(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115242558 B
(45)授权公告日 2022.12.09

(21)申请号 202211154453.0

(22)申请日 2022.09.22

(65)同一申请的已公布的文献号
申请公布号 CN 115242558 A

(43)申请公布日 2022.10.25

(73)专利权人 城云科技(中国)有限公司
地址 310052 浙江省杭州市滨江区长河街道江南大道588号恒鑫大厦主楼17层、18层

(72)发明人 李圣权 高博文 任通 彭大蒙 方玲洪

(74)专利代理机构 杭州汇和信专利代理有限公司 33475
专利代理师 吴琰

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/08(2006.01)

(56)对比文件
CN 113196263 A,2021.07.30
CN 112153015 A,2020.12.29
US 11405189 B1,2022.08.02
WO 2021137769 A1,2021.07.08
US 2012290838 A1,2012.11.15
JP 2012079284 A,2012.04.19
CN 112738024 A,2021.04.30
CN 113821787 A,2021.12.21

审查员 张燕燕

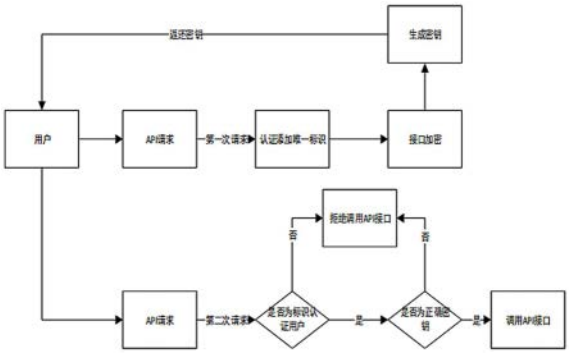
权利要求书2页 说明书7页 附图2页

(54)发明名称

API接口安全加密方法和认证方法及装置、可读存储介质

(57)摘要

本申请提出了一种API接口安全加密方法和认证方法及其应用,包括以下步骤:响应用户的首次API调用命令并生成赋予用户一随机的唯一标识;通过唯一标识向后台发出加密请求;后台响应加密请求并认证唯一标识,随机生成三个数字和三角形图案,三个数字随机分别附于该三角形图案的每个点上以得到正确密钥,该正确密钥返回给用户;根据正确密钥生成设定个数或随机个数的同样形式的错误密钥;响应用户的API调用命令并验证用户的唯一标识;若验证通过,则验证密钥是否正确;若密钥正确,则调用API接口进行对接。本申请实现简单且逻辑清晰,流程合理,解决了大部分API接口的安全性问题,以及对使用者进行识别。



CN 115242558 B

1.API接口安全加密方法,其特征在于,包括以下步骤:

S00、响应用户的首次API调用命令并生成赋予用户一随机的唯一标识;

S10、通过所述唯一标识向后台发出加密请求;

S20、后台响应加密请求并认证所述唯一标识,随机生成三个数字和三角形图案,三个数字随机分别附于该三角形图案的每个点上以得到正确密钥,该正确密钥返回给所述用户;

S30、根据所述正确密钥生成设定个数或随机个数的同样形式的错误密钥;

其中,所述错误密钥的三角形图案与所述正确密钥的三角形图案互为不相似三角形。

2.如权利要求1所述的API接口安全加密方法,其特征在于,步骤S20中,通过将三个数字中任意两个附于九宫格内同一直线上的任意两点,剩余一个数字附于九宫格内除该直线外的任意一点上,以形成三角形图案。

3.API接口安全认证方法,其特征在于,用于对权利要求1-2任意一项所述的API接口安全加密方法生成的密钥进行认证,包括以下步骤:

S40、响应用户的API调用命令并验证用户的唯一标识;

S50、若验证通过,则分别比较用户输入密钥的三角形图案和正确密钥的三角形图案,以及用户输入密钥的三个数字和正确密钥的三个数字;

