(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111008399 B
(45)授权公告日 2021.04.13

(21)申请号 201911199828.3
(22)申请日 2019.11.29
(65)同一申请的已公布的文献号
申请公布号 CN 111008399 A
(43)申请公布日 2020.04.14
(73)专利权人 卓尔智联(武汉)研究院有限公司
地址 430000 湖北省武汉市黄陂区盘龙城经济开发区汉口北大道88号汉口北国际交易中心D1区7层
(72)发明人 吴良顺
(74)专利代理机构 深圳市赛恩倍吉知识产权代理有限公司 44334
代理人 饶智彬
(51)Int.Cl.
G06F 21/62(2013.01)
H04L 9/08(2006.01)
(56)对比文件
CN 109829328 A,2019.05.31
CN 109768854 A,2019.05.17
CN 108280356 A,2018.07.13
CN 110472445 A,2019.11.19
审查员 段玥

权利要求书3页 说明书13页 附图5页

(54)发明名称

姓名数据脱敏装置、方法及可读存储介质

(57)摘要

一种姓名数据脱敏方法、装置及计算机可读存储介质，所述方法包括：将待脱敏姓名分解为姓氏部分及名字部分；查找预设姓氏库映射表得到与姓氏部分对应的数值及查找预设名字库映射表得到与名字部分对应的数值；根据预设密钥及待脱敏姓名的长度生成迭代轮次N，其中预设密钥为生成迭代轮次N所使用的随机数生成器的种子；分别对姓氏部分对应的数值及名字部分对应的数值进行N次加密得到姓氏加密值及名字加密值；查找预设姓氏库映射表得到与姓氏加密值对应的姓氏词，及查找预设名字库映射表得到与名字加密值对应的名字词；及基于查找得到的姓氏词及名字词得到与待脱敏姓名对应的加密姓名。本发明可对脱敏之后的数据进行还原，且密文破解难度高。

CN 111008399 B

1.一种姓名数据脱敏方法,其特征在于,所述方法包括:

基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分;

判断所述姓氏部分及所述名字部分是否包含有两个或大于两个的词;

若所述姓氏部分和/或所述名字部分包含有两个或大于两个的词,则对所述姓氏部分和/或所述名字部分继续进行分解,直至将所述姓氏部分和/或所述名字部分分解至单个词;

查找预设姓氏库映射表得到与每一单姓氏词对应的数值,及查找预设名字库映射表得到与每一单名字词对应的数值;

根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N,其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子;

对每一所述单姓氏词对应的数值进行N次加密得到姓氏加密值,及对每一所述单名字词对应的数值进行N次加密得到名字加密值;

查找所述预设姓氏库映射表得到与每一所述姓氏加密值对应的姓氏词,及查找所述预设名字库映射表得到与每一所述名字加密值对应的名字词;及

基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名;

其中,所述预设姓氏库映射表包括多个单姓氏词,每一所述单姓氏词一一对应一唯一的数值,所述对每一所述单姓氏词对应的数值进行N次加密得到姓氏加密值,包括:

对所述预设姓氏库映射表进行初始化,得到由每一所述单姓氏词的数值构成的姓氏库数值集;

利用预设分组加密算法对所述姓氏库数值集中的每一元素进行加密,得到由每一加密元素构成的第一元组;

依据每一所述加密元素的大小对所述第一元组中的每一所述加密元素进行排序;

基于每一所述加密元素与所述姓氏库数值集的每一元素的对应关系,将经过排序处理的第一元组转换得到第二元组,其中所述第二元组的每一元素的下标与所述姓氏库数值集中的每一元素一一对应;及

从所述第二元组中提取下标为所述单姓氏词对应的数值的元素,并将提取到的元素作为下一次迭代提取的下标值,直至将第N次提取得到的元素作为所述单姓氏词对应的数值的姓氏加密值;

所述迭代轮次N通过以下算式计算得到:

$$N = \sum_{i=1}^{l} Gen_{seed}(\Omega)/l;$$

其中,l为所述待脱敏姓名的长度,Ω为加密轮次空间,Gen为所述随机数生成器,seed为所述预设密钥。

2.如权利要求1所述的方法,其特征在于,所述方法还包括:

若查找所述预设姓氏库映射表未得到与某一单姓氏词对应的数值,则根据预设姓氏映射规则建立与未在所述姓氏库映射表中的单姓氏词对应的姓氏映射记录,并将所述姓氏映射记录添加至所述姓氏库映射表中;及

若查找所述预设名字库映射表未得到与某一单名字词对应的数值,则根据预设名字映射规则建立与未在所述名字库映射表中的单名字词对应的名字映射记录,并将所述名字映

射记录添加至所述名字库映射表中。

3.如权利要求1所述的方法,其特征在于,所述查找预设姓氏库映射表得到与每一单姓氏词对应的数值之前,还包括:

判断分解得到的每一所述单姓氏词是否在所述姓氏库映射表中;

若分解得到的某一单姓氏词不在所述姓氏库映射表中,则根据预设姓氏映射规则建立与未在所述姓氏库映射表中的单姓氏词对应的姓氏映射记录,并将所述姓氏映射记录添加至所述姓氏库映射表中;

判断分解得到的每一所述单名字词是否在所述名字库映射表中;及

若分解得到的某一单名字词不在所述名字库映射表中,则根据预设名字映射规则建立与未在所述名字库映射表中的单名字词对应的名字映射记录,并将所述名字映射记录添加至所述名字库映射表中。

4.如权利要求1所述的方法,其特征在于,所述预设名字库映射表包括多个单名字词,每一所述单名字词一一对应一唯一的数值,所述对每一所述单名字词对应的数值进行N次加密得到名字加密值,包括:

对所述预设名字库映射表进行初始化,得到由每一所述单名字词的数值构成的名字库数值集;

利用预设分组加密算法对所述名字库数值集中的每一元素进行加密,得到由每一加密元素构成的第三元组;

依据每一所述加密元素的大小对所述第三元组中的每一所述加密元素进行排序;

基于每一所述加密元素与所述名字库数值集的每一元素的对应关系,将经过排序处理的第三元组转换得到第四元组,其中所述第四元组的每一元素的下标与所述名字库数值集中的每一元素一一对应;及

从所述第四元组中提取下标为所述单名字词对应的数值的元素,并将提取到的元素作为下一次迭代提取的下标值,直至将第N次提取得到的元素作为所述单名字词对应的数值的名字加密值。

5.如权利要求1所述的方法,其特征在于,所述方法还包括:

基于所述预设分解规则将所述加密姓名分解为加密姓氏部分及加密名字部分;

判断所述加密姓氏部分及所述加密名字部分是否包含有两个或大于两个的词;

若所述加密姓氏部分和/或所述加密名字部分包含有两个或大于两个的词,则对所述加密姓氏部分和/或所述加密名字部分继续进行分解,直至将所述加密姓氏部分和/或所述加密名字部分分解至单个词;

查找所述预设姓氏库映射表得到与每一加密单姓氏词对应的数值,及查找所述预设名字库映射表得到与每一加密单名字词对应的数值;

对每一所述加密单姓氏词对应的数值进行N次解密得到姓氏解密值,及对每一所述加密单名字词对应的数值进行N次解密得到名字解密值;

查找所述预设姓氏库映射表得到与每一所述姓氏解密值对应的姓氏词,及查找所述预设名字库映射表得到与每一所述名字解密值对应的名字词;及

基于查找得到的姓氏词及名字词得到与所述加密姓名对应的待脱敏姓名。

6.一种姓名数据脱敏方法,其特征在于,所述方法包括:

基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分；

查找预设姓氏库映射表得到与所述姓氏部分对应的数值，及查找预设名字库映射表得到与所述名字部分对应的数值；

根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N，其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子；

