次连续点击按压,在压力形式确定以后再进一步检测施加的压力等级,如,如果确定了用户压力的压力形式为持续按压,进一步检测该持续按压的按压持续时间;或者,如果确定了用户压力的压力形式为多次连续点击按压,进一步检测多次连续点击按压后的最后一次点击的按压持续时间;或者,如果确定了用户压力的压力形式为持续按压,进一步检测该持续按压的按压力度等。

[0127] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0128] 其次、将针对用户指纹的图像和/或用户指纹的滑动方式的检测进行说明:

[0129] 在本发明实施例中,可以有三种检测方案:

[0130] 方案一:终端可以仅对用户指纹的图像信息进行检测。

[0131] 对用户指纹的图像信息的检测包括:扫描放置在指纹识别装置上的手指的指纹,并记录该手指指纹的图像信息,将该图像信息与终端中预存的用户的专有指纹图像信息相比较,判定记录的图像信息与预存的用户的专有指纹图像信息是否相匹配。

[0132] 在对用户指纹的图像信息进行检测以后,通过上述的判定结果来生成与该判定结果相对应的散列值,我们可以通过以下几种判定结果来生成不同的散列值:

[0133] 情况一、记录的图像信息与预存的用户的专有指纹图像信息相匹配,和/或用户的手指一直处于该指纹识别装置上。

[0134] 情况二、记录的图像信息与预存的用户的专有指纹图像信息相匹配,和/或用户的手指在预定时间内与该指纹识别装置进行过匹配。

[0135] 方案二:终端可以仅对用户指纹的滑动方式信息进行检测。

[0136] 对用户指纹的图像信息的检测包括:扫描手指在指纹识别装置上的滑动操作,并记录该手指的滑动操作方式,将该滑动操作方式与终端中预存的滑动方式相比较,判定记录的该手指的滑动操作方式与预存的滑动方式是否相匹配。

[0137] 这里需要说明的是,指纹的滑动方式包括用户可执行的任意滑动方式,如,左右滑动、上下滑动,以及用户自定义的任意滑动图形,如,以圆圈滑动、以三角形滑动、以字母形式进行滑动、以数字形式进行滑动等。

[0138] 在对用户指纹的滑动方式进行检测以后,通过上述的判定结果来生成与该判定结果相对应的散列值,我们可以通过以下几种判定结果来生成不同的散列值:

[0139] 情况一、如果记录的滑动操作方式与终端中预存的滑动方式相匹配,和/或用户的手指一直处于该指纹识别装置上。

[0140] 情况二、如果记录的滑动操作方式与终端中预存的滑动方式相匹配,和/或用户的手指在预定时间内与在该指纹识别装置上滑动过。

[0141] 方案三:终端可以对用户指纹的图像信息和指纹的滑动方式信息相结合进行检测。

[0142] 相结合的检测方案是指,对用户的指纹的图像信息进行检测以后再检测指纹的滑动方式信息,或者对用户的指纹的滑动方式信息进行检测以后再检测指纹的图像信息,只有在两种检测的结果都与预存信息相匹配时才能生成相应的散列值;两种检测的结果任何一个与预存信息不匹配时不会生成相应的散列值。另外,该结合方案还可以如上所述,与手指在指纹识别装置上的停留状态相结合,或者与用户的手指在预定时间内是否在该指纹识别装置上有过操作的情况相结合,在此不再赘述。

[0143] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0144] 最后、将针对密码输入顺序和/或密码输入类型的检测进行说明:

[0145] 在本发明实施例中,可以有三种检测方案:

[0146] 方案一、终端可以仅对密码输入顺序进行检测。

[0147] 对用户的密码输入顺序进行检测包括:记录用户输入某一密码的先后顺序,将该先后顺序与终端中预存的输入顺序相比较,判定记录的先后顺序与预存的输入顺序是否相匹配。

[0148] 具体地,记录用户输入某一密码的先后顺序包括:记录输入键盘上的第几行第几列的按键的先后按动次序。如,优先按动第一行第二列的按键、第二次按动第二行第三列的按键、第三次按动第一行第五列的按键,这一按键的按动顺序便可以作为一种密码输入顺序,对应一个散列值。当然,对于输入键盘上哪是第一行或哪是第一列的定义可以进行自行设置。并且,上述内容中提到的键盘可以是常规的硬件键盘,也可以是触摸屏的输入键盘,总之,在本发明实施例中不对该键盘的具体形式作严格限制,只要能完成本发明的密码输入的任何形式或意义上的键盘均可。

