(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 107659398 A
(43)申请公布日 2018.02.02

(21)申请号 201710918043.1

(22)申请日 2017.09.28

(71)申请人 四川长虹电器股份有限公司
地址 621000 四川省绵阳市高新区绵兴东路35号

(72)发明人 胡秩铭 刘蛟 李伟光 郑鸿

(74)专利代理机构 四川省成都市天策商标专利事务所 51213
代理人 袁辰亮 王荔

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
G06N 3/08(2006.01)

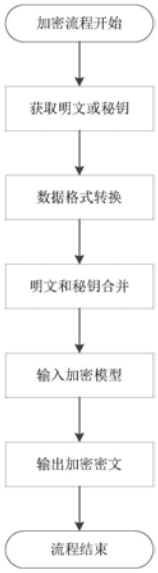
权利要求书1页 说明书4页 附图2页

(54)发明名称

适用于Android的对称加密方法

(57)摘要

本发明公开了一种适用于Android的对称加密方法，包括加密流程和解密流程；所述的方法包括以下步骤：使用TensorFlow搭建神经网络模型计算图；对模型进行训练，随机生成一个大小为4096的输入数据数组，每个数据为长度为8的向量；随机生成密钥，合并输入加密模型，加密输出数据再与同一个秘钥进行合并，然后输入解密模型，将解密模型的输出和原数据进行比较并计算平均误差；将训练好的模型参数和模型计算图保存为文件，导入到Android asset资源中，用TensorFlow的Android library调用即可。本发明结合了神经网络来实现加解密，使其核心算法不同于传统的对称加密算法，可以加强安全性。并且神经网络的结构，使用者可以根据自己的需要进行变化，只需重新训练参数。



CN 107659398 A

1.一种适用于Android的对称加密方法，包括加密流程和解密流程；其特征在于：所述的方法包括以下步骤：

使用TensorFlow搭建神经网络模型计算图；

对模型进行训练，随机生成一个大小为4096的输入数据数组，每个数据为长度为8的向量；

随机生成密钥，合并输入加密模型，加密输出数据再与同一个秘钥进行合并，然后输入解密模型，将解密模型的输出和原数据进行比较并计算平均误差；

将训练好的模型参数和模型计算图保存为文件，导入到Android asset资源中，用TensorFlow的Android library调用即可。

2.根据权利要求1所述的适用于Android的对称加密方法，其特征在于所述加密流程包括以下步骤：

步骤一、获取到待加密的明文和密钥；

步骤二、将明文和密钥转换为二进制方式表示，并将0映射为-1,1保持为1；

步骤三、将明文和密钥合并，首先取明文的第一个字节和密钥的第一个字节，将密钥拼接在明文之后构成一组数据，然后取明文的第二个字节和密钥的第二个字节进行合并，依次类推，取到密钥的最后一个字节之后再从密钥的第一个字节开始取，直到明文的每一个字节均与密钥完成合并；

步骤四、将合并的数据按组输入加密模型；

步骤五、最后的输出即为加密后的密文。

3.根据权利要求2所述的适用于Android的对称加密方法，其特征在于所述的步骤四中加密模型是一个已训练好的多层神经网络，每次取一组合并数据作为输入。

4.根据权利要求1所述的适用于Android的对称加密方法，其特征在于所述的解密流程包括以下步骤：

步骤一、获取到密文和密钥；

步骤二、将密钥表示为二进制形式并将0映射为-1,1保持为1；

步骤三、将密文和密钥进行合并，首先提取相当于一个字节的密文和密钥的第一个字节，然后将密钥拼接在密文之后构成一组数据，重复这个过程直到所有密文和密钥完成合并，当取到密钥的最后一个字节之后再从第一个字节开始取密钥；

步骤四、将合并后的数据按组输入解密模型；

步骤五、输出数据即为明文的二进制位近似数据，将其按字节恢复和解映射，得到明文二进制数据。

适用于Android的对称加密方法

技术领域

[0001] 本发明涉及信息加密技术领域,具体涉及一种适用于Android的对称加密方法。

背景技术

[0002] 对称加密是一种成熟的加密方式,因其计算量小、加密速度快、加密效率高等优点而广泛应用于安卓应用的密码、文件、核心数据的加密上。现在比较流行的对称加密方法有DES、AES、Blowfish等等。

[0003] 但是对称加密的算法是公开的,且加密双方发送数据前必须保存好商定好的密钥,如果需要和多个对象完成通信,那么就会拥有数量巨大的密钥,管理如此多的密钥对双方来说都是一个很大的负担。而且只要一方的密钥泄露,那么加密信息也就不完全了。