对所述姓氏部分对应的数值进行N次加密得到姓氏加密值，及对所述名字部分对应的数值进行N次加密得到名字加密值；

查找所述预设姓氏库映射表得到与所述姓氏加密值对应的姓氏词，及查找所述预设名字库映射表得到与所述名字加密值对应的名字词；及

基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名；

其中，所述预设姓氏库映射表包括多个姓氏词，每一所述姓氏词一一对应一唯一的数值，所述对所述姓氏部分对应的数值进行N次加密得到姓氏加密值，包括：

对所述预设姓氏库映射表进行初始化，得到由每一所述姓氏词的数值构成的姓氏库数值集；

利用预设分组加密算法对所述姓氏库数值集中的每一元素进行加密，得到由每一加密元素构成的第一元组；

依据每一所述加密元素的大小对所述第一元组中的每一所述加密元素进行排序；

基于每一所述加密元素与所述姓氏库数值集的每一元素的对应关系，将经过排序处理的第一元组转换得到第二元组，其中所述第二元组的每一元素的下标与所述姓氏库数值集中的每一元素一一对应；及

从所述第二元组中提取下标为所述姓氏部分对应的数值的元素，并将提取到的元素作为下一次迭代提取的下标值，直至将第N次提取得到的元素作为所述姓氏部分对应的数值的姓氏加密值；

所述迭代轮次N通过以下算式计算得到：

$$N = \sum_{i=1}^{l} Gen_{seed}(\Omega)/l;$$

其中，l为所述待脱敏姓名的长度，Ω为加密轮次空间，Gen为所述随机数生成器，seed为所述预设密钥。

7.一种姓名数据脱敏装置，所述装置包括处理器及存储器，所述存储器上存储有若干计算机程序，其特征在于，所述处理器用于执行存储器中存储的计算机程序时实现如权利要求1-6任一项所述的姓名数据脱敏方法的步骤。

8.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有多条指令，多条所述指令可被一个或者多个处理器执行，以实现如权利要求1-6任一项所述的姓名数据脱敏方法的步骤。

姓名数据脱敏装置、方法及可读存储介质

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种姓名数据脱敏装置、方法及计算机可读存储介质。

背景技术

[0002] 在跨部门信息共享、信息发布等应用场景中，常常需要将客户数据交付给第三方机构、不可信部门、社会公众等，数据交付过程中客户隐私的保护至关重要。姓名是一种具有代表性的用户隐私信息，通常需要进行数据脱敏处理。现有的数据脱敏方法一般是采用基于格式保留的数据脱敏方法，但采用该种脱敏方式在脱敏之后数据无法还原，且相同的明文加密后得到的密文也相同，增加了破解风险。

发明内容

[0003] 有鉴于此，有必要提供一种姓名数据脱敏装置、方法及计算机可读存储介质，脱敏之后的数据可还原，且密文破解难度高。

[0004] 本发明一实施方式提供一种姓名数据脱敏方法，所述方法包括：

[0005] 基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分；

[0006] 判断所述姓氏部分及所述名字部分是否包含有两个或两个以上的词；

[0007] 若所述姓氏部分和/或所述名字部分包含有两个或两个以上的词，则对所述姓氏部分和/或所述名字部分继续进行分解，直至将所述姓氏部分和/或所述名字部分分解至单个词；

[0008] 查找预设姓氏库映射表得到与每一单姓氏词对应的数值，及查找预设名字库映射表得到与每一单名字词对应的数值；

[0009] 根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N，其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子；

[0010] 对每一所述单姓氏词对应的数值进行N次加密得到姓氏加密值，及对每一所述单名字词对应的数值进行N次加密得到名字加密值；

[0011] 查找所述预设姓氏库映射表得到与每一所述姓氏加密值对应的姓氏词，及查找所述预设名字库映射表得到与每一所述名字加密值对应的名字词；及

[0012] 基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名。

[0013] 优选地，所述方法还包括：

[0014] 若查找所述预设姓氏库映射表未得到与某一单姓氏词对应的数值，则根据预设姓氏映射规则建立与未在所述姓氏库映射表中的单姓氏词对应的姓氏映射记录，并将所述姓氏映射记录添加至所述姓氏库映射表中；及

[0015] 若查找所述预设名字库映射表未得到与某一单名字词对应的数值，则根据预设名字映射规则建立与未在所述名字库映射表中的单名字词对应的名字映射记录，并将所述名字映射记录添加至所述名字库映射表中。

[0016] 优选地，所述查找预设姓氏库映射表得到与每一单姓氏词对应的数值之前，还包括：

[0017] 判断分解得到的每一所述单姓氏词是否在所述姓氏库映射表中；

[0018] 若分解得到的某一单姓氏词不在所述姓氏库映射表中，则根据预设姓氏映射规则建立与未在所述姓氏库映射表中的单姓氏词对应的姓氏映射记录，并将所述姓氏映射记录添加至所述姓氏库映射表中；

[0019] 判断分解得到的每一所述单名字词是否在所述名字库映射表中；及

[0020] 若分解得到的某一单名字词不在所述名字库映射表中，则根据预设名字映射规则建立与未在所述名字库映射表中的单名字词对应的名字映射记录，并将所述名字映射记录添加至所述名字库映射表中。

[0021] 优选地，所述迭代轮次N通过以下算式计算得到：

[0022] $$N = \sum_{i=1}^{l} Gen_{seed}(\Omega)/l;$$

[0023] 其中，l为所述待脱敏姓名的长度，Ω为加密轮次空间，Gen为所述随机数生成器，seed为所述预设密钥。

[0024] 优选地，所述预设姓氏库映射表包括多个单姓氏词，每一所述单姓氏词一一对应一唯一的数值，所述对每一所述单姓氏词对应的数值进行N次加密得到姓氏加密值，包括：

[0025] 对所述预设姓氏库映射表进行初始化，得到由每一所述单姓氏词的数值构成的姓氏库数值集；

[0026] 利用预设分组加密算法对所述姓氏库数值集中的每一元素进行加密，得到由每一加密元素构成的第一元组；

[0027] 依据每一所述加密元素的大小对所述第一元组中的每一所述加密元素进行排序；

[0028] 基于每一所述加密元素与所述姓氏库数值集的每一元素的对应关系，将经过排序处理的第一元组转换得到第二元组；及

[0029] 从所述第二元组中提取下标为所述单姓氏词对应的数值的元素，并将提取到的元素作为下一次迭代提取的下标值，直至将第N次提取得到的元素作为所述单姓氏词对应的数值的姓氏加密值。

[0030] 优选地，所述预设名字库映射表包括多个单名字词，每一所述单名字词一一对应一唯一的数值，所述对每一所述单名字词对应的数值进行N次加密得到名字加密值，包括：

[0031] 对所述预设名字库映射表进行初始化，得到由每一所述单名字词的数值构成的名字库数值集；

[0032] 利用预设分组加密算法对所述名字库数值集中的每一元素进行加密，得到由每一加密元素构成的第三元组；

[0033] 依据每一所述加密元素的大小对所述第三元组中的每一所述加密元素进行排序；

[0034] 基于每一所述加密元素与所述名字库数值集的每一元素的对应关系，将经过排序处理的第三元组转换得到第四元组；及

[0035] 从所述第四元组中提取下标为所述单名字词对应的数值的元素，并将提取到的元素作为下一次迭代提取的下标值，直至将第N次提取得到的元素作为所述单名字词对应的数值的名字加密值。

[0036] 优选地，所述方法还包括：

[0037] 基于所述预设分解规则将所述加密姓名分解为加密姓氏部分及加密名字部分；

[0038] 判断所述加密姓氏部分及所述加密名字部分是否包含有两个或两个以上的词；

[0039] 若所述加密姓氏部分和/或所述加密名字部分包含有两个或两个以上的词，则对所述加密姓氏部分和/或所述加密名字部分继续进行分解，直至将所述加密姓氏部分和/或所述加密名字部分分解至单个词；

[0040] 查找所述预设姓氏库映射表得到与每一加密单姓氏词对应的数值，及查找所述预设名字库映射表得到与每一加密单名字词对应的数值；

[0041] 对每一所述加密单姓氏词对应的数值进行N次解密得到姓氏解密值，及对每一所述加密单名字词对应的数值进行N次解密得到名字解密值；

[0042] 查找所述预设姓氏库映射表得到与每一所述姓氏解密值对应的姓氏词，及查找所述预设名字库映射表得到与每一所述名字解密值对应的名字词；及

[0043] 基于查找得到的姓氏词及名字词得到与所述加密姓名对应的待脱敏姓名。

[0044] 本发明一实施方式提供一种姓名数据脱敏方法，所述方法包括：

[0045] 基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分；

[0046] 查找预设姓氏库映射表得到与所述姓氏部分对应的数值，及查找预设名字库映射表得到与所述名字部分对应的数值；

[0047] 根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N，其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子；

