(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 108063742 B
(45)授权公告日 2021.06.29

(21)申请号 201610977429.5

(22)申请日 2016.11.07

(65)同一申请的已公布的文献号
申请公布号 CN 108063742 A

(43)申请公布日 2018.05.22

(73)专利权人 北京京东尚科信息技术有限公司
地址 100195 北京市海淀区杏石口路65号西杉创意园四区11号楼东段1-4层西段1-4层
专利权人 北京京东世纪贸易有限公司

(72)发明人 钟颖

(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 张一军 姜劲

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)
G06F 21/62(2013.01)

(56)对比文件
CN 103942470 A,2014.07.23
CN 106022039 A,2016.10.12

审查员 吴晗

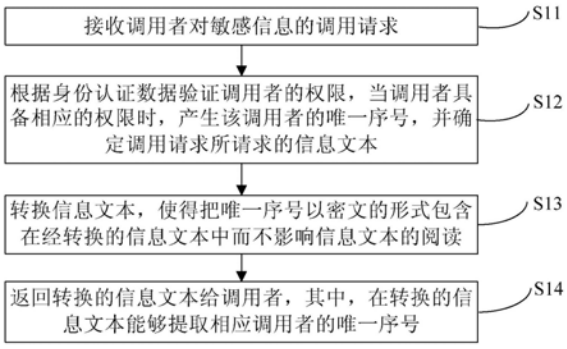
权利要求书3页 说明书9页 附图3页

(54)发明名称

一种敏感信息提供和跟踪方法及装置

(57)摘要

本发明提供一种敏感信息提供和跟踪方法及装置，在敏感信息中加入调用者的相关信息，在不影响敏感信息阅读的情况下，可以跟踪到相关人员对敏感信息的调用情况，使得当有调用者泄漏敏感信息时可以跟踪泄密来源。本发明的敏感信息提供和跟踪方法包括：接收调用者对敏感信息的调用请求，该调用请求具有该调用者的身份认证数据；根据身份认证数据验证调用者的权限，当调用者具备相应的权限时，产生该调用者的唯一序号，并确定调用请求所请求的信息文本；转换信息文本，使得把唯一序号以密文的形式包含在经转换的信息文本中而不影响信息文本的阅读；返回转换的信息文本给调用者，其中，在转换的信息文本能够提取相应调用者的唯一序号。



CN 108063742 B

1.一种敏感信息提供和跟踪方法,其特征在于,包括:

接收调用者对敏感信息的调用请求,该调用请求具有该调用者的身份认证数据;

根据所述身份认证数据验证所述调用者的权限,当所述调用者具备相应的权限时,产生该调用者的唯一序号,并确定所述调用请求所请求的信息文本;

转换所述信息文本,使得把所述唯一序号以密文的形式包含在经转换的信息文本中而不影响所述信息文本的阅读;其中,所述转换所述信息文本,包括:选择所述信息文本的文本段,该文本段包括连续N个字符,使得按顺序所述唯一序号的二进制数表示的每位二进制数对应该文本段的一个字符,对所述唯一序号的二进制数表示的每位二进制数,执行该二进制数与对应的字符的二进制码的末位数字的第一逻辑运算,并且根据运算结果在该字符后面增补空格,所增补空格的数量与该运算结果相对应;N是正整数且为所述唯一序号的二进制数表示的长度;

返回所述转换的信息文本给所述调用者,

其中,在所述转换的信息文本能够提取相应调用者的唯一序号。

2.根据权利要求1所述的方法,其特征在于,

提取相应调用者的唯一序号包括:

去除所述转换的信息文本中包括所选择文本段的部分的增补空格,然后根据相应字符后面被去除的增补空格的数量,将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算,得到N个运算结果,根据所述运算结果组成的二进制序列得到所述调用者的唯一序号。

3.根据权利要求2所述的方法,其特征在于,所述第一逻辑运算为异或运算,并且,根据运算结果在该字符后面增补空格,包括:

当所述字符非空格时,

如果运算结果为0,则在该字符后面生成0个增补空格;

如果运算结果为1,则在该字符后面生成1个增补空格;