发明内容

[0004] 本发明克服了现有技术的不足,提供一种适用于Android的对称加密方法。

[0005] 为解决上述的技术问题,本发明采用以下技术方案:

[0006] 一种适用于Android的对称加密方法,包括加密流程和解密流程;所述的方法包括以下步骤:

[0007] 使用TensorFlow搭建神经网络模型计算图;

[0008] 对模型进行训练,随机生成一个大小为4096的输入数据数组,每个数据为长度为8的向量;

[0009] 随机生成密钥,合并输入加密模型,加密输出数据再与同一个秘钥进行合并,然后输入解密模型,将解密模型的输出和原数据进行比较并计算平均误差;

[0010] 将训练好的模型参数和模型计算图保存为文件,导入到Android asset资源中,用TensorFlow的Android library调用即可。

[0011] 更进一步的技术方案是所述加密流程包括以下步骤:

[0012] 步骤一、获取到待加密的明文和密钥;

[0013] 步骤二、将明文和密钥转换为二进制方式表示,并将0映射为-1,1保持为1;

[0014] 步骤三、将明文和密钥合并,首先取明文的第一个字节和密钥的第一个字节,将密钥拼接在明文之后构成一组数据,然后取明文的第二个字节和密钥的第二个字节进行合并,依次类推,取到密钥的最后一个字节之后再从密钥的第一个字节开始取,直到明文的每一个字节均与密钥完成合并;

[0015] 步骤四、将合并的数据按组输入加密模型;

[0016] 步骤五、最后的输出即为加密后的密文。

[0017] 更进一步的技术方案是所述的步骤四中加密模型是一个已训练好的多层神经网络,每次取一组合并数据作为输入。

[0018] 更进一步的技术方案是所述的解密流程包括以下步骤:

[0019] 步骤一、获取到密文和密钥;

[0020] 步骤二、将密钥表示为二进制形式并将0映射为-1,1保持为1；

[0021] 步骤三、将密文和密钥进行合并，首先提取相当于一个字节的密文和密钥的第一个字节，然后将密钥拼接在密文之后构成一组数据，重复这个过程直到所有密文和密钥完成合并，当取到密钥的最后一个字节之后再从第一个字节开始取密钥；

[0022] 步骤四、将合并后的数据按组输入解密模型；

[0023] 步骤五、输出数据即为明文的二进制位近似数据，将其按字节恢复和解映射，得到明文二进制数据。

[0024] 与现有技术相比，本发明实施例的有益效果之一是：本发明结合了神经网络来实现加解密，使其核心算法不同于传统的对称加密算法，可以加强安全性。并且神经网络的结构，使用者可以根据自己的需要进行变化，只需重新训练参数。该算法可用来对文本类型数据进行加密，可以对ASCII字符进行加解密。

附图说明

[0025] 图1为本发明一个实施例中加密模型结构示意图。

[0026] 图2为本发明一个实施例中加密流程图。

[0027] 图3为本发明一个实施例中解密流程图。

具体实施方式

[0028] 本说明书中公开的所有特征，或公开的所有方法或过程中的步骤，除了互相排斥的特征和/或步骤以外，均可以以任何方式组合。

[0029] 本说明书(包括任何附加权利要求、摘要和附图)中公开的任一特征，除非特别叙述，均可被其他等效或具有类似目的的替代特征加以替换。即，除非特别叙述，每个特征只是一系列等效或类似特征中的一个例子而已。

[0030] 下面结合附图及实施例对本发明的具体实施方式进行详细描述。

[0031] 在下面的详细描述中，出于解释的目的描述了许多具体描述以便能够彻底理解所公开的实施方案，然而，很明显一个或多个实施方式可以在不使用这些具体描述的情况下实施，在其他实例中，示意性地显示已知结构和装置，以便简化附图。

[0032] 根据本发明的一个实施例，本实施例公开一种适用于Android的对称加密方法，该方法首先需要使用TensorFlow搭建神经网络模型计算图，其次对模型进行训练，训练方法为随机生成一个大小为4096的输入数据数组，每个数据为长度为8的向量，表示一个字节的数据，随机数据的样本空间为可能被用作明文进行加密的字符，比如常用的ASCII字符。然后随机生成密钥，合并后输入加密模型，加密输出数据再输入解密模型，将解密模型的输出和原数据进行比较并计算平均误差，优化器采用AdamOptimizer。将训练好的模型参数和计算图保存为文件，导入到Android asset资源中，用TensorFlow的Android library调用即可。