若与正确密钥的三角形图案为相似三角形,且与正确密钥的三个数字相同且在三角形图案上的位置相同,则验证通过;若任意一项不符合,则验证不通过;

S60、若密钥正确,则调用API接口进行对接;

其中,密钥正确需同时满足:与正确密钥的三个数字相同且在三角形图案上的位置相同;与正确密钥的三角形图案为相似三角形。

4.一种API接口安全加密和认证装置,其特征在于,包括:

输入模块,用于供用户输入API调用命令和密钥;

对接模块,用于在验证通过后调用API接口;

加密模块,用于响应用户的首次API调用命令并生成赋予用户一随机的唯一标识;用于在认证模块响应加密请求并认证唯一标识后,随机生成三个数字和三角形图案,三个数字随机分别附于该三角形图案的每个点上以得到正确密钥,该正确密钥返回给用户;用于根据正确密钥生成设定个数或随机个数的同样形式的错误密钥;

其中,错误密钥的三角形图案与所述正确密钥的三角形图案互为不相似三角形;

认证模块,用于响应用户的API调用命令并验证用户的唯一标识;若验证通过,则分别比较用户输入密钥的三角形图案和正确密钥的三角形图案,以及用户输入密钥的三个数字和正确密钥的三个数字;若与正确密钥的三角形图案为相似三角形,且与正确密钥的三个数字相同且在三角形图案上的位置相同,则验证通过;若任意一项不符合,则验证不通过;若密钥正确,则调用API接口进行对接;

其中,密钥正确需同时满足:与正确密钥的三个数字相同且在三角形图案上的位置相同;与正确密钥的三角形图案为相似三角形。

5.一种电子装置,包括存储器和处理器,其特征在于,所述存储器中存储有计算机程序,所述处理器被设置为运行所述计算机程序以执行权利要求3所述的API接口安全认证方法。

6.一种可读存储介质,其特征在于,所述可读存储介质中存储有计算机程序,所述计算机程序包括用于控制过程以执行过程的程序代码,所述过程包括根据权利要求3所述的API接口安全认证方法。

API接口安全加密方法和认证方法及装置、可读存储介质

技术领域

[0001] 本申请涉及API接口领域,特别是一种涉及API接口安全加密方法和认证方法及其应用。

背景技术

[0002] 随着网络技术的迅速发展,API接口的运用越来越多,对于API接口的研究也越来越多,API(Application Programming Interface,应用程序编程接口)是一些预先定义的函数,目的是提供应用程序与开发人员基于某软件或硬件的以访问一组例程的能力,而又无需访问源码,或理解内部工作机制的细节。API的运用具有高效率、逻辑简单以及过程严密的特点,同时API优势巨大的同时,带来的风险也是巨大的,在API的调用中,依然存在着安全风险和认证的问题,因此对于API的安全认证,是一个需要重点研究的对象。

[0003] 目前对于API的认证以及安全识别的技术,大部分API接口还没有有效的安全认证方法,且有些API接口有识别的技术,但是识别方法并不合理或者非常复杂。在如今各个公司推广自己产品以及服务的同时,都会对本公司以及第三方用户提供API,在使用频率非常多的情况下,API的认证方式急需一种简单快速且有效的方法来进行识别以及加密API的方式。

发明内容

[0004] 本申请实施例提供了一种API接口安全加密方法和认证方法及其应用,针对目前技术存在没有有效的安全认证和识别方法等问题。

[0005] 本发明核心技术主要是通过随机生成随机字符和随机三个数字以及随机三角形,并将三个数字与随机三角形的三个点随机一一对应作为正确密钥,同时生成若干三角形状的错误密钥实现干扰,用户利用正确密钥即可验证调用API接口。

[0006] 第一方面,本申请提供了一种API接口安全加密方法,所述方法包括以下步骤:

[0007] S00、响应用户的首次API调用命令并生成赋予用户一随机的唯一标识;

[0008] S10、通过唯一标识向后台发出加密请求;