当所述字符是空格时,

如果运算结果为0,则在该字符后面生成1个增补空格;

如果运算结果为1,则在该字符后面生成2个增补空格。

4.根据权利要求3所述的方法,其特征在于,所述第二逻辑运算为异或运算,并且,根据相应字符后面被去除的增补空格的数量,将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算,包括:

当该字符非空格时,

如果去除的增补空格的数量为0,则将该字符的二进制码的末位数字与0进行异或运算;

如果去除的增补空格的数量为1,将该字符的二进制码的末位数字与1进行异或运算;

当该字符是空格时,

如果去除的增补空格的数量为1,则将该字符的二进制码的末位数字与0进行异或运算;

如果去除的增补空格的数量为2,则将该字符的二进制码的末位数字与1进行异或运算。

5.根据权利要求2所述的方法,其特征在于,确定所述调用请求所请求的信息文本的步骤之后,还包括:

对所述信息文本执行去空格处理,以使所述信息文本的非空格字符之间最多包含一个空格。

6.一种敏感信息提供和跟踪装置,其特征在于,包括:

接收模块,用于接收调用者对敏感信息的调用请求,该调用请求具有该调用者的身份认证数据;

验证模块,用于根据所述身份认证数据验证所述调用者的权限,当所述调用者具备相应的权限时,产生该调用者的唯一序号,并确定所述调用请求所请求的信息文本;

转换模块,用于转换所述信息文本,使得把所述唯一序号以密文的形式包含在经转换的信息文本中而不影响所述信息文本的阅读;其中,通过如下方式转换所述信息文本:选择所述信息文本的文本段,该文本段包括连续N个字符,使得按顺序所述唯一序号的二进制数表示的每位二进制数对应该文本段的一个字符,对所述唯一序号的二进制数表示的每位二进制数,执行该二进制数与对应的字符的二进制码的末位数字的第一逻辑运算,并且根据运算结果在该字符后面增补空格,所增补空格的数量与该运算结果相对应;N是正整数且为所述唯一序号的二进制数表示的长度;

返回模块,用于返回所述转换的信息文本给所述调用者;

提取模块,用于在所述转换的信息文本提取相应调用者的唯一序号。

7.根据权利要求6所述的装置,其特征在于,

所述提取模块还用于:

去除所述转换的信息文本中包括所选择文本段的部分的增补空格,然后根据相应字符后面被去除的增补空格的数量,将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算,得到N个运算结果,根据所述运算结果组成的二进制序列得到所述调用者的唯一序号。

8.根据权利要求7所述的装置,其特征在于,所述第一逻辑运算为异或运算,并且,根据运算结果在该字符后面增补空格,包括:

当所述字符非空格时,

如果运算结果为0,则在该字符后面生成0个增补空格;

如果运算结果为1,则在该字符后面生成1个增补空格;

当所述字符是空格时,

如果运算结果为0,则在该字符后面生成1个增补空格;

如果运算结果为1,则在该字符后面生成2个增补空格。

9.根据权利要求8所述的装置,其特征在于,所述第二逻辑运算为异或运算,并且,根据相应字符后面被去除的增补空格的数量,将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算,包括:

当该字符非空格时,

如果去除的增补空格的数量为0,则将该字符的二进制码的末位数字与0进行异或运算;

如果去除的增补空格的数量为1,将该字符的二进制码的末位数字与1进行异或运算;

当该字符是空格时，

如果去除的增补空格的数量为1，则将该字符的二进制码的末位数字与0进行异或运算；

如果去除的增补空格的数量为2，则将该字符的二进制码的末位数字与1进行异或运算。

10.根据权利要求7所述的装置，其特征在于，所述装置还包括处理模块：

所述处理模块用于对所述信息文本执行去空格处理，以使所述信息文本的非空格字符之间最多包含一个空格。

一种敏感信息提供和跟踪方法及装置

技术领域

[0001] 本发明涉及计算机及其软件技术领域，特别地涉及一种敏感信息提供和跟踪方法及装置。

背景技术

[0002] 在信息时代，敏感信息的泄漏给企业系统造成很大的信息安全隐患，因此敏感信息的管理不容忽视。所谓敏感信息，是指当其丢失、不当使用或未经授权而被人接触或修改时，将不利于国家利益或政府计划的实行，或者不利于个人依法享有的个人隐私权的所有信息。