[0033] 具体的，如图2和图3所示，本实施例对加密解密模型细节作出具体阐述。

[0034] 本实施例中该对称加密包含两个流程：加密流程和解密流程，下面分别描述这两个流程。

[0035] 如图2所示，所述加密流程包括以下步骤：

[0036] 1、获取到待加密的明文和密钥。

[0037] 2、将明文和密钥转换为二进制方式表示，并将0映射为-1,1保持为1。

[0038] 例如，需要加密的明文字符串为“abc”，密钥字符串为“123”，编码方式为ASCII，将其转换为二进制并进行映射之后的数据为

[0039] “[-1,1,1,-1,-1,-1,-1,1],[-1,1,1,-1,-1,-1,1,-1],[-1,1,1,-1,-1,-1,1,1]”(abc)和“[-1,-1,1,1,-1,-1,-1,1],[-1,-1,1,1,-1,-1,1,-1],

[0040] [-1,-1,1,1,-1,-1,1,1]”(123)。

[0041] 3、将明文和密钥合并，首先取明文的第一个字节(8个二进制位)和密钥的第一个字节，将密钥拼接在明文之后构成一组数据，然后取明文的第二个字节和密钥的第二个字节进行合并，依次类推，取到密钥的最后一个字节之后再从密钥的第一个字节开始取，直到明文的每一个字节均与密钥完成合并。

[0042] 例如，将明文“abc”和密文“123”的合并结果为

[0043] “[-1,1,1,-1,-1,-1,-1,1,-1,-1,1,1,-1,-1,-1,1],

[0044] [-1,1,1,-1,-1,-1,1,-1,-1,-1,1,1,-1,-1,1,-1],

[0045] [-1,1,1,-1,-1,-1,1,1,-1,-1,1,1,-1,-1,1,1]”(a1b2c3)

[0046] 4、将合并的数据按组输入加密模型。加密模型是一个已训练好的多层神经网络，每次取一组合并数据作为输入，网络结构如图1所示。

[0047] 加密网络的第一层为全连接层，有16个神经元，令输入向量为X，第i个神经元的权重向量为$W_{1,i}$，bias为b，则第i个神经元的输出$h_{1,i}=W_{1,i}^{T}X+b$。输入数据经过第一层之后的输出H_1为长度16的向量。第二层为卷积层，有两个神经元，激活函数为sigmoid，令第i个神经元的卷积核为$W_{2,i}$，bias为b，则第i个神经元的输出特征map为$H_{2,i}=sigmoid(H_1*W_{2,i}+b)$，第二层卷积的步长为2，输出两个特征map，即最终输出H_2为2×8的矩阵。第三层卷积层有一个神经元，激活函数为sigmoid，对明文特征和密文特征进行混合提取特征，输出为$H_3=sigmoid(H_2*W_3+b)$，最后一层卷积层有一个神经元，激活函数为tanh，输出为$H_4=tanh(H_3*W_4+b)$。

[0048] 5、最后的输出即为加密后的密文。

[0049] 具体的，如图3所示，所述解密流程包括以下步骤：

[0050] 1、获取到密文和密钥。

[0051] 2、将密钥表示为二进制形式并将0映射为-1,1保持为1。

[0052] 3、将密文和密钥进行合并，首先提取相当于一个字节的密文(8个数据)和密钥的第一个字节(8个二进制位)，然后将密钥拼接在密文之后构成一组数据，重复这个过程直到所有密文和密钥完成合并，当取到密钥的最后一个字节之后再从第一个字节开始取密钥。该过程和加密时类似。

[0053] 4、将合并后的数据按组输入解密模型。解密模型和加密模型结构和算法上完全一致，区别在于各层神经元的权重和偏差参数不同。

[0054] 5、输出数据即为明文的二进制位近似数据，将其按字节恢复和解映射，得到明文二进制数据。例如取前8个输出数据a_1～a_8，代表明文的第一个字节。首先计算$b_i=(a_i+1)\div 2(i\in[1,8])$，其次计算$y=\sum_{i=1}^{8} b_i * 2^{8-i}$，将y四舍五入后得到的整数即为明文第一个字节的内容。

[0055] 在本说明书中所谈到的“一个实施例”、“另一个实施例”、“实施例”等，指的是结合该实施例描述的具体特征、结构或者特点包括在本申请概括性描述的至少一个实施例中。在说明书中多个地方出现同种表述不是一定指的是同一个实施例。进一步来说，结合任一个实施例描述一个具体特征、结构或者特点时，所要主张的是结合其他实施例来实现这种特征、结构或者特点也落在本发明的范围内。

[0056] 尽管这里参照发明的多个解释性实施例对本发明进行了描述，但是，应该理解，本领域技术人员可以设计出很多其他的修改和实施方式，这些修改和实施方式将落在本申请公开的原则范围和精神之内。更具体地说，在本申请公开权利要求的范围内，可以对主题组合布局的组成部件和/或布局进行多种变型和改进。除了对组成部件和/或布局进行的变型和改进外，对于本领域技术人员来说，其他的用途也将是明显的。