[0048] 对所述姓氏部分对应的数值进行N次加密得到姓氏加密值，及对所述名字部分对应的数值进行N次加密得到名字加密值；

[0049] 查找所述预设姓氏库映射表得到与所述姓氏加密值对应的姓氏词，及查找所述预设名字库映射表得到与所述名字加密值对应的名字词；及

[0050] 基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名。

[0051] 本发明一实施方式提供一种姓名数据脱敏装置，所述装置包括处理器及存储器，所述存储器上存储有若干计算机程序，所述处理器用于执行存储器中存储的计算机程序时实现上述姓名数据脱敏方法的步骤。

[0052] 本发明一实施方式还提供一种计算机可读存储介质，所述计算机可读存储介质存储有多条指令，多条所述指令可被一个或者多个处理器执行，以实现上述姓名数据脱敏方法的步骤。

[0053] 与现有技术相比，上述姓名数据脱敏装置、方法及计算机可读存储介质，以加密方所持有的密钥作为生成迭代轮次的随机种子，可以调节加解密的轮次数，减小了密文与明文的相关性，通过调节姓氏加解密的轮次数使相同明文加密后的结果呈现出差异化，可增加密文的迷惑性和破解难度。

附图说明

[0054] 图1是本发明一实施方式的姓名数据脱敏装置的功能模块图。

[0055] 图2是本发明一实施方式的姓名数据脱敏程序的功能模块图。

[0056] 图3是本发明另一实施方式的姓名数据脱敏程序的功能模块图。

[0057] 图4是本发明一实施方式的姓名数据脱敏方法的流程图。

[0058] 图5是本发明另一实施方式的姓名数据脱敏方法的流程图。

[0059] 主要元件符号说明

[0060]

存储器	10

[0061]

处理器	20
姓名数据脱敏程序	30
分解模块	101
判断模块	102
查找模块	103
添加模块	104
第一生成模块	105
加密模块	106
第二生成模块	107
解密模块	108
姓名数据脱敏装置	100

[0062] 如下具体实施方式将结合上述附图进一步说明本发明。

具体实施方式

[0063] 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。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0064] 进一步需要说明的是，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。

[0065] 请参阅图1,为本发明姓名数据脱敏装置较佳实施例的示意图。

[0066] 姓名数据脱敏装置100可以包括存储器10、处理器20以及存储在所述存储器10中并可在所述处理器20上运行的姓名数据脱敏程序30。所述处理器20执行所述姓名数据脱敏程序30时实现姓名数据脱敏方法实施例中的步骤,例如图4所示的步骤S400～S414,或图5所示的步骤S500～S510。或者,所述处理器20执行所述姓名数据脱敏程序30时实现图2中各模块的功能,例如模块101～108,或者实现图3中各模块的功能,例如模块101,103～108。

[0067] 所述姓名数据脱敏程序30可以被分割成一个或多个模块,所述一个或者多个模块被存储在所述存储器10中,并由所述处理器20执行,以完成本发明。所述一个或多个模块可以是能够完成特定功能的一系列计算机程序指令段,所述指令段用于描述所述姓名数据脱敏程序30在所述姓名数据脱敏装置100中的执行过程。例如,所述姓名数据脱敏程序30可以被分割成图2中的分解模块101、判断模块102、查找模块103、添加模块104、第一生成模块105、加密模块106、第二生成模块107及解密模块108,或者被分割成图3中的分解模块101、查找模块103、添加模块104、第一生成模块105、加密模块106、第二生成模块107及解密模块108。各模块具体功能参见下图2、图3中各模块的功能。

[0068] 本领域技术人员可以理解,所述示意图仅是姓名数据脱敏装置100的示例,并不构成对姓名数据脱敏装置100的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件,例如所述姓名数据脱敏装置100还可以包括通信模块、显示模块、总线等。

[0069] 所称处理器20可以是中央处理单元(Central Processing Unit,CPU),还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者所述处理器20也可以是任何常规的处理器等,所述处理器20可以利用各种接口和总线连接姓名数据脱敏装置100的各个部分。

[0070] 所述存储器10可用于存储所述姓名数据脱敏程序30和/或模块,所述处理器20通过运行或执行存储在所述存储器10内的计算机程序和/或模块,以及调用存储在存储器10内的数据,实现所述姓名数据脱敏装置100的各种功能。所述存储器10可以包括高速随机存取存储器,还可以包括非易失性存储器,例如硬盘、内存、插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字(Secure Digital,SD)卡,闪存卡(Flash Card)、至少一个磁盘存储器件、闪存器件、或其他非易失性固态存储器件。

[0071] 图2为本发明姓名数据脱敏程序一较佳实施例的功能模块图。

[0072] 参阅图2所示,姓名数据脱敏程序30可以包括分解模块101、判断模块102、查找模块103、添加模块104、第一生成模块105、加密模块106、第二生成模块107及解密模块108。在一实施方式中,上述模块可以为存储于所述存储器10中且可被所述处理器20调用执行的可程序化软件指令。可以理解的是,在其他实施方式中,上述模块也可为固化于所述处理器20中的程序指令或固件(firmware)。

[0073] 分解模块101用于基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分。

[0074] 在一实施方式中,所述待脱敏姓名可以是中文姓名,所述待脱敏姓名的来源在此不作限定。所述预设分解规则可以包括一个姓名库或姓氏库,分解模块可以基于姓名库或

姓氏库来将待脱敏姓名分解为姓氏部分及名字部分。所述预设分解规则还可以包括当确定某一部分为姓氏部分/名字部分，则其他部分默认被划分为名字部分/姓氏部分。比如，分解模块101通过姓氏库来确定待脱敏姓名的姓氏部分，而其他部分则被认定为名字部分，进而可以将待脱敏姓名分解为姓氏部分及名字部分。在本发明的其他实施方式中，所述待脱敏姓名可以是其他语言类型的姓名，比如英文姓名。

[0075] 举例而言，所述待脱敏姓名为“$X_1X_2X_3X_4$”，姓氏库包括姓氏“X_1X_2”，则分解模块101可以通过姓氏库可以确定该待脱敏姓名的姓氏部分为“X_1X_2”，名字部分则为“X_3X_4”。所述待脱敏姓名为“X_5X_6”，姓氏库包括姓氏“X_5”，则分解模块101可以通过姓氏库可以确定该待脱敏姓名的姓氏部分为“X_5”，名字部分则为“X_6”。

[0076] 判断模块102用于判断所述姓氏部分及所述名字部分是否包含有两个或两个以上的词。

[0077] 在一实施方式中，当分解得到姓氏部分及名字部分后，判断模块102可以判断所述姓氏部分及所述名字部分是否包含有两个或两个以上的词。具体地，判断模块102可以通过分别统计所述姓氏部分、所述名字部分的字数，再判断所述姓氏部分及所述名字部分是否包含有两个或两个以上的词。

[0078] 当所述姓氏部分和/或所述名字部分包含有两个或两个以上的词时，分解模块101还用于对所述姓氏部分和/或所述名字部分继续进行分解，直至将所述姓氏部分和/或所述名字部分分解至单个词。举例而言，若分解到的姓氏部分为“X_1X_2”，该姓氏部分包含2个词，分解模块101对姓氏部分继续进行分解，得到单个词“X_1”与“X_2”；若分解到的姓氏部分为“X_5”，由于该姓氏部分为单个词，因此分解模块101无需对该姓氏部分继续进行分解；若分解到的名字部分为“X_3X_4”，该名字部分包含2个词，分解模块101对名字部分进行继续分解，得到单个词“X_3”与“X_4”。

[0079] 查找模块103用于查找预设姓氏库映射表得到与每一单姓氏词对应的数值，及查找预设名字库映射表得到与每一单名字词对应的数值。

[0080] 在一实施方式中，为了方便后续进行数值运算，所述数值优选为整数值。所述预设姓氏库映射表可以包括多个单姓氏词，每一所述单姓氏词一一对应一唯一的数值，即每一所述单姓氏词对应的数值无重复数值，比如预设姓氏库映射表包括335个单姓氏词，该335个单姓氏词分别对应数值：0,1,2,3,…,334。所述预设名字库映射表可以包括多个单名字词，每一所述单名字词一一对应一唯一的数值，即每一所述单名字词对应的数值无重复数值，比如预设名字库映射表包括900个单名字词，该900个单名字词分别对应数值：0,1,2,3,…,899。