[0009] S20、后台响应加密请求并认证唯一标识,随机生成三个数字和三角形图案,三个数字随机分别附于该三角形图案的每个点上以得到正确密钥,该正确密钥返回给用户;

[0010] S30、根据正确密钥生成设定个数或随机个数的同样形式的错误密钥。

[0011] 进一步地,步骤S20中,通过将三个数字中任意两个附于九宫格内同一直线上的任意两点,剩余一个数字附于九宫格内处该直线外的任意一点上,以形成三角形图案。

[0012] 进一步地,步骤S30中,错误密钥的三角形图案与正确密钥的三角形图案互为不相似三角形。

[0013] 第二方面,本申请提供了API接口安全认证方法,用于对上述的API接口安全加密方法生成的密钥进行认证,包括以下步骤:

[0014] S40、响应用户的API调用命令并验证用户的唯一标识;

[0015] S50、若验证通过，则验证密钥是否正确；

[0016] S60、若密钥正确，则调用API接口进行对接。

[0017] 进一步地，步骤S50中，密钥正确需同时满足：与正确密钥的三个数字相同且在三角形图案上的位置相同；与正确密钥的三角形图案为相似三角形。

[0018] 进一步地，步骤S50中，验证密钥是否正确具体步骤为：

[0019] S51、分别比较用户输入密钥的三角形图案和正确密钥的三角形图案，以及用户输入密钥的三个数字和正确密钥的三个数字；

[0020] S52、若与正确密钥的三角形图案为相似三角形，且与正确密钥的三个数字相同且在三角形图案上的位置相同，则验证通过；若任意一项不符合，则验证不通过。

[0021] 第三方面，本申请提供了一种API接口安全加密和认证装置，包括：

[0022] 输入模块，用于供用户输入API调用命令和密钥；

[0023] 对接模块，用于在验证通过后调用API接口；

[0024] 加密模块，用于响应用户的首次API调用命令并生成赋予用户一随机的唯一标识；用于在认证模块响应加密请求并认证唯一标识后，随机生成三个数字和三角形图案，三个数字随机分别附于该三角形图案的每个点上以得到正确密钥，该正确密钥返回给用户；用于根据正确密钥生成设定个数或随机个数的同样形式的错误密钥；

[0025] 认证模块，用于响应用户的API调用命令并验证用户的唯一标识；若验证通过，则验证密钥是否正确；若密钥正确，则调用API接口进行对接。

[0026] 第四方面，本申请提供了一种电子装置，包括存储器和处理器，存储器中存储有计算机程序，处理器被设置为运行计算机程序以执行上述的API接口安全认证方法。

[0027] 第五方面，本申请提供了一种可读存储介质，可读存储介质中存储有计算机程序，计算机程序包括用于控制过程以执行过程的程序代码，过程包括根据上述的API接口安全认证方法。

[0028] 本发明的主要贡献和创新点如下：1、与现有技术相比，本申请通过对API接口随机生成的数字，使数字密码生成图形密码，相当于二次加密，而数字密码与图形密码的结构不易被破解，显著提高了安全性能，同时正确密钥在生成后还会有多个错误密钥，可混淆不法分子，以及保护接口的安全性(防止API接口被恶意攻击或者有人故意调用接口而非用户本人)；

[0029] 2、与现有技术相比，本申请只有利用三角形这种最简单图形，且其拥有相似三角形的基础数学原理，因此可适用于其他所有多边形，而且相对于其他加密技术，本申请实现简单且逻辑清晰，流程合理，解决了大部分API接口的安全性问题，以及对使用者进行识别，而且当相同接口被多次调用时，新增的唯一标识可以方便平台进行用户身份管理以及监控。

[0030] 本申请的一个或多个实施例的细节在以下附图和描述中提出，以使本申请的其他特征、目的和优点更加简明易懂。

附图说明

[0031] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0032] 图1是根据本申请实施例的API接口安全加密方法和认证方法的流程；