[0149] 方案二、终端可以仅对密码输入类型进行检测。

[0150] 对用户的密码输入类型进行检测包括:记录用户输入某一密码的类型,将该输入类型与终端中预存的输入类型相比较,判定记录的输入类型与预存的输入类型是否相匹配。

[0151] 在本发明实施例中,密码输入类型可以包括:数字、字母、字符串、图画、线条、二进制码以及自定义的任意图形或图像等,总之,本发明不对该输入类型做具体限制,任何可以

作为输入的形体或类型均可。

[0152] 具体地,对用户的密码输入类型进行检测举例说明:如,如果在终端中记录的输入类型为数字,当用户在输入窗口上输入一个数字1或2时,该输入类型与终端记录的类型相匹配,则可以生成相应的散列值。如果在终端中记录的输入类型为数字,当用户在输入窗口上输入一个字母a或m时,该输入类型与终端记录的类型不匹配,则不会生成相应的散列值。或者,如果在终端中记录的输入类型为二进制码,当用户在输入窗口上输入1111时,该输入类型与终端记录的类型相匹配,则可以生成相应的散列值。如果在终端中记录的输入类型为二进制码,当用户在输入窗口上输入一个阿拉伯数字16时,该输入类型与终端记录的类型不匹配,则不会生成相应的散列值。

[0153] 方案三、终端可以对密码输入顺序和密码输入类型相结合进行检测。

[0154] 相结合的检测方案是指,对用户的密码输入顺序进行检测以后再检测密码输入类型,或者对用户的密码输入类型进行检测以后再检测密码输入顺序,只有在两种检测的结果都与预存信息相匹配时才能生成相应的散列值;两种检测的结果任何一个与预存信息不匹配时不会生成相应的散列值。

[0155] 举例说明,如,如果在终端中记录的输入类型为数字,输入顺序为2468,则当我们输入2468时,会生成相应的散列值,反之,如果我们同样是按照预定的键盘顺序输入,但相应的按键上还会输入@￥……\*等符号,当我们输入@￥……\*时,虽然输入顺序正确,但输入的类型不是数字,则不会生成相应的散列值。

[0156] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0157] 以上内容详细描述了对于各种操作的检测方式,下面继续对终端中的检测装置作进一步说明。

[0158] 在本发明实施例中,不限制终端中使用何种操作检测装置,如,压力传感器、指纹识别装置和/或输入键盘等,并且对操作检测装置在终端上的安装位置也不作要求,可以在屏幕上,也可以在侧面边框、底壳上等,也可以与其它的功能键复用。并且本发明中的操作检测装置可以是一个或多个,并且每种类型的操作装置可以单独使用,也可以混合使用。

[0159] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0160] 本发明还提供了一种加密传输终端,该终端用于:

[0161] 当需要发送信息时,检测施加在终端上的预定的操作;根据该操作生成预定的第一散列值;将携带有信息明文与第一散列值的报文发送给中间服务器。

[0162] 当需要接收信息时,接收中间服务器发送的报文,并检测施加在该终端上的与施加在发送该信息的终端上的操作相同的操作;并根据该操作生成预定的第二散列值,将第二散列值与报文中携带的第一散列值相比较,当第二散列值与第一散列值相匹配时,终端能够读取报文中所携带的信息明文。

[0163] 优选地,预定的加密操作包括以下形式的一种或多种:对发送终端和接收终端的用力握持、挤压、按压、滑动以及密码输入。

[0164] 需要说明的是,在发送消息时,为了与接收消息时生成的散列值相区分,这里称为第一散列值,发送消息时称为第二散列值。另外,在终端中可以预存不同的操作与不同的第一散列值或不同的第二散列值的映射关系表,不同的操作与不同的散列值需一一对应。另外,本发明实施例中的散列值可以通过对原文进行HASH运算获得(类似于报文摘要),也可以通过预设的映射关系表获得,当检测并识别该特定操作后,直接通过映射关系表获得相应的散列值。