[0081] 在一实施方式中，分解模块101可以将所述姓氏部分分解得到一个或一个以上的单姓氏词，将所述名字部分分解得到一个或一个以上的单名字词。查找模块103可以查找所述预设姓氏库映射表得到与每一单姓氏词对应的数值，及查找预设名字库映射表得到与每一单名字词对应的数值。举例而言，在所述预设姓氏库映射表中，单姓氏词“何”对应的数值为“100”，若对待脱敏姓名分解得到单姓氏词“何”，则查找模块103可以查找所述预设姓氏库映射表得到单姓氏词“何”对应的数值为“100”。在所述预设名字库映射表中，单名字词“林”对应的数值为“50”，单名字词“国”对应的数值为“365”，若对待脱敏姓名分解得到两个单名字词“林”及“国”，则查找模块103可以查找所述预设名字库映射表得到单名字词“林”

对应的数值为“50”，单名字词“国”对应的数值为“365”。

[0082] 在一实施方式中，由于所述预设姓氏库映射表和/或所述预设名字库映射表预先建立的局限性，可能无法包含所有的姓氏词及名字词。在进行单姓氏词查找时，若查找模块103查找所述预设姓氏库映射表未得到与某一单姓氏词对应的数值，则添加模块104可以根据预设姓氏映射规则建立与未在所述姓氏库映射表中的单姓氏词对应的姓氏映射记录，并将所述姓氏映射记录添加至所述姓氏库映射表中。所述预设姓氏映射规则可以根据实际使用需求进行设定，比如按照预设姓氏库映射表中的最后一条姓氏映射记录的数值进行设定。举例而言，所述预设姓氏库映射表包括335个单姓氏词，该335个单姓氏词分别对应数值:0,1,2,3,…,334，最后一条姓氏映射记录为{“单”,334}，假设查找模块103查找所述预设姓氏库映射表未得到与单姓氏词“舒”对应的数值，则添加模块104可以建立一条姓氏映射记录{“舒”,335}，并将{“舒”,335}添加至所述姓氏库映射表中，进而更新后的所述姓氏库映射表包括了336个单姓氏词。

[0083] 在进行单名字词查找时，若查找模块103查找所述预设名字库映射表未得到与某一单名字词对应的数值，则添加模块104可以根据预设名字映射规则建立与未在所述名字库映射表中的单名字词对应的名字映射记录，并将所述名字映射记录添加至所述名字库映射表中。所述预设名字映射规则同样可以根据实际使用需求进行设定，比如按照预设名字库映射表中的最后一条名字映射记录的数值大小顺序进行设定。举例而言，预设名字库映射表包括900个单名字词，该900个单名字词分别对应数值:0,1,2,3,…,899，最后一条名字映射记录为{“雄”,899}，假设查找模块103查找所述预设名字库映射表未得到与单名字词“议”对应的数值，则添加模块104可以建立一条名字映射记录{“议”,900}，并将{“议”,900}添加至所述名字库映射表中，进而更新后的所述名字库映射表包括了901个单名字词。

[0084] 在一实施方式中，在进行单姓氏词查找前，还可以通过判断模块102来判断分解得到的每一所述单姓氏词是否在所述姓氏库映射表中；若判断模块102判定分解得到的某一单姓氏词不在所述姓氏库映射表中，则添加模块104可以根据预设姓氏映射规则建立与未在所述姓氏库映射表中的单姓氏词对应的姓氏映射记录，并将所述姓氏映射记录添加至所述姓氏库映射表中。在进行单名字词查找前，还可以通过判断模块102来判断分解得到的每一所述单名字词是否在所述名字库映射表中；若判断模块102判定分解得到的某一单名字词不在所述名字库映射表中，则添加模块104可以根据预设名字映射规则建立与未在所述名字库映射表中的单名字词对应的名字映射记录，并将所述名字映射记录添加至所述名字库映射表中。

[0085] 第一生成模块105用于根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N，其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子。

[0086] 在一实施方式中，所述预设密钥可以是当前脱敏方所拥有的密钥，不为公众所知。比如所述预设密钥是一个6-10位的数字，也可以是其他位数的数字，在此不作限定。第一生成模块105在生成所述迭代轮次N时，将所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子，进而即使对于相同密钥和姓名长度，每次随机数生成器运行1次，根据随机数生成的原理，迭代轮次N均会不同，实现通过调节姓名加解密的轮次数使得相同明文加密后的结果呈现出差异化，增强了密文的迷惑性和破解难度，减小密文与明文的相关性。

[0087] 在一实施方式中，所述迭代轮次N可以通过以下算式计算得到：

[0088] $N = \sum_{i=1}^{l} Gen_{seed}(\Omega)/l;$

[0089] 其中，l为所述待脱敏姓名的长度，Ω为加密轮次空间，Gen为所述随机数生成器，seed为所述预设密钥K(以预设密钥K作为种子)，Ω的大小可以根据实际需求进行设定，一般可以设定在10～50之间。在本发明的其他实施方式中，第一生成模块105还可以直接根据预设密钥来生成迭代轮次N，其中所述预设密钥同样为生成所述迭代轮次N所使用的随机数生成器的种子。

[0090] 加密模块106用于对每一所述单姓氏词对应的数值进行N次加密得到姓氏加密值，及对每一所述单名字词对应的数值进行N次加密得到名字加密值。

[0091] 在一实施方式中，当计算得到迭代轮次N时，加密模块106可以对分解得到的每一所述单姓氏词对应的数值进行N次加密得到姓氏加密值，及对每一所述单名字词对应的数值进行N次加密得到名字加密值。

[0092] 举例而言，所述预设姓氏库映射表包括n个单姓氏词，该n个单姓氏词分别对应数值:0,1,2,3,…,n-1，通过查找所述预设姓氏库映射表得到某一单姓氏词对应的数值为i，加密模块106对数值i进行N次加密得到姓氏加密值j，具体加密过程可以为:第一步，对所述预设姓氏库映射表进行初始化，得到由每一所述单姓氏词的数值构成的姓氏库数值集M，M＝{0,1,2,…,n-1}；第二步，利用预设分组加密算法(比如AES加密算法、SM4加密算法或其他分组加密算法)对所述姓氏库数值集中的每一元素进行加密，得到由每一加密元素构成的第一元组A，A＝{E(0),E(1),E(2),…,E(n-1)}；第三步，依据每一所述加密元素的大小对所述第一元组中的每一所述加密元素进行排序，可以是从小到大或从大到小进行排序，再基于每一所述加密元素与所述姓氏库数值集的每一元素的对应关系，将经过排序处理的第一元组转换得到第二元组B，B＝{r_0,r_1,r_2,r_{n-1}}，比如经过排序处理的第一元组A＝{E(6),E(16),E(2),…,E(0)}，则r_0对应的数值为“6”，r_1对应的数值为“16”，r_2对应的数值为“2”，r_{n-1}对应的数值为“0”；第四步，从所述第二元组B中提取下标为所述单姓氏词对应的数值i的元素r_i，完成一次迭代加密；第五步，重复第四步，将上一次提取到的元素作为下一次迭代提取的下标值，直至完成N次迭代加密，并将第N次提取得到的元素作为所述单姓氏词对应的数值i的姓氏加密值j。

[0093] 举例而言，姓氏库数值集M＝{0,1,2,3,4,5,6,7,8,9}，对所述姓氏库数值集M中的每一元素进行加密，得到由每一加密元素构成的第一元组A，A＝{E(0),E(1),E(2),E(3),E(4),E(5),E(6),E(7),E(8),E(9)}，依据第一元组A中每一加密元素的大小从小到大排序得到排序处理的第一元组A＝{E(2),E(8),E(3),E(9),E(7),E(5),E(0),E(1),E(4),E(6)}，则第二元组B＝{r_0＝2,r_1＝8,r_2＝3,r_3＝9,r_4＝7,r_5＝5,r_6＝0,r_7＝1),r_8＝4,r_9＝6}，假设迭代轮次N＝3，某一单姓氏词对应的数值为i＝2，则第一轮加密得到r_2＝3，第二轮加密得到r_3＝9，第三轮加密得到r_9＝6，即某一单姓氏词对应的数值i进行N(N＝3)次加密得到姓氏加密值j＝6。