[0003] 对于企业系统，例如电商企业，敏感信息包含但不限于以下信息：用户姓名、用户联系电话、送货地址、订单金额等。由于电商企业对外部用户通常都有严格的权限控制，因此，现有电商企业中敏感信息的泄漏大多由内部人员泄漏出去，对于这种情况，目前电商企业采用的解决方案通常是通过严格的权限控制和分级的数据使用来避免敏感信息的外泄。

[0004] 然而，由于电商企业内部人员较多，权限控制比较困难，一旦发生敏感信息外泄的情况，往往难以追踪外泄的源头，造成对内威胁力不够，损失难以挽回。

发明内容

[0005] 有鉴于此，本发明提供一种敏感信息提供和跟踪方法及装置，在敏感信息中加入调用者的相关信息，在不影响敏感信息阅读的情况下，可以跟踪到相关人员对敏感信息的调用情况，使得当有调用者泄漏敏感信息时可以跟踪泄密来源。

[0006] 为实现上述目的，根据本发明的一个方面，提供了一种敏感信息提供和跟踪方法。

[0007] 一种敏感信息提供和跟踪方法，包括：接收调用者对敏感信息的调用请求，该调用请求具有该调用者的身份认证数据；根据所述身份认证数据验证所述调用者的权限，当所述调用者具备相应的权限时，产生该调用者的唯一序号，并确定所述调用请求所请求的信息文本；转换所述信息文本，使得把所述唯一序号以密文的形式包含在经转换的信息文本中而不影响所述信息文本的阅读；返回所述转换的信息文本给所述调用者，其中，在所述转换的信息文本能够提取相应调用者的唯一序号。

[0008] 可选地，所述唯一序号的二进制数表示的长度是N，N是正整数，所述的转换所述信息文本包括：选择所述信息文本的文本段，该文本段包括连续N个字符，使得按顺序所述唯一序号的二进制数表示的每位二进制数对应该文本段的一个字符，对所述唯一序号的二进制数表示的每位二进制数，执行该二进制数与对应的字符的二进制码的末位数字的第一逻辑运算，并且根据运算结果在该字符后面增补空格，所增补空格的数量与该运算结果相对应；以及，提取相应调用者的唯一序号包括：去除所述转换的信息文本中包括所选择文本段的部分的增补空格，然后根据相应字符后面被去除的增补空格的数量，将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算，得到N个运算结果，根据所述运算结果组成的二进制序列得到所述调用者的唯一序号。

[0009] 可选地，所述第一逻辑运算为异或运算，并且，根据运算结果在该字符后面增补空格，包括：当所述字符非空格时，如果运算结果为0，则在该字符后面生成0个增补空格；如果运算结果为1，则在该字符后面生成1个增补空格；当所述字符是空格时，如果运算结果为0，则在该字符后面生成1个增补空格；如果运算结果为1，则在该字符后面生成2个增补空格。

[0010] 可选地，所述第二逻辑运算为异或运算，并且，根据相应字符后面被去除的增补空格的数量，将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算，包括：当该字符非空格时，如果去除的增补空格的数量为0，则将该字符的二进制码的末位数字与0进行异或运算；如果去除的增补空格的数量为1，将该字符的二进制码的末位数字与1进行异或运算；当该字符是空格时，如果去除的增补空格的数量为1，则将该字符的二进制码的末位数字与0进行异或运算；如果去除的增补空格的数量为2，则将该字符的二进制码的末位数字与1进行异或运算。

[0011] 可选地，确定所述调用请求所请求的信息文本的步骤之后，还包括：对所述信息文本执行去空格处理，以使所述信息文本的非空格字符之间最多包含一个空格。

[0012] 根据本发明的另一方面，提供了一种敏感信息提供和跟踪装置。

[0013] 一种敏感信息提供和跟踪装置，包括：接收模块，用于接收调用者对敏感信息的调用请求，该调用请求具有该调用者的身份认证数据；验证模块，用于根据所述身份认证数据验证所述调用者的权限，当所述调用者具备相应的权限时，产生该调用者的唯一序号，并确定所述调用请求所请求的信息文本；转换模块，用于转换所述信息文本，使得把所述唯一序号以密文的形式包含在经转换的信息文本中而不影响所述信息文本的阅读；返回模块，用于返回所述转换的信息文本给所述调用者；提取模块，用于在所述转换的信息文本提取相应调用者的唯一序号。