[0165] 另外,在这里,如对加密传输系统的说明中所述,在本发明实施例中不限于MD5、SHA-1两种散列函数,任何适用于本发明的散列函数都在本发明保护范围之内。本发明实施例中的预定的操作也不仅仅限于上述的操作形式,能够施加在终端上的任何适用于本发明的操作都在本发明的保护范围之内。并且,在本发明实施例中,也不限制终端中使用何种形式的操作检测方法,如,对施加的压力进行压力形式和/或压力等级的检测;对指纹进行用户指纹的图像和/或用户指纹的滑动方式的检测;对密码输入顺序和/或密码输入类型的检测。在本发明实施例中,不限制终端中使用何种操作检测装置,如,压力传感器、指纹识别装置和/或输入键盘等,并且对操作检测装置在终端上的安装位置也不作要求,可以在屏幕上,也可以在侧面边框、底壳上等,也可以与其它的功能键复用。并且本发明中的操作检测装置可以是一个或多个,并且每种类型的操作装置可以单独使用,也可以混合使用。在加密传输终端中的任何实施例同样适用于本发明的加密传输系统。

[0166] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0167] 此外,本发明还提出了一种中间服务器,该中间服务器用于:

[0168] 预先保存不同的发送终端和不同的接收终端之间在进行加密传输时预定的操作所对应的不同的预定的散列值;其中,不同的预定的散列值与不同的发送终端以及不同的接收终端一一对应。

[0169] 接收到发送终端发送的报文后,将报文中携带的第一散列值与预存的一个或多个预定的散列值相比较,当第一散列值与预存的一个或多个预定的散列值中的任意一个相匹配时,将报文发送至与第一散列值相匹配的该预定的散列值相对应的接收终端。

[0170] 优选地,预定的操作包括以下形式的一种或多种:对发送终端和接收终端的用力握持、挤压、按压、滑动以及密码输入。

[0171] 需要说明的是,在这里,如对加密传输系统的说明中所述,在本发明实施例中不限于MD5、SHA-1两种散列函数,任何适用于本发明的散列函数都在本发明保护范围之内。本发明实施例中的散列值可以通过对原文进行HASH运算获得(类似于报文摘要),也可以通过预设的映射关系表获得,当检测并识别该特定操作后,直接通过映射关系表获得相应的散列值。本发明实施例中的预定的操作也仅仅限于上述的操作形式,能够施加在终端上的任何适用于本发明的操作都在本发明的保护范围之内。并且,在本发明实施例中,也不限制终端中使用何种形式的操作检测方法,如,对施加的压力进行压力形式和/或压力等级的检测;对指纹进行用户指纹的图像和/或用户指纹的滑动方式的检测;对密码输入顺序和/或密码输入类型的检测。在本发明实施例中,不限制终端中使用何种操作检测装置,如,压力传感器、指纹识别装置和/或输入键盘等,并且对操作检测装置在终端上的安装位置也不作

要求,可以在屏幕上,也可以在侧面边框、底壳上等,也可以与其它的功能键复用。并且本发明中的操作检测装置可以是一个或多个,并且每种类型的操作装置可以单独使用,也可以混合使用。在加密传输终端中的任何实施例同样适用于本发明的中间服务器。

[0172] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0173] 此外,为实现上述目的,本发明还提出一种加密传输方法,该方法包括:

[0174] 当需要发送信息时,检测施加在发送终端上的预定的操作;根据该操作生成预定的第一散列值;将携带有信息明文与所述第一散列值的报文发送给中间服务器。

[0175] 当需要接收信息时,接收所述中间服务器发送的报文,并检测施加在接收终端上的与施加在发送该信息的发送终端上的操作相同的操作;并根据该操作生成预定的第二散列值,将第二散列值与报文中携带的第一散列值相比较,当第二散列值与第一散列值相匹配时,接收终端能够读取所述报文中所携带的信息明文。

[0176] 优选地,该方法还包括:

[0177] 在中间服务器中预先保存不同的发送终端和不同的接收终端之间在进行加密传输时预定的加密操作所对应的不同的预定的散列值;其中,不同的预定的散列值与不同的发送客户端以及不同的接收客户端一一对应。

[0178] 在中间服务器接收到发送终端发送的报文后,将报文中携带的第一散列值与预存的一个或多个预定的散列值相比较,当第一散列值与预存的一个或多个预定的散列值中的任意一个相匹配时,将报文发送至与第一散列值相匹配的预定的散列值相对应的接收终端。

[0179] 优选地,发送终端和接收终端中均预存有预定的操作与预定的散列值之间的映射关系,并且发送终端中预存的加密操作所对应的散列值与接收终端中预存的相同的操作所对应的散列值相同。