[0033] 图2是正确密钥的一种实例图；

[0034] 图3是根据正确密钥得到的一些错误密钥的实例图；

[0035] 图4是根据本申请实施例的电子装置的硬件结构示意图。

具体实施方式

[0036] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[0037] 需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[0038] 目前对于API的认证以及安全识别的技术，目前大部分API接口还没有有效的安全认证方法，且有些API接口有识别的技术，但是识别方法并不合理或者非常复杂。

[0039] 基于此，本发明基于数字和图案加密来解决现有技术存在的问题。

[0040] 实施例一

[0041] 本申请旨在提出API接口安全加密和认证方法，通过随机生成随机字符和随机三个数字以及随机三角形，并将三个数字与随机三角形的三个点随机一一对应作为正确密钥，同时生成若干三角形状的错误密钥实现干扰，用户利用正确密钥即可验证调用API接口。

[0042] 具体地，本申请实施例提供了一种API接口安全加密和认证方法，具体地，参考图1(图1为简略流程，具体内容以说明书为准)，所述方法包括：

[0043] S00、响应用户的首次API调用命令并生成赋予用户一随机的唯一标识；

[0044] 在本实施例中，如API在被用户调用时随机生成唯一标识，标识为带有#的随机字符，此随机字符绑定用户，当然可以是其他任意形式字符。

[0045] S10、通过唯一标识向后台发出加密请求；

[0046] 在本实施例中，API接口在接收到调用信息后，会利用随机生成的带有#的唯一标识向后台服务器发出加密请求。

[0047] S20、后台响应加密请求并认证唯一标识，随机生成三个数字和三角形图案，三个数字随机分别附于该三角形图案的每个点上以得到正确密钥，该正确密钥返回给用户；

[0048] 在本实施例中，后台服务器程序接收API的加密请求，对含有唯一标识#的信息进行认证，随后随机生成三个数字(这三个数字均不相同，如在0~9之间任意取三个不同数字)，通过九宫格的点，以排列的形式形成三角形图案，此加密信息为真实有效密码，此过程为生成数字密码如图2所示。可见图2中是取1、2、3三个数字，并在九宫格上按规则相对随机占点，形成了图2中的三角形图案，即为正确密钥。

[0049] 其中，通过将三个数字中任意两个附于九宫格内同一直线上的任意两点，剩余一个数字附于九宫格内除该直线外的任意一点上，以形成三角形图案；

[0050] S30、根据正确密钥生成设定个数或随机个数的同样形式的错误密钥。

[0051] 其中，且错误密钥的三角形图案与正确密钥的三角形图案互为不相似三角形。

[0052] 在本实施例中，可参见图3(仅随机展示了几种)，错误密钥的三角形图案不能够和正确密钥的相同或为相似三角形，梳理可以是几个或几十个或上百个，不限定，目的在于防止有人攻击API接口，如有黑客骇进API接口，就会得到多个密码，但是正确的是有一个，通过相似三角形生成的密钥方式只有客户知道。

[0053] 由于后台服务器会根据生成的正确密码图形再返还正确密钥，此过程为了防止API接口被恶意攻击或者有人故意调用接口而非用户本人，因此生成多种三角形图形密钥且含有不同标识，来进行维护API接口的安全调用。

[0054] 实施例二

[0055] 基于相同的构思，参见图1，本申请还提出了一种API接口安全认证方法，用于对实施例一的API接口安全加密方法生成的密钥进行认证，包括以下步骤：

[0056] S40、响应用户的API调用命令并验证用户的唯一标识；

[0057] S50、若验证通过，则验证密钥是否正确；若验证不通过，则拒绝调用；

[0058] 其中，密钥正确需同时满足：与正确密钥的三个数字相同且在三角形图案上的位置相同；与正确密钥的三角形图案为相似三角形。

[0059] 验证密钥是否正确具体步骤为：

[0060] S51、分别比较用户输入密钥的三角形图案和正确密钥的三角形图案，以及用户输入密钥的三个数字和正确密钥的三个数字；

[0061] S52、若与正确密钥的三角形图案为相似三角形，且与正确密钥的三个数字相同且在三角形图案上的位置相同，则验证通过；若任意一项不符合，则验证不通过，拒绝调用API接口；