[0094] 可以理解的，若对姓氏加密值“6”进行解密，第一轮解密，即得知r_m＝6，则通过查第二元组B可以得到此轮m＝9；第二轮解密，即得知r_m＝9，则通过查第二元组B得到此轮的m＝3；第三轮解密，即得知r_m＝3，则通过查第二元组B得到此轮的m＝2，即经过三轮解密得到某一单姓氏词对应的数值i＝2。

[0095] 假设所述预设名字库映射表包括2n个单名字词，该2n个单名字词分别对应数值：

0,1,2,3,…,2n-1,通过查找所述预设名字库映射表得到某一单名字词对应的数值为p,加密模块106对单名字词对应的数值p进行N次加密得到名字加密值的过程可以是:第一步,对所述预设名字库映射表进行初始化,得到由每一所述单名字词的数值构成的名字库数值集N,N＝{0,1,2,…,2n-1};第二步,利用所述预设分组加密算法对所述名字库数值集中的每一元素进行加密,得到由每一加密元素构成的第三元组C,C＝{E(0),E(1),E(2),…,E(2n-1)};第三步,依据每一所述加密元素的大小对所述第三元组C中的每一所述加密元素进行排序,再基于每一所述加密元素与所述名字库数值集的每一元素的对应关系,将经过排序处理的第三元组转换得到第四元组D,D＝{r_0,r_1,r_2,r_{2n-1}};第四步,从所述第四元组D中提取下标为所述单名字词对应的数值的元素,并将提取到的元素作为下一次迭代提取的下标值,直至将第N次提取得到的元素作为所述单名字词对应的数值p的名字加密值q。可以理解的,加密模块106对单名字词对应的数值p进行N次加密的过程与对单姓氏词对应的数值i进行N次加密的过程基本相同,在此不再举例说明。

[0096] 当加密得到每一所述单姓氏词对应的数值的姓氏加密值,及每一所述单名字词对应的数值的名字加密值时,查找模块103可以查找所述预设姓氏库映射表得到与每一所述姓氏加密值对应的姓氏词,及查找所述预设名字库映射表得到与每一所述名字加密值对应的名字词。

[0097] 举例而言,待脱敏姓名为“林三”,经过分解得到单姓氏词为“林”,单名字词为“三”,假设通过查找模块103查找所述预设姓氏库映射表得到“林”对应的数值为“3”,查找所述预设名字库映射表得到“三”对应的数值为“50”;通过加密模块106对“林”对应的数值“3”进行N次加密得到姓氏加密值“10”,对“三”对应的数值“50”进行N次加密得到名字加密值“5”,假设所述预设姓氏库映射表的一姓氏映射记录为{张,10},所述预设名字库映射表的一名字映射记录为{谦,5},则查找模块103可以查找得到姓氏加密值“10”对应的姓氏词为“张”,名字加密值“5”对应的名字词为“谦”。

[0098] 第二生成模块107用于基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名。

[0099] 在一实施方式中,当查找模块103查找得到每一所述姓氏加密值对应的姓氏词及每一所述名字加密值对应的名字词时,第二生成模块107可以基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名。比如待脱敏姓名为“林三”,查找模块103可以查找得到姓氏加密值“10”对应的姓氏词为“张”,名字加密值“5”对应的名字词为“谦”,则第二生成模块107得到与所述待脱敏姓名对应的加密姓名为“张谦”。

[0100] 在一实施方式中,可以通过所述预设密钥对加密姓名进行解密得到初始的待脱敏姓名,比如对加密姓名“张谦”进行解密得到待脱敏姓名“林三”。解密过程即为上述加密过程的逆过程,解密过程可以包括:分解模块101基于预设分解规则将所述加密姓名分解为加密姓氏部分及加密名字部分;判断模块102判断所述加密姓氏部分及所述加密名字部分是否包含有两个或两个以上的词;若所述加密姓氏部分和/或所述加密名字部分包含有两个或两个以上的词,则分解模块101对所述加密姓氏部分和/或所述加密名字部分继续进行分解,直至将所述加密姓氏部分和/或所述加密名字部分分解至单个词;查找模块103查找所述预设姓氏库映射表得到与每一加密单姓氏词对应的数值,及查找所述预设名字库映射表得到与每一加密单名字词对应的数值;解密模块108对每一所述加密单姓氏词对应的数值

进行N次解密得到姓氏解密值，及对每一所述加密单名字词对应的数值进行N次解密得到名字解密值；查找模块103查找所述预设姓氏库映射表得到与每一所述姓氏解密值对应的姓氏词，及查找所述预设名字库映射表得到与每一所述名字解密值对应的名字词；第二生成模块107基于查找得到的姓氏词及名字词得到与加密姓名对应的原始待脱敏姓名。

[0101] 图3为本发明姓名数据脱敏程序另一较佳实施例的功能模块图。

[0102] 参阅图3所示，与图2相比，姓名数据脱敏程序30省去了判断模块102。图3的姓名数据脱敏程序30包括分解模块101、查找模块103、添加模块104、第一生成模块105、加密模块106、第二生成模块107及解密模块108。在一实施方式中，上述模块可以为存储于所述存储器10中且可被所述处理器20调用执行的可程序化软件指令。可以理解的是，在其他实施方式中，上述模块也可为固化于所述处理器20中的程序指令或固件(firmware)。

[0103] 分解模块101用于基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分。

[0104] 在一实施方式中，所述待脱敏姓名可以是中文姓名，所述待脱敏姓名的来源在此不作限定。所述预设分解规则可以包括一个姓名库或姓氏库，分解模块可以基于姓名库或姓氏库来将待脱敏姓名分解为姓氏部分及名字部分。所述预设分解规则还可以包括当确定某一部分为姓氏部分/名字部分，则其他部分默认被划分为名字部分/姓氏部分。比如，分解模块101通过姓氏库来确定待脱敏姓名的姓氏部分，而其他部分则被认定为名字部分，进而可以将待脱敏姓名分解为姓氏部分及名字部分。在本发明的其他实施方式中，所述待脱敏姓名可以是其他语言类型的姓名，比如英文姓名。

[0105] 举例而言，所述待脱敏姓名为“$X_1X_2X_3X_4$”，姓氏库包括姓氏“X_1X_2”，则分解模块101可以通过姓氏库可以确定该待脱敏姓名的姓氏部分为“X_1X_2”，名字部分则为“X_3X_4”。所述待脱敏姓名为“X_5X_6”，姓氏库包括姓氏“X_5”，则分解模块101可以通过姓氏库可以确定该待脱敏姓名的姓氏部分为“X_5”，名字部分则为“X_6”。

[0106] 查找模块103用于查找预设姓氏库映射表得到与所述姓氏部分对应的数值，及查找预设名字库映射表得到与所述名字部分对应的数值。

[0107] 在一实施方式中，为了方便后续进行数值运算，所述数值优选为整数值。所述预设姓氏库映射表可以包括多个姓氏词，每一所述姓氏词一一对应一唯一的数值，即每一所述姓氏词对应的数值无重复数值，比如预设姓氏库映射表包括335个姓氏词(可以是单姓氏词，双姓氏词等)，该335个姓氏词分别对应数值：0,1,2,3,…,334。所述预设名字库映射表可以包括多个名字词(可以是单名字词，双名字词，三名字词等)，每一所述名字词一一对应一唯一的数值，即每一所述名字词对应的数值无重复数值，比如预设名字库映射表包括900个名字词，该900个名字词分别对应数值：0,1,2,3,…,899。

[0108] 举例而言，在所述预设姓氏库映射表中，姓氏词“何”对应的数值为“100”，若对待脱敏姓名分解得到姓氏词“何”，则查找模块103可以查找所述预设姓氏库映射表得到姓氏词“何”对应的数值为“100”；姓氏词“上官”对应的数值为“110”，若对待脱敏姓名分解得到姓氏词“上官”，则查找模块103可以查找所述预设姓氏库映射表得到姓氏词“上官”对应的数值为“110”。