[0180] 优选地,预定的加密操作包括以下形式的一种或多种:对发送终端和接收终端的用力握持、挤压、按压、滑动以及密码输入。

[0181] 需要说明的是,在这里,如对加密传输系统的说明中所述,在本发明实施例中不限于MD5、SHA-1两种散列函数,任何适用于本发明的散列函数都在本发明保护范围之内。本发明实施例中的散列值可以通过对原文进行HASH运算获得(类似于报文摘要),也可以通过预定的映射关系表获得,当检测并识别该特定操作后,直接通过映射关系表获得相应的散列值。本发明实施例中的预定的操作也不仅仅限于上述的操作形式,能够施加在终端上的任何适用于本发明的操作都在本发明的保护范围之内。并且,在本发明实施例中,也不限制终端中使用何种形式的操作检测方法,如,对施加的压力进行压力形式和/或压力等级的检测;对指纹进行用户指纹的图像和/或用户指纹的滑动方式的检测;对密码输入顺序和/或密码输入类型的检测。在本发明实施例中,不限制终端中使用何种操作检测装置,如,压力传感器、指纹识别装置和/或输入键盘等,并且对操作检测装置在终端上的安装位置也不作要求,可以在屏幕上,也可以在侧面边框、底壳上等,也可以与其它的功能键复用。并且本发明中的操作检测装置可以是一个或多个,并且每种类型的操作装置可以单独使用,也可以混合使用。在加密传输终端中的任何实施例同样适用于本发明的中间服务器。

[0182] 需要说明的是,上述内容仅是本发明的一种具体实施例,任何与上述实施例相同或相似的方案,以及上述实施例的变体都在本发明的保护范围之内,并且上述实施例和本发明涉及的任何基本方案特征的任意组合也均在本发明的保护范围之内。

[0183] 下面通过完整的操作流程具体说明本发明的操作方案。

[0184] 示例1(接收终端鉴权),如图4所示:

[0185] S101、发送终端及接收终端设置特定的操作。

[0186] 特定操作可以为按压挤压手机两侧边缘位置,手机两侧分布有压力传感器,通过压力传感器检测按压力度大小,当按压力度超过一定值的时候则识别为特定操作。需要说明的是,特定操作方式包括但不限于挤压,在手机边缘(边框)按压或者滑动等,对于智能终端而言,特定操作尽管操作方式不同,但目的相同,均是为了生成标识符,方便后续进行判断。

[0187] S102、发送终端检测到施加在发送终端上的特定操作时,生成一个与该特定操作相对应的散列值(标识符)。

[0188] 当检测并识别出施加在发送终端上的特定操作与预存的特定操作相符时,发送终端生成与该特定操作相对应的散列值(标识符),该散列值可以通过对原文进行HASH运算获得(类似于报文摘要),也可以定义一个不同的特定操作与不同的散列值的映射关系表,该映射关系表同时存在于发送终端与接收终端,用于进行鉴权,当检测并识别该特定操作后,直接通过映射关系表获得相应的散列值。

[0189] S103、发送终端发送报文至中间服务器。

[0190] 报文中携带有明文和散列值,散列值作为标识符,放在报头,供后续接收终端鉴权使用。

[0191] S104、中间服务器根据该散列值将该报文发送至相应的接收终端。

[0192] S105、接收终端接收到该报文后,生成一散列值,通过将生成的散列值与报文中的散列值相比对,判断是否匹配,若匹配则打开该报文,否则打开失败。

[0193] 对于接收终端而言,接收到该报文时只产生一个消息提示响应,但具体的明文暂不可见,需要接收终端作出同样的特定操作,从而生成同样的散列值(标识符),当收到的散列值和生成的散列值相匹配时,才能打开文件。生成散列值是根据事先保存的特定操作与散列值的映射关系表生成的,例如接收终端做出与发送终端同样的按压操作,则查询该映射关系表后,按压操作对应的散列值为H(x),则生成的散列值即为H(x)。

[0194] 对于用户而言,其操作可以简单描述为:用户A发送消息前,按压手机,该消息转发至用户B,用户B实现同样的操作,打开该消息,否则打开失败。

[0195] 示例2(中间服务器进行鉴权),如图5所示:

[0196] S201、发送终端及接收终端设置特定的操作。

[0197] 特定操作可以为按压挤压手机两侧边缘位置,手机两侧分布有压力传感器,通过压力传感器检测按压力度大小,当按压力度超过一定值的时候则识别为特定操作。需要说明的是,特定操作方式包括但不限于挤压,在手机边缘(边框)按压或者滑动等,对于智能终端而言,特定操作尽管操作方式不同,但目的相同,均是为了生成标识符,方便后续进行判断。

[0198] S202、发送终端检测到施加在发送终端上的特定操作时,生成一个与该特定操作

相对应的散列值(标识符)。

[0199] 当检测并识别出施加在发送终端上的特定操作与预存的特定操作相符时,发送终端生成与该特定操作相对应的散列值(标识符),该散列值可以通过对原文进行HASH运算获得(类似于报文摘要),也可以定义一个不同的特定操作与不同的散列值的映射关系表,该映射关系表同时存在于发送端与接收端,用于进行鉴权,当检测并识别该特定操作后,直接通过映射关系表获得相应的散列值。

[0200] S203、发送终端将明文及散列值发送到中间服务器。

[0201] S204、中间服务器将发送一消息提示给接收终端,该消息提示并不附带真正的明文。

[0202] S205、接收终端将生成的散列值发送给中间服务器。

[0203] 该散列值为接收端自己生成的散列值,接收终端做出与发送终端相同的特定操作,从而生成相同的散列值(标识符),具体过程同S105。

[0204] S206、中间服务器判断发送终端和接收终端发送的散列值是否相同,若相同则下发明文至接收终端,供接收终端进行查阅。

[0205] 该过程是一种轻量级的鉴权过程,通过简单的动作手势完成轻加密。对于轻量级的通信方式中可采用该方式,相对于传统的数字证书,数字签名方式,该方式更加高效,简单。

[0206] 需要说明的是,在本文中,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0207] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0208] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算机,服务器,空调器,或者网络设备等)执行本发明各个实施例所述的方法。

[0209] 以上仅为本发明的优选实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本发明的专利保护范围内。