[0062] 其中，返还的密钥图形和正确的加密图形遵循数学中相似三角形定理，具体的相似三角形判定定理如下：

[0063] 定理1在多边形中，若对应角相等且夹角的边成比例，则称它们是相似多边形。将满足定理1的相似也称作严格相似。

[0064] 两个三角形不满足定理1称作这两个三角形不是严格相似。定理1在相似三角形中，等角所对的边对应成比例，等角所对的边是对应边。定理2如果两个三角形的三边对应成比例，那么对应角相等。由定理1、定理1和定理2，易知判定三角形相似的如下定理3：定理3两个三角形相似当且仅当三边对应成比例。

[0065] 当且仅当两者三角形的图形密码与密钥满足严格相似，应该同时满足以下性质：

[0066] (1)相似三角形对应角相等，对应边成正比例。

[0067] (2)相似三角形的一切对应线段(对应高、对应中线、对应角平分线、外接圆半径、内切圆半径等)的比等于相似比。

[0068] (3)相似三角形周长的比等于相似比。

[0069] (4)相似三角形面积的比等于相似比的平方。

[0070] (5)相似三角形内切圆、外接圆直径比和周长比都和相似比相同，内切圆、外接圆

面积比是相似比的平方。

[0071] S60、若密钥正确，则调用API接口进行对接；若不正确，则拒绝调用。

[0072] 即，用户在调用API时产生的加密信息，要符合满足三个条件：

[0073] 1.生成的数字密码要相同且形成的三角形位置排列顺序要相同；

[0074] 2.必须含有一开始的唯一的标识#；

[0075] 3.必须符合严格相似三角形定理，加密三角形图形和密钥三角形图形必须要成为对应的相似三角形才能完成API的接口对接。

[0076] 即由后台服务器先进行加密，同时生成密钥，密钥返还给用户，用户凭借返还的密钥去对API接口进行调用。

[0077] 实施例三

[0078] 基于相同的构思，本申请还提出了一种API接口安全加密和认证装置，包括：

[0079] 输入模块，用于供用户输入API调用命令和密钥；

[0080] 对接模块，用于在验证通过后调用API接口；

[0081] 加密模块，用于响应用户的首次API调用命令并生成赋予用户一随机的唯一标识；用于在认证模块响应加密请求并认证唯一标识后，随机生成三个数字和三角形图案，三个数字随机分别附于该三角形图案的每个点上以得到正确密钥，该正确密钥返回给用户；用于根据正确密钥生成设定个数或随机个数的同样形式的错误密钥；

[0082] 认证模块，用于响应用户的API调用命令并验证用户的唯一标识；若验证通过，则验证密钥是否正确；若密钥正确，则调用API接口进行对接。

[0083] 实施例四

[0084] 本实施例还提供了一种电子装置，参考图4，包括存储器404和处理器402，该存储器404中存储有计算机程序，该处理器402被设置为运行计算机程序以执行上述任一项方法实施例中的步骤。

[0085] 具体地，上述处理器402可以包括中央处理器(CPU)，或者特定集成电路(ApplicationSpecificIntegratedCircuit，简称为ASIC)，或者可以被配置成实施本申请实施例的一个或多个集成电路。