[0014] 可选地，所述唯一序号的二进制数表示的长度是N，N是正整数，

[0015] 所述转换模块还用于：选择所述信息文本的文本段，该文本段包括连续N个字符，使得按顺序所述唯一序号的二进制数表示的每位二进制数对应该文本段的一个字符，对所述唯一序号的二进制数表示的每位二进制数，执行该二进制数与对应的字符的二进制码的末位数字的第一逻辑运算，并且根据运算结果在该字符后面增补空格，所增补空格的数量与该运算结果相对应；以及，所述提取模块还用于：去除所述转换的信息文本中包括所选择文本段的部分的增补空格，然后根据相应字符后面被去除的增补空格的数量，将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算，得到N个运算结果，根据所述运算结果组成的二进制序列得到所述调用者的唯一序号。

[0016] 可选地，所述第一逻辑运算为异或运算，并且，根据运算结果在该字符后面增补空格，包括：当所述字符非空格时，如果运算结果为0，则在该字符后面生成0个增补空格；如果运算结果为1，则在该字符后面生成1个增补空格；当所述字符是空格时，如果运算结果为0，则在该字符后面生成1个增补空格；如果运算结果为1，则在该字符后面生成2个增补空格。

[0017] 可选地，所述第二逻辑运算为异或运算，并且，根据相应字符后面被去除的增补空格的数量，将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算，包括：当该字符非空格时，如果去除的增补空格的数量为0，则将该字符的二进制码的末位数字与0进行异或运算；如果去除的增补空格的数量为1，将该字符的二进制码的末位数字与1进行异或运算；当该字符是空格时，如果去除的增补空格的数量为1，则将该字符的二进制码的

末位数字与0进行异或运算;如果去除的增补空格的数量为2,则将该字符的二进制码的末位数字与1进行异或运算。

[0018] 可选地,所述装置还包括处理模块:所述处理模块用于对所述信息文本执行去空格处理,以使所述信息文本的非空格字符之间最多包含一个空格。

[0019] 根据本发明的技术方案,接收调用者对敏感信息的调用请求,该调用请求具有该调用者的身份认证数据,根据身份认证数据验证调用者的权限,当调用者具备相应的权限时,产生该调用者的唯一序号,并确定调用请求所请求的信息文本,转换信息文本,使得把唯一序号以密文的形式包含在经转换的信息文本中而不影响信息文本的阅读,然后返回转换的信息文本给调用者,其中,在转换的信息文本能够提取相应调用者的唯一序号。使用本发明的技术方案,能够近乎零影响地在敏感信息中加入调用者的相关信息,在不影响敏感信息阅读的情况下,可以跟踪到相关人员对敏感信息的调用情况,使得当有调用者泄漏敏感信息时可以跟踪泄密来源。

附图说明

[0020] 附图用于更好地理解本发明,不构成对本发明的不当限定。其中:

[0021] 图1是根据本发明实施例的敏感信息提供和跟踪方法的主要步骤示意图;

[0022] 图2是根据本发明实施例的敏感信息提供和跟踪方法的优选流程示意图;

[0023] 图3是根据本发明实施例的敏感信息提供和跟踪装置的主要模块示意图;

[0024] 图4是根据本发明实施例的敏感信息提供和跟踪的优选系统架构示意图。

具体实施方式

[0025] 以下结合附图对本发明的示范性实施例做出说明,其中包括本发明实施例的各种细节以助于理解,应当将它们认为仅仅是示范性的。因此,本领域普通技术人员应当认识到,可以对这里描述的实施例做出各种改变和修改,而不会背离本发明的范围和精神。同样,为了清楚和简明,以下的描述中省略了对公知功能和结构的描述。