[0109] 在一实施方式中，由于所述预设姓氏库映射表和/或所述预设名字库映射表预先建立的局限性，可能无法包含所有的姓氏词及名字词。在进行姓氏词查找时，若查找模块103查找所述预设姓氏库映射表未得到与某一姓氏词对应的数值，则添加模块104可以根据

预设姓氏映射规则建立与未在所述姓氏库映射表中的姓氏词对应的姓氏映射记录，并将所述姓氏映射记录添加至所述姓氏库映射表中。所述预设姓氏映射规则可以根据实际使用需求进行设定，比如按照预设姓氏库映射表中的最后一条姓氏映射记录的数值进行设定。举例而言，所述预设姓氏库映射表包括335个单姓氏词，该335个单姓氏词分别对应数值：0,1,2,3,…,334，最后一条姓氏映射记录为{“单”,334}，假设查找模块103查找所述预设姓氏库映射表未得到与姓氏词“舒”对应的数值，则添加模块104可以建立一条姓氏映射记录{“舒”,335}，并将{“舒”,335}添加至所述姓氏库映射表中，进而更新后的所述姓氏库映射表包括了336个姓氏词。

[0110] 在进行名字词查找时，若查找模块103查找所述预设名字库映射表未得到与某一名字词对应的数值，则添加模块104可以根据预设名字映射规则建立与未在所述名字库映射表中的名字词对应的名字映射记录，并将所述名字映射记录添加至所述名字库映射表中。所述预设名字映射规则同样可以根据实际使用需求进行设定，比如按照预设名字库映射表中的最后一条名字映射记录的数值大小顺序进行设定。举例而言，预设名字库映射表包括900个名字词，该900个名字词分别对应数值：0,1,2,3,…,899，最后一条名字映射记录为{“雄”,899}，假设查找模块103查找所述预设名字库映射表未得到与名字词“婉儿”对应的数值，则添加模块104可以建立一条名字映射记录{“婉儿”,900}，并将{“婉儿”,900}添加至所述名字库映射表中，进而更新后的所述名字库映射表包括了901个名字词。

[0111] 在一实施方式中，在进行姓氏词查找前，还可以通过判断模块102来判断分解得到的姓氏部分是否在所述姓氏库映射表中；若判断模块102判定分解得到的姓氏部分不在所述姓氏库映射表中，则添加模块104可以根据预设姓氏映射规则建立与未在所述姓氏库映射表中的姓氏词对应的姓氏映射记录，并将所述姓氏映射记录添加至所述姓氏库映射表中。在进行名字词查找前，还可以通过判断模块102来判断分解得到的名字部分是否在所述名字库映射表中；若判断模块102判定分解得到的名字部分不在所述名字库映射表中，则添加模块104可以根据预设名字映射规则建立与未在所述名字库映射表中的名字词对应的名字映射记录，并将所述名字映射记录添加至所述名字库映射表中。

[0112] 第一生成模块105用于根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N，其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子。

[0113] 在一实施方式中，所述预设密钥可以是当前脱敏方所拥有的密钥，不为公众所知。比如所述预设密钥是一个6-10位的数字，也可以是其他位数的数字，在此不作限定。第一生成模块105在生成所述迭代轮次N时，将所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子，进而即使对于相同密钥和姓名长度，每次随机数生成器运行1次，根据随机数生成的原理，迭代轮次N均会不同，实现通过调节姓名加解密的轮次数使得相同明文加密后的结果呈现出差异化，增强了密文的迷惑性和破解难度，减小密文与明文的相关性。

[0114] 在一实施方式中，所述迭代轮次N可以通过以下算式计算得到：

[0115] $$N = \sum_{i=1}^{l} Gen_{seed}(\Omega)/l;$$

[0116] 其中，l为所述待脱敏姓名的长度，Ω为加密轮次空间，Gen为所述随机数生成器，seed为所述预设密钥K(以预设密钥K作为种子)，Ω的大小可以根据实际需求进行设定，一般可以设定在10～50之间。在本发明的其他实施方式中，第一生成模块105还可以直接根据预设密钥来生成迭代轮次N，其中所述预设密钥同样为生成所述迭代轮次N所使用的随机数

生成器的种子。

[0117] 加密模块106用于对所述姓氏部分对应的数值进行N次加密得到姓氏加密值，及对所述名字部分对应的数值进行N次加密得到名字加密值。

[0118] 在一实施方式中，当计算得到迭代轮次N时，加密模块106可以对分解得到的姓氏部分对应的数值进行N次加密得到姓氏加密值，及对分解得到的名字部分对应的数值进行N次加密得到名字加密值。可以理解的，姓氏部分对应的数值与名字部分对应的数值的加密过程与上一实施例的加密过程基本相同，在此不再赘述。

[0119] 当加密得到姓氏部分对应的数值的姓氏加密值，及名字部分对应的数值的名字加密值时，查找模块103可以查找所述预设姓氏库映射表得到与所述姓氏加密值对应的姓氏词，及查找所述预设名字库映射表得到与所述名字加密值对应的名字词。

[0120] 第二生成模块107用于基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名。

[0121] 在一实施方式中，当查找模块103查找得到所述姓氏加密值对应的姓氏词及所述名字加密值对应的名字词时，第二生成模块107可以基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名。比如待脱敏姓名为“林三”，查找模块103查找得到姓氏加密值“10”对应的姓氏词为“张”，名字加密值“5”对应的名字词为“谦”，则第二生成模块107得到与所述待脱敏姓名对应的加密姓名为“张谦”。

[0122] 在一实施方式中，可以通过所述预设密钥对加密姓名进行解密得到初始的待脱敏姓名，比如对加密姓名“张谦”进行解密得到待脱敏姓名“林三”。解密过程即为上述加密过程的逆过程，其与上一实施例的解密过程基本相同，在此不再赘述。

[0123] 图4为本发明一实施方式中姓名数据脱敏方法的流程图。根据不同的需求，所述流程图中步骤的顺序可以改变，某些步骤可以省略。

[0124] 步骤S400，基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分。

[0125] 步骤S402，判断所述姓氏部分及所述名字部分是否包含有两个或两个以上的词。

[0126] 步骤S404，若所述姓氏部分和/或所述名字部分包含有两个或两个以上的词，则对所述姓氏部分和/或所述名字部分继续进行分解，直至将所述姓氏部分和/或所述名字部分分解至单个词。若所述姓氏部分和所述名字部分均不包含有两个或两个以上的词，则跳转至步骤S406。

[0127] 步骤S406，查找预设姓氏库映射表得到与每一单姓氏词对应的数值，及查找预设名字库映射表得到与每一单名字词对应的数值。

[0128] 步骤S408，根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N，其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子。

[0129] 步骤S410，对每一所述单姓氏词对应的数值进行N次加密得到姓氏加密值，及对每一所述单名字词对应的数值进行N次加密得到名字加密值。

[0130] 步骤S412，查找所述预设姓氏库映射表得到与每一所述姓氏加密值对应的姓氏词，及查找所述预设名字库映射表得到与每一所述名字加密值对应的名字词。

[0131] 步骤S414，基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名。

[0132] 图5为本发明另一实施方式中姓名数据脱敏方法的流程图。根据不同的需求，所述

流程图中步骤的顺序可以改变，某些步骤可以省略。

[0133] 步骤S500，基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分。

[0134] 步骤S502，查找预设姓氏库映射表得到与所述姓氏部分对应的数值，及查找预设名字库映射表得到与所述名字部分对应的数值。

[0135] 步骤S504，根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N，其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子。

[0136] 步骤S506，对所述姓氏部分对应的数值进行N次加密得到姓氏加密值，及对所述名字部分对应的数值进行N次加密得到名字加密值。

[0137] 步骤S508，查找所述预设姓氏库映射表得到与所述姓氏加密值对应的姓氏词，及查找所述预设名字库映射表得到与所述名字加密值对应的名字词。

[0138] 步骤S510，基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名。

[0139] 上述姓名数据脱敏装置、方法及计算机可读存储介质，以加密方所持有的密钥作为生成迭代轮次的随机种子，可以调节加解密的轮次数，减小了密文与明文的相关性，通过调节姓氏加解密的轮次数使相同明文加密后的结果呈现出差异化，可增加密文的迷惑性和破解难度。