[0086] 其中，存储器404可以包括用于数据或指令的大容量存储器404。举例来说而非限制，存储器404可包括硬盘驱动器(HardDiskDrive，简称为HDD)、软盘驱动器、固态驱动器(SolidStateDrive，简称为SSD)、闪存、光盘、磁光盘、磁带或通用串行总线(UniversalSerialBus，简称为USB)驱动器或者两个或更多个以上这些的组合。在合适的情况下，存储器404可包括可移除或不可移除(或固定)的介质。在合适的情况下，存储器404可在数据处理装置的内部或外部。在特定实施例中，存储器404是非易失性(Non-Volatile)存储器。在特定实施例中，存储器404包括只读存储器(Read-OnlyMemory，简称为ROM)和随机存取存储器(RandomAccessMemory，简称为RAM)。在合适的情况下，该ROM可以是掩模编程的ROM、可编程ROM(ProgrammableRead-OnlyMemory，简称为PROM)、可擦除PROM(ErasableProgrammableRead-OnlyMemory，简称为EPROM)、电可擦除PROM(ElectricallyErasableProgrammableRead-OnlyMemory，简称为EEPROM)、电可改写ROM(ElectricallyAlterableRead-OnlyMemory，简称为EAROM)或闪存(FLASH)或者两个或更多个以上这些的组合。在合适的情况下，该RAM可以是静态随机存取存储器(StaticRandom-

AccessMemory,简称为SRAM)或动态随机存取存储器(DynamicRandomAccessMemory,简称为DRAM),其中,DRAM可以是快速页模式动态随机存取存储器404(FastPageModeDynamicRandomAccessMemory,简称为FPMDRAM)、扩展数据输出动态随机存取存储器(ExtendedDateOutDynamicRandomAccessMemory,简称为EDODRAM)、同步动态随机存取内存(SynchronousDynamicRandom-AccessMemory,简称SDRAM)等。

[0087] 存储器404可以用来存储或者缓存需要处理和/或通信使用的各种数据文件,以及处理器402所执行的可能的计算机程序指令。

[0088] 处理器402通过读取并执行存储器404中存储的计算机程序指令,以实现上述实施例中的任意一种API接口安全认证方法。

[0089] 可选地,上述电子装置还可以包括传输设备406以及输入输出设备408,其中,该传输设备406和上述处理器402连接,该输入输出设备408和上述处理器402连接。

[0090] 传输设备406可以用来经由一个网络接收或者发送数据。上述的网络具体实例可包括电子装置的通信供应商提供的有线或无线网络。在一个实例中,传输设备包括一个网络适配器(Network Interface Controller,简称为NIC),其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中,传输设备406可以为射频(Radio Frequency,简称为RF)模块,其用于通过无线方式与互联网进行通讯。

[0091] 输入输出设备408用于输入或输出信息。在本实施例中,输入的信息可以是API调用命令和密钥等,输出的信息可以是调用结果和验证信息以及正确密钥等。

[0092] 实施例五

[0093] 本实施例还提供了一种可读存储介质,可读存储介质中存储有计算机程序,计算机程序包括用于控制过程以执行过程的程序代码,过程包括根据实施例一的API接口安全认证方法。

[0094] 需要说明的是,本实施例中的具体示例可以参考上述实施例及可选实施方式中所描述的示例,本实施例在此不再赘述。

[0095] 通常,各种实施例可以以硬件或专用电路、软件、逻辑或其任何组合来实现。本发明的一些方面可以以硬件来实现,而其他方面可以由控制器、微处理器或其他计算设备执行的固件或软件来实现,但是本发明不限于此。尽管本发明的各个方面可以被示出和描述为框图、流程图或使用一些其他图形表示,但是应当理解,作为非限制性示例,本文中描述的这些框、装置、系统、技术或方法可以以硬件、软件、固件、专用电路或逻辑、通用硬件或控制器或其他计算设备或其某种组合来实现。

[0096] 本发明的实施例可以由计算机软件来实现,该计算机软件由移动设备的数据处理器诸如在处理器实体中可执行,或者由硬件来实现,或者由软件和硬件的组合来实现。包括软件例程、小程序和/或宏的计算机软件或程序(也称为程序产品)可以存储在任何装置可读数据存储介质中,并且它们包括用于执行特定任务的程序指令。计算机程序产品可以包括当程序运行时被配置为执行实施例的一个或多个计算机可执行组件。一个或多个计算机可执行组件可以是至少一个软件代码或其一部分。另外,在这一点上,应当注意,如图中的逻辑流程的任何框可以表示程序步骤、或者互连的逻辑电路、框和功能、或者程序步骤和逻辑电路、框和功能的组合。软件可以存储在诸如存储器芯片或在处理器内实现的存储块等物理介质、诸如硬盘或软盘等磁性介质、以及诸如例如DVD及其数据变体、CD等光学介质上。