[0026] 图1是根据本发明实施例的敏感信息提供和跟踪方法的主要步骤示意图。

[0027] 本发明实施例的敏感信息提供和跟踪方法主要包括如下的步骤S11至步骤S14。

[0028] 步骤S11:接收调用者对敏感信息的调用请求。

[0029] 其中,该调用请求具有该调用者的身份认证数据。

[0030] 步骤S12:根据身份认证数据验证调用者的权限,当调用者具备相应的权限时,产生该调用者的唯一序号,并确定调用请求所请求的信息文本。

[0031] 其中,唯一序号的二进制码的长度是N,且N是正整数。

[0032] 确定调用请求所请求的信息文本的步骤之后,还可以对信息文本执行去空格处理,以使信息文本的非空格字符之间最多包含一个空格。

[0033] 步骤S13:转换信息文本,使得把唯一序号以密文的形式包含在经转换的信息文本中而不影响信息文本的阅读。

[0034] 其中,转换信息文本主要包括:

[0035] 选择信息文本的文本段,该文本段包括连续N个字符,使得按顺序唯一序号的二进制码的每位二进制数对应该文本段的一个字符,对唯一序号的二进制码的每位二进制数,

执行该二进制数与对应的字符的二进制码的末位数字的第一逻辑运算，并且根据该第一逻辑运算的运算结果在该字符后面增补空格，所增补空格的数量与该运算结果相对应。

[0036] 其中第一逻辑运算可以为异或运算，根据该第一逻辑运算的运算结果在该字符后面增补空格，具体可以包括：

[0037] 当字符非空格时，

[0038] 如果运算结果为0，则在该字符后面生成0个增补空格；

[0039] 如果运算结果为1，则在该字符后面生成1个增补空格；

[0040] 当字符为空格时，

[0041] 如果运算结果为0，则在该字符后面生成1个增补空格；

[0042] 如果运算结果为1，则在该字符后面生成2个增补空格。

[0043] 文本段中的每个字符的二进制码可以为该字符的UTF8编码所对应的二进制码。UTF-8(8-bit Unicode Transformation Format)编码是一种针对Unicode的可变长度字符编码，又称万国码。其由Ken Thompson于1992年创建。现在已经标准化为RFC3629。UTF-8用1到4个字节编码UNICODE字符，应用在网页上可以在同一页面显示中文简体、繁体及其它语言(如英文，日文，韩文等)。

[0044] 步骤S14：返回转换的信息文本给调用者，其中，在转换的信息文本能够提取相应调用者的唯一序号。

[0045] 提取相应调用者的唯一序号主要包括：

[0046] 去除转换的信息文本中包括所选择文本段的部分的增补空格，然后根据相应字符后面被去除的增补空格的数量，将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算，得到该第二逻辑运算的N个运算结果，并根据这些运算结果组成的二进制序列得到调用者的唯一序号。

[0047] 其中第二逻辑运算可以为异或运算，并且，根据相应字符后面被去除的增补空格的数量，将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算，具体可以包括：

[0048] 当该字符非空格时，

[0049] 如果去除的增补空格的数量为0，则将该字符的二进制码的末位数字与0进行异或运算；

[0050] 如果去除的增补空格的数量为1，将该字符的二进制码的末位数字与1进行异或运算；

[0051] 当该字符为空格时，

[0052] 如果去除的增补空格的数量为1，则将该字符的二进制码的末位数字与0进行异或运算；

[0053] 如果去除的增补空格的数量为2，则将该字符的二进制码的末位数字与1进行异或运算。

[0054] 图2是根据本发明实施例的敏感信息提供和跟踪方法的优选流程示意图。

[0055] 本发明实施例的敏感信息提供和跟踪方法的优选流程包括如下的步骤S21至步骤S28。

[0056] 步骤S21：接收调用者对敏感信息的调用请求。

[0057] 其中，调用者可以通过相应地信息调用接口发起对敏感信息的调用请求，该调用请求可以为Json格式的报文的形式。并且，调用请求中包括身份认证数据和敏感信息ID(标识)。身份认证数据例如包括调用者的身份ID等。敏感信息ID可以为敏感信息存储在数据库中时被赋予的编码，通过该编码可以查找到该敏感信息对应的文本。