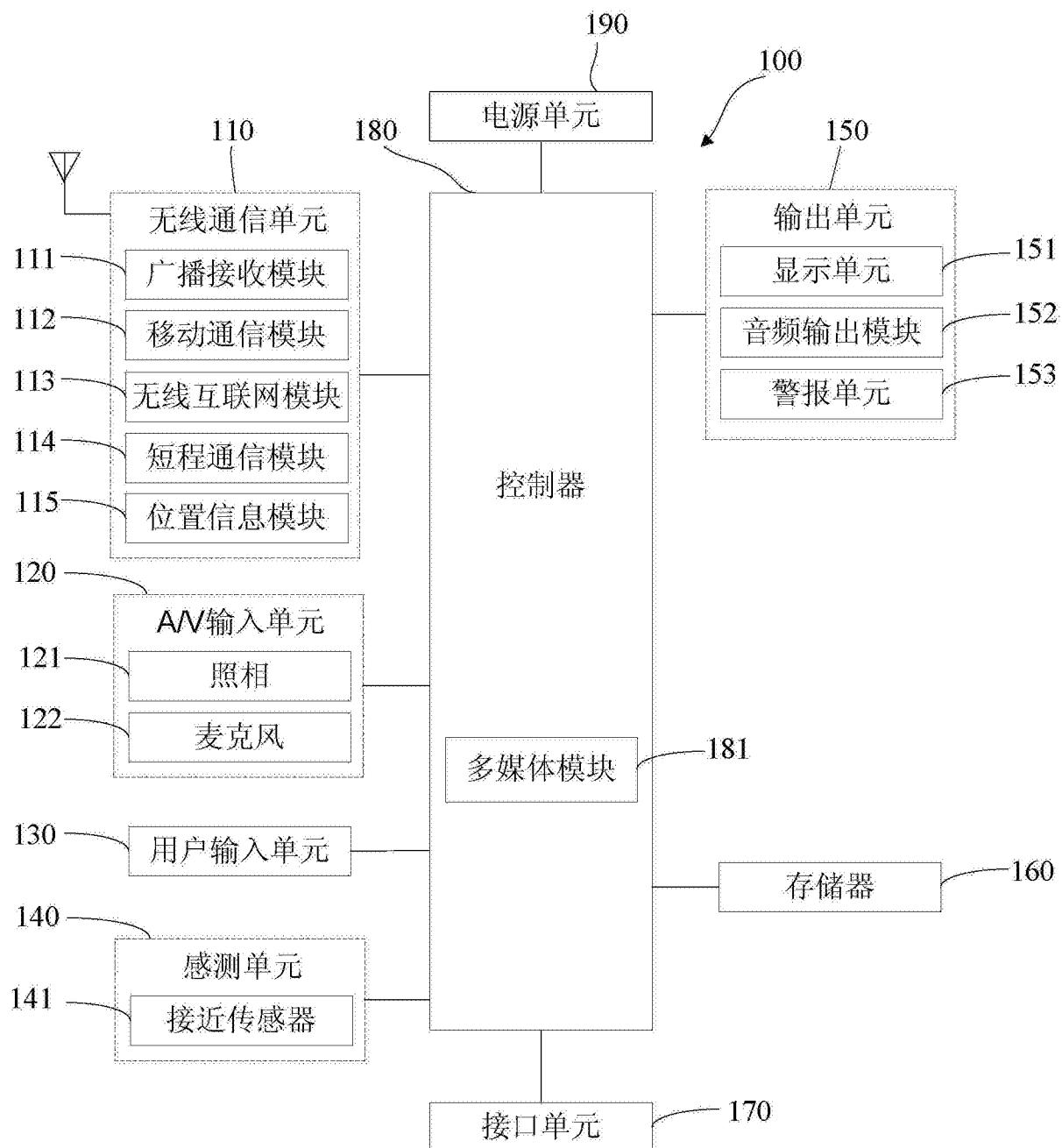


图1

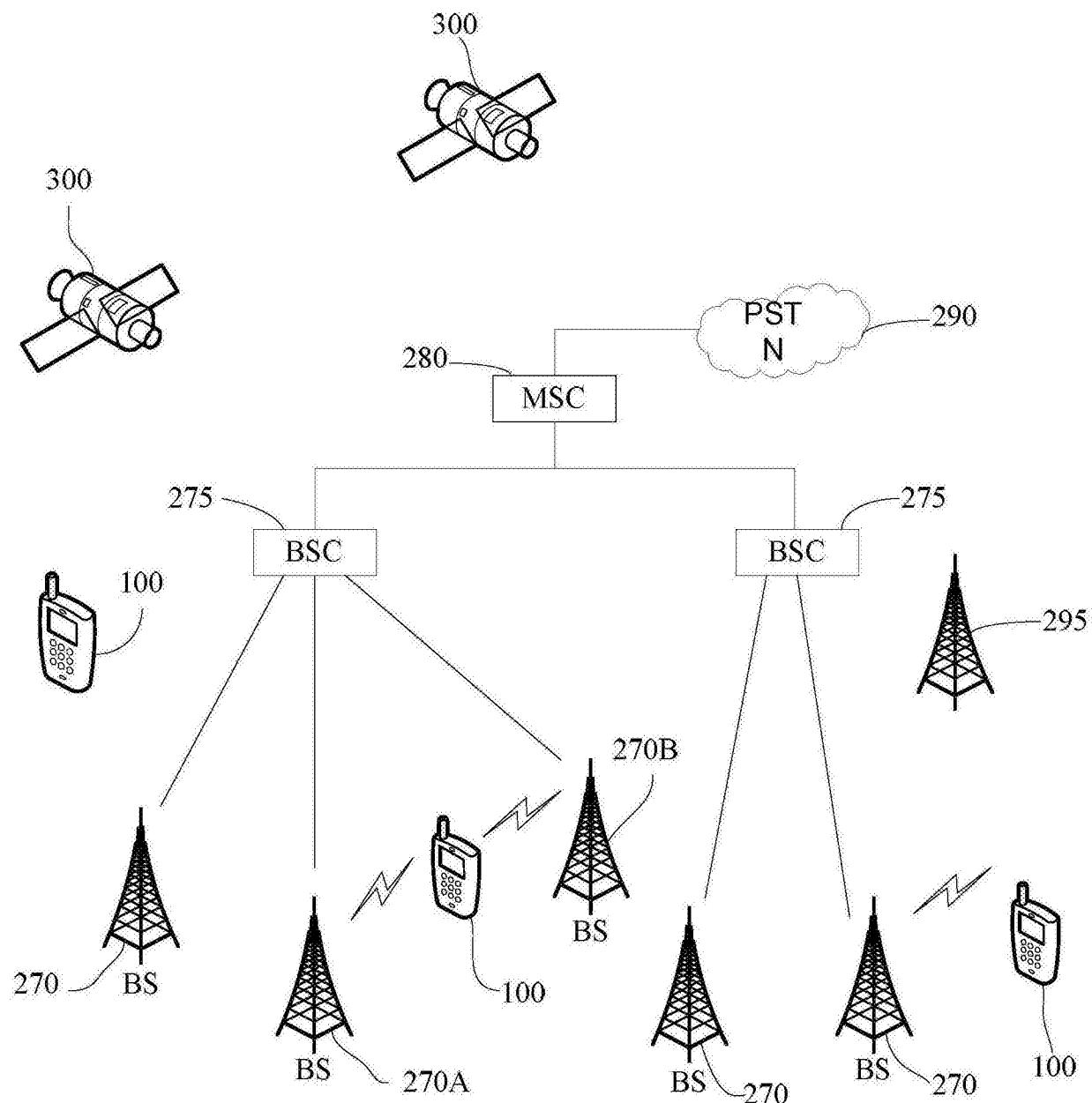


图2