物理介质是非瞬态介质。

[0097] 本领域的技术人员应该明白，以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0098] 以上实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本申请范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以作出若干变形和改进，这些都属于本申请的保护范围。因此，本申请的保护范围应以所附权利要求为准。

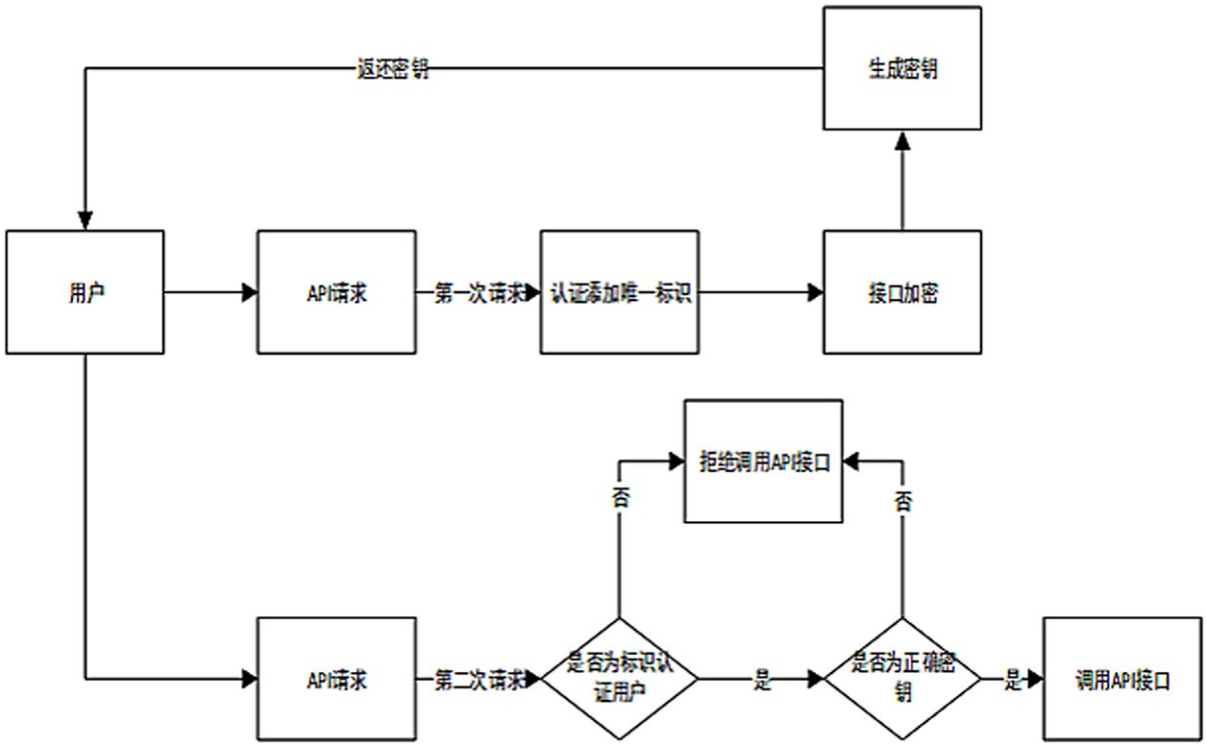

返还密钥
生成密钥
用户
API请求
第一次请求
认证添加唯一标识
接口加密
拒绝调用API接口
否
否
API请求
第二次请求
是否为标识认证用户
是
是否为正确密钥
是
调用API接口