[0140] 对本领域的技术人员来说，可以根据本发明的发明方案和发明构思结合生产的实际需要做出其他相应的改变或调整，而这些改变和调整都应属于本发明所公开的范围。

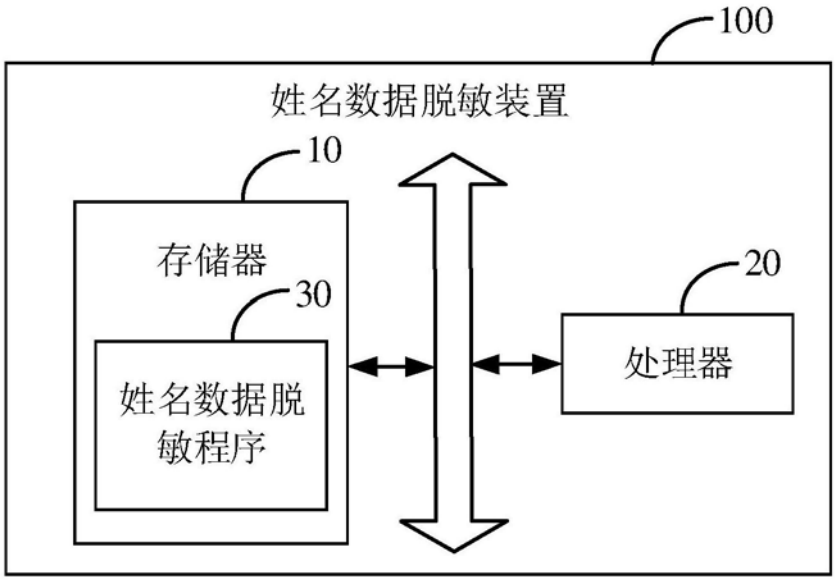

图1

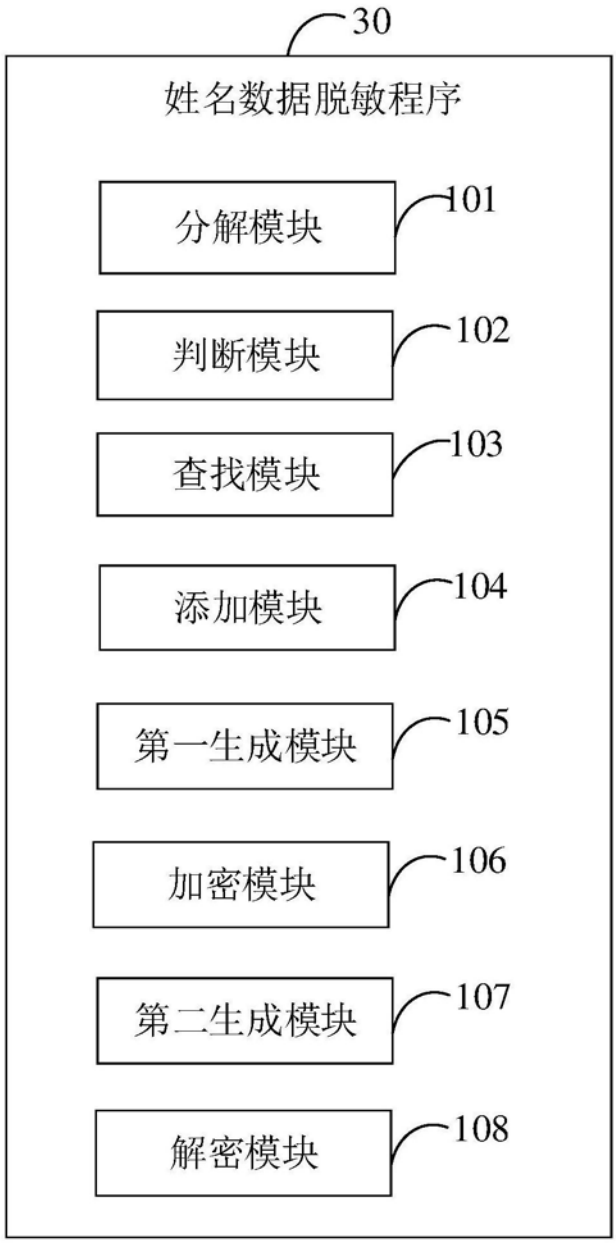
30
姓名数据脱敏程序
分解模块
101
判断模块
102
查找模块
103
添加模块
104
第一生成模块
105
加密模块
106
第二生成模块
107
解密模块
108

图2

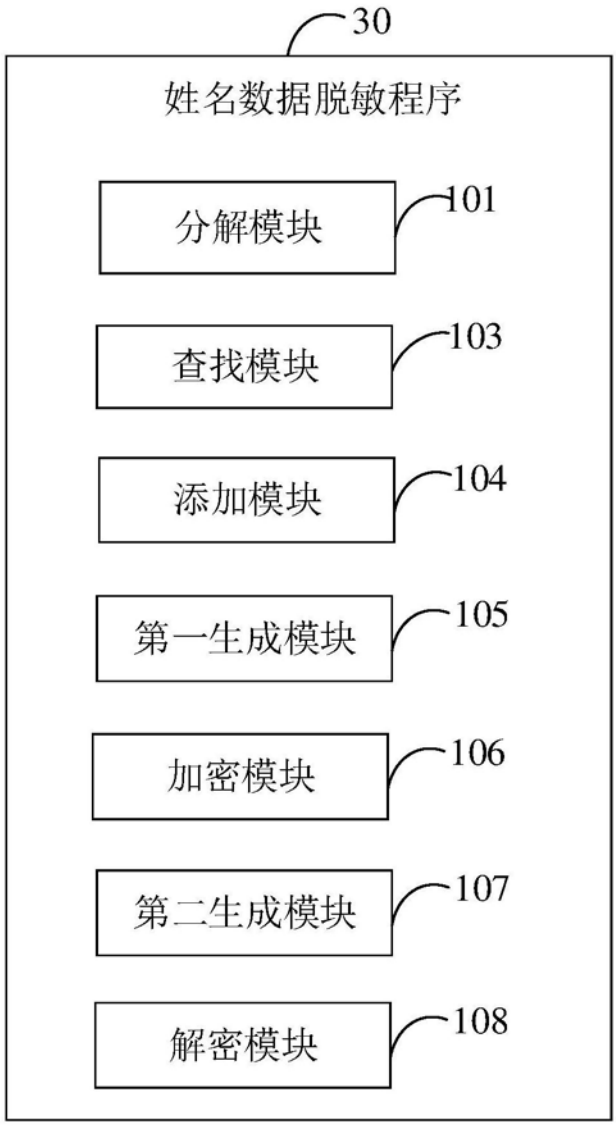
30
姓名数据脱敏程序
分解模块
101
查找模块
103
添加模块
104
第一生成模块
105
加密模块
106
第二生成模块
107
解密模块
108