图3

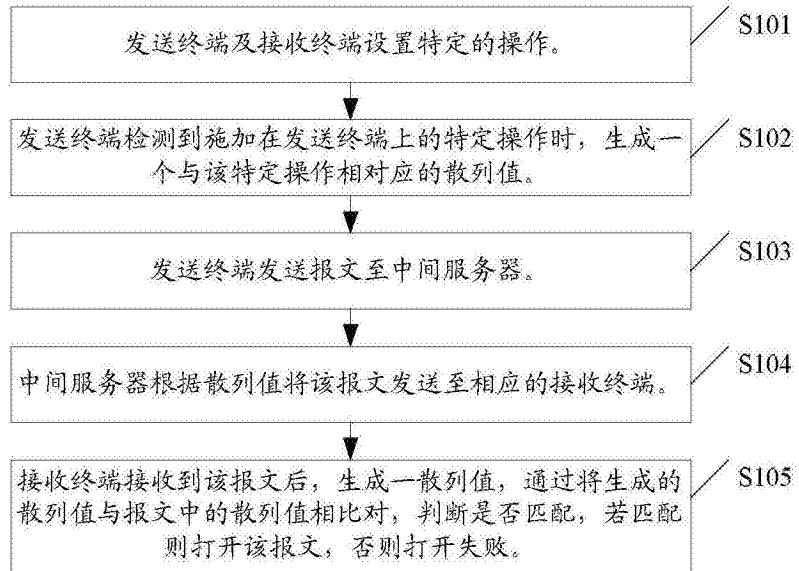


图4

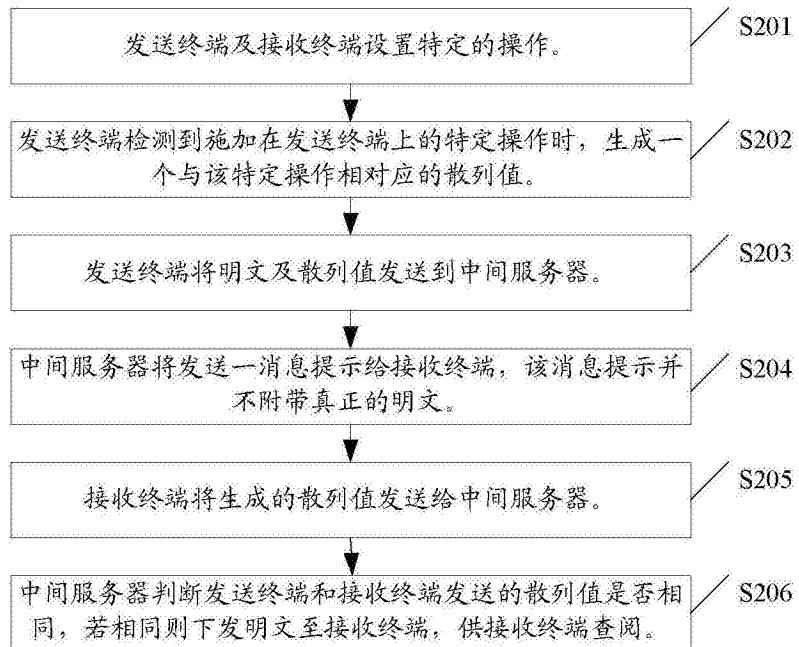


图5