图1

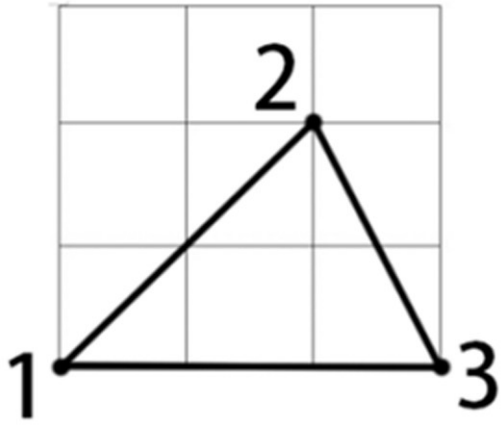

2
1
3

图2

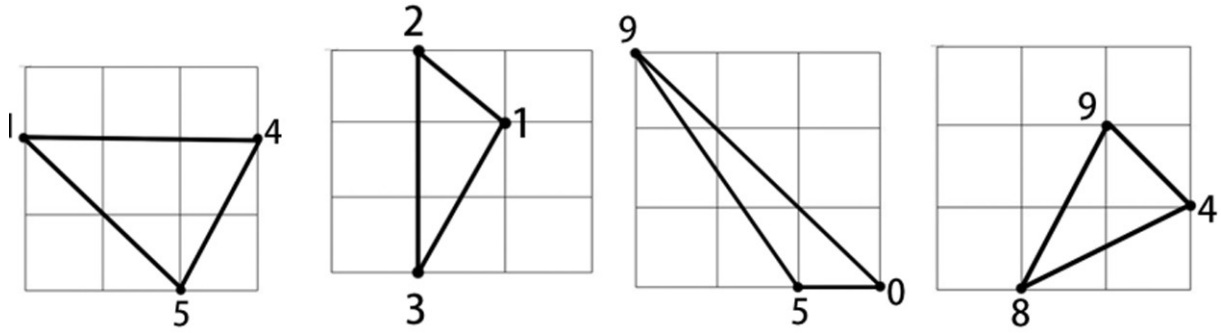


图3

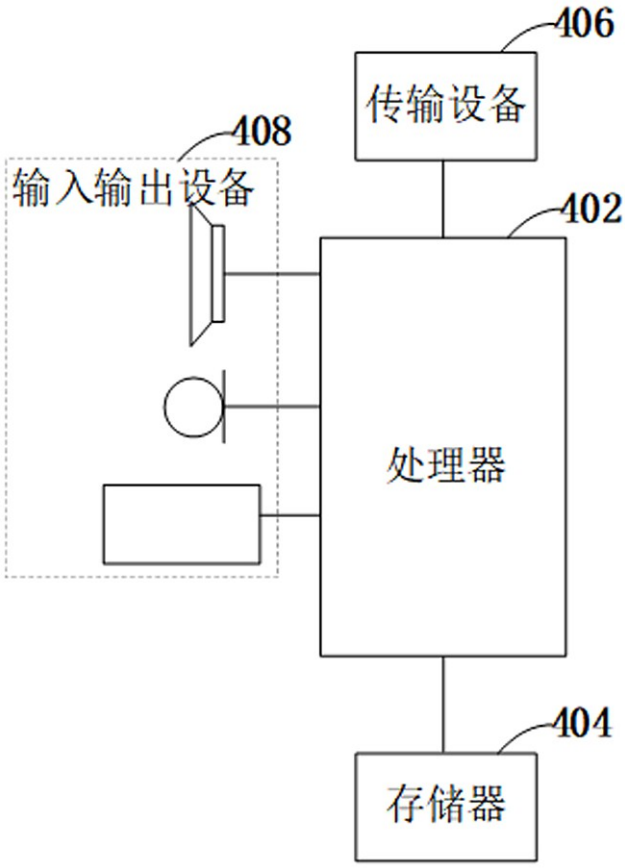


图4