图3

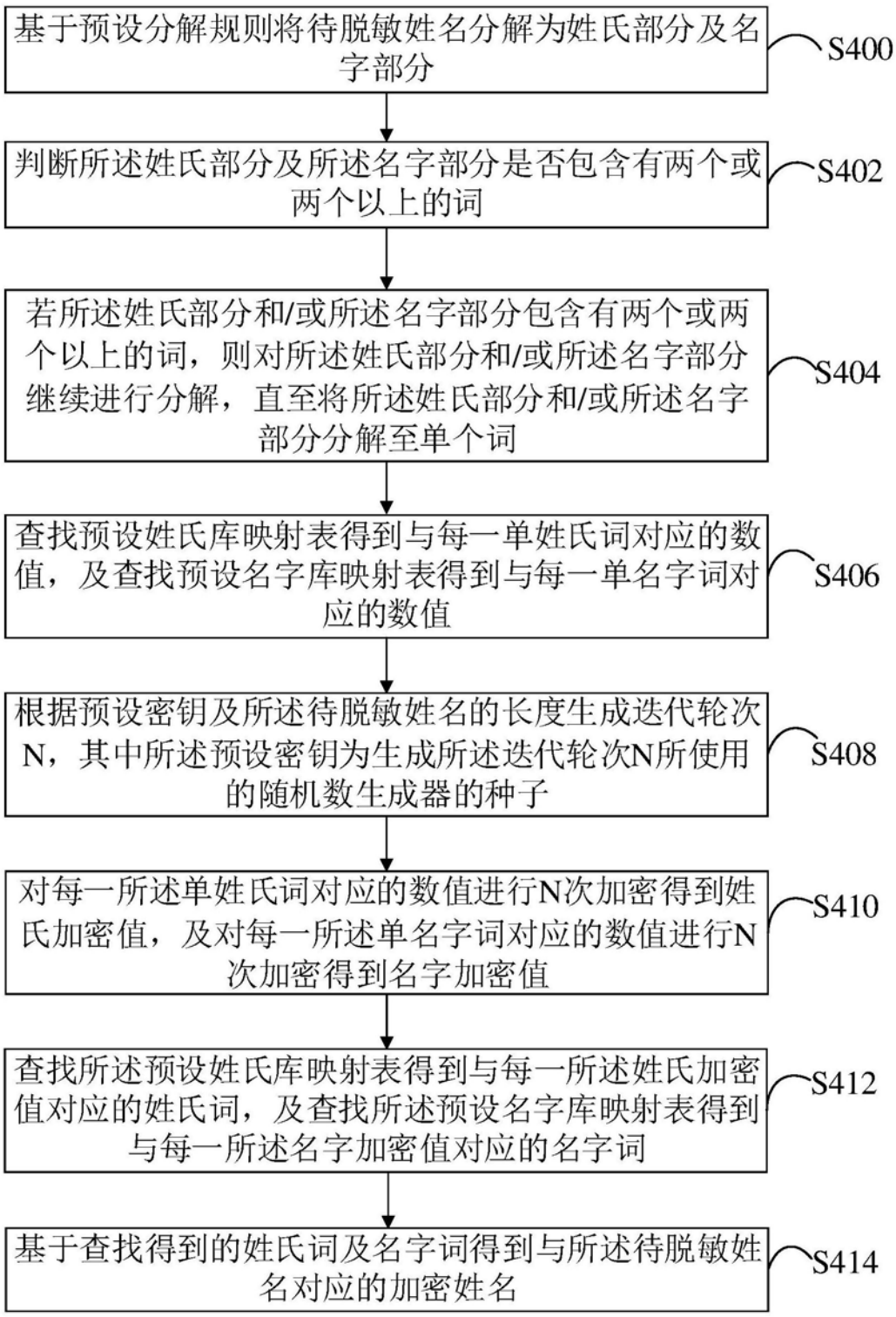
基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分
S400
判断所述姓氏部分及所述名字部分是否包含有两个或两个以上的词
S402
若所述姓氏部分和/或所述名字部分包含有两个或两个以上的词，则对所述姓氏部分和/或所述名字部分继续进行分解，直至将所述姓氏部分和/或所述名字部分分解至单个词
S404
查找预设姓氏库映射表得到与每一单姓氏词对应的数值，及查找预设名字库映射表得到与每一单名字词对应的数值
S406
根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N，其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子
S408
对每一所述单姓氏词对应的数值进行N次加密得到姓氏加密值，及对每一所述单名字词对应的数值进行N次加密得到名字加密值
S410
查找所述预设姓氏库映射表得到与每一所述姓氏加密值对应的姓氏词，及查找所述预设名字库映射表得到与每一所述名字加密值对应的名字词
S412
基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名
S414

图4

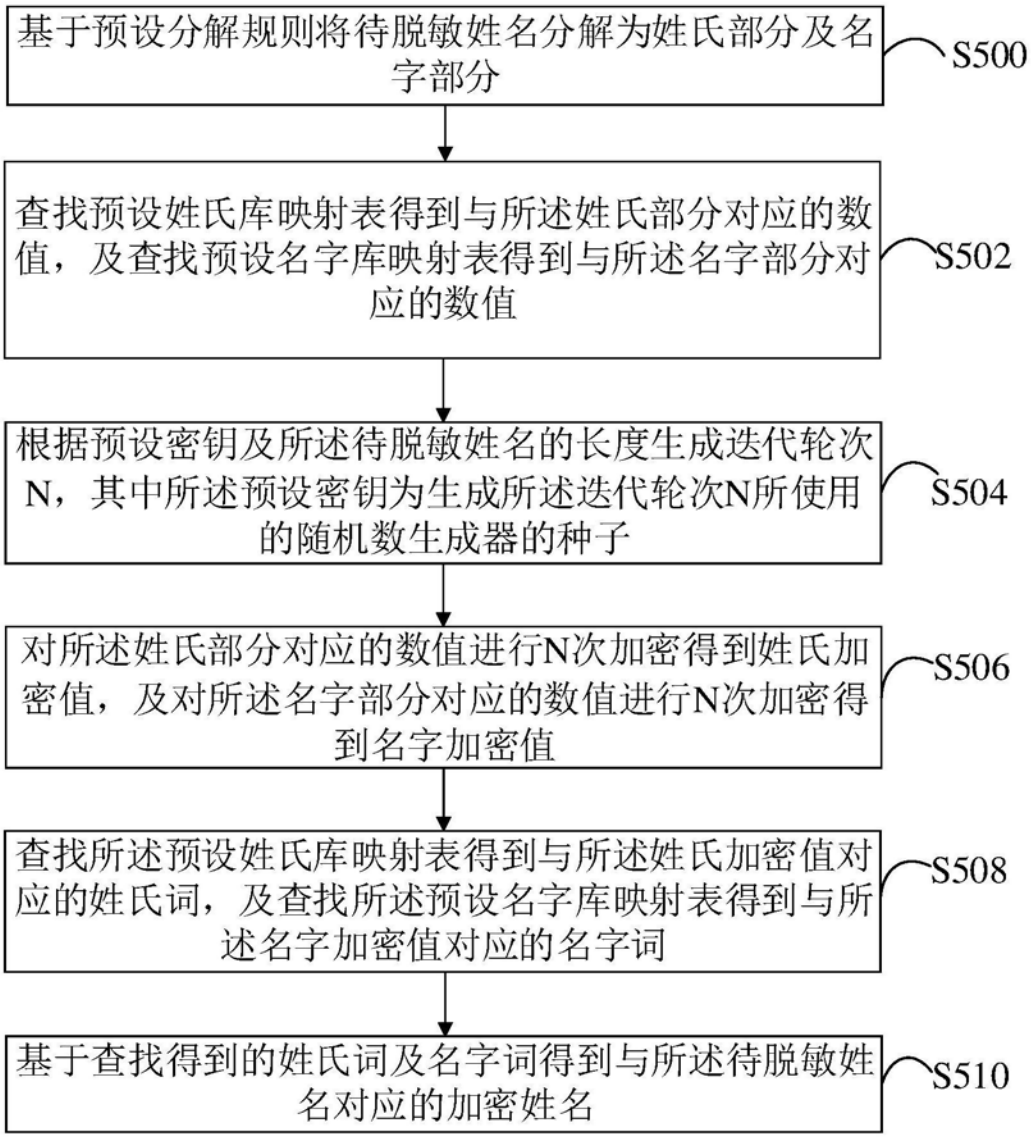
基于预设分解规则将待脱敏姓名分解为姓氏部分及名字部分
S500
查找预设姓氏库映射表得到与所述姓氏部分对应的数值，及查找预设名字库映射表得到与所述名字部分对应的数值
S502
根据预设密钥及所述待脱敏姓名的长度生成迭代轮次N，其中所述预设密钥为生成所述迭代轮次N所使用的随机数生成器的种子
S504
对所述姓氏部分对应的数值进行N次加密得到姓氏加密值，及对所述名字部分对应的数值进行N次加密得到名字加密值
S506
查找所述预设姓氏库映射表得到与所述姓氏加密值对应的姓氏词，及查找所述预设名字库映射表得到与所述名字加密值对应的名字词
S508
基于查找得到的姓氏词及名字词得到与所述待脱敏姓名对应的加密姓名
S510

图5