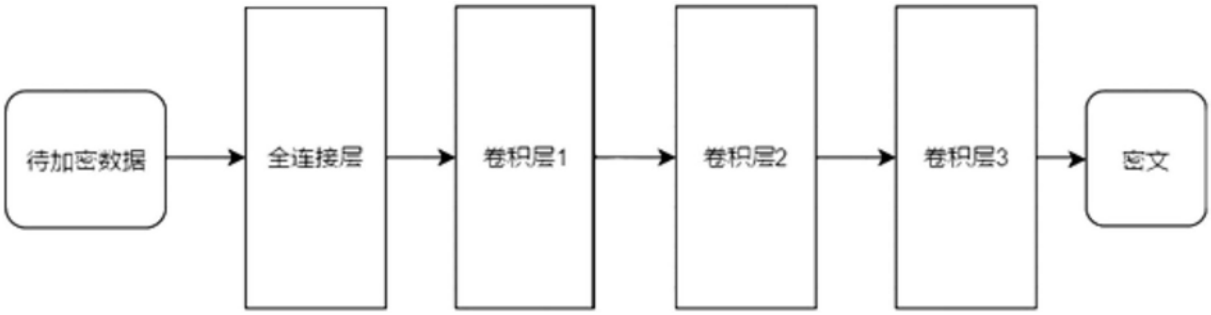

待加密数据
全连接层
卷积层1
卷积层2
卷积层3
密文

图1

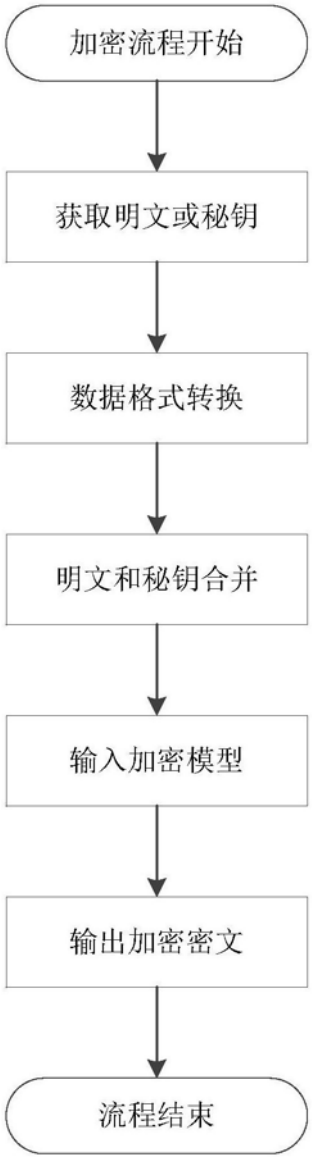

加密流程开始
获取明文或秘钥
数据格式转换
明文和秘钥合并
输入加密模型
输出加密密文
流程结束

图2

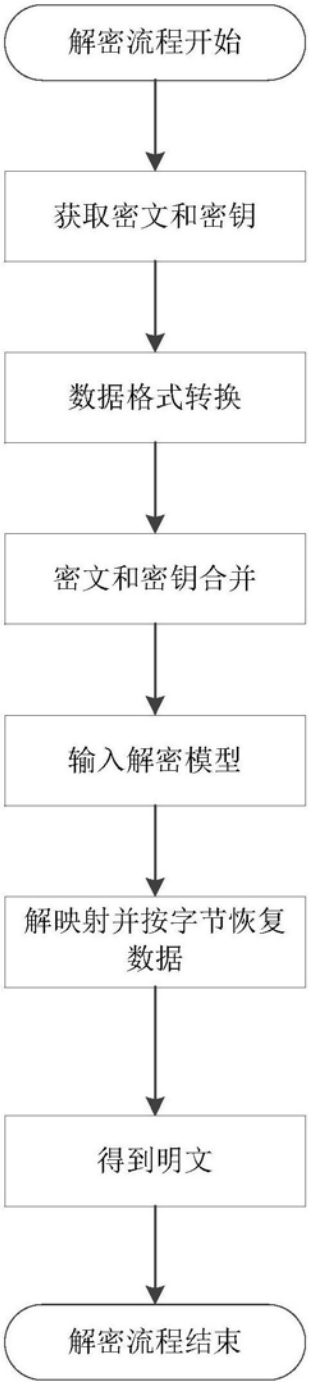

解密流程开始
获取密文和密钥
数据格式转换
密文和密钥合并
输入解密模型
解映射并按字节恢复数据
得到明文
解密流程结束

图3