[0058] 步骤S22：提取调用请求中的身份认证数据和敏感信息ID，并根据身份认证数据发起权限验证请求。

[0059] 权限验证请求中包含该调用者的身份认证数据。

[0060] 步骤S23：根据身份认证数据验证调用者的权限，如果调用者具备相应的权限，则执行步骤S24，否则执行步骤S25。

[0061] 验证调用者的权限主要是验证该调用者是否具备调用敏感信息的权限，例如验证调用者的身份ID是否合法，对于企业(如电商企业)，合法的调用者通常为该企业的内部员工。

[0062] 步骤S24：获取调用者请求的信息文本，产生调用者的唯一序号，并发起信息转换请求。

[0063] 其中，当调用者具备相应的权限时，从存储敏感信息的数据库中获取敏感信息ID对应的信息文本，并产生调用者的唯一序号，然后发起信息转换请求并执行步骤S26，其中，信息转换请求中包含敏感信息ID对应的信息文本以及调用者的唯一序号。

[0064] 调用者的唯一序号在数据库中生成，并且唯一序号的二进制数表示的长度是N，且N是正整数。对于企业来讲，唯一序号可以为调用企业敏感信息的企业内部员工的序号，其数值不超过该企业员工的总数量。例如电商企业，通常员工数量不超过百万数量级，因此序号范围可以在000000-999999。十进制数999999转换为二进制数，表示为11110100001000111111，共20位。因此N通常可以不超过20。

[0065] 步骤S25：返回错误信息，以拒绝调用者调用该敏感信息。

[0066] 步骤S26：根据唯一序号转换信息文本，使得唯一序号以增补空格的形式包含在经转换的信息文本中。

[0067] 以生成的唯一序号为999999为例，首先将该十进制表示的唯一序号转换为20位的二进制数表示形式：11110100001000111111，并将该二进制数表示存储在数组a[n]中，即a[n]＝{11110100001000111111}。然后，将敏感信息ID对应的信息文本存储在一个数组b[m]中，其中每个数组元素为一个字符，字符可以为非空格(如字母(例如英文字母、汉字)、数字、特殊符号等)，也可以为空格。每个字符可转化为UTF8编码表示，并且每个UTF8编码表示有其对应的一串二进制码。通常情况下，信息文本包含的字符个数M大于20，即：数组b[m]的元素个数通常大于数组a[n]的元素个数。那么，可从信息文本的M个字符中选择连续的20个字符，将该20个字符按照字符顺序依次对应唯一序号“999999”的二进制数表示“11110100001000111111”中的每一位二进制数，并对每位二进制数，执行该二进制数与对应的字符的二进制码的末位数字的异或运算。其中，从信息文本选取连续的20个字符时，可以从信息文本的起始位置选取，也可以从该信息文本其他任何位置选取。以从信息文本起始位置选取为例，假设信息文本起始位置包含“严”、“格”、“控”、“制”等20个字符，且对应数组b[m]中，b[0]＝“严”，b[1]＝“格”，、b[2]＝“控”、b[3]＝“制”，则将数组a[n]中的每一位二进制数分别与“严”、“格”、“控”、“制”等20个字符的二进制码的末位数字进行异或运算，

例如，字符“严”的UTF8编码表示为&#x4E25，转换为二进制码为11100100 1011100010100101，那么执行上述异或运算时，将a[0]＝1与字符“严”的二进制码的末位数字1进行异或运算，相应地，将a[1]＝1与字符“格”的二进制码的末位数字进行异或运算，将a[2]＝1与字符“控”的二进制码的末位数字进行异或运算，将a[3]＝1与字符“制”的二进制码的末位数字进行异或运算，以此类推，直到完成a[n]中20个二进制数与各自对应的20个字符的二进制码的末位数字之间的异或运算。根据各异或运算结果在相应的字符后面增补空格，所增补空格的数量与各异或运算结果相对应，具体地，当字符非空格时，如果异或结果为0，则在该字符后面生成0个增补空格，如果异或结果为1，则在该字符后面生成1个增补空格。当字符为空格时，如果异或结果为0，则在该字符后面生成1个增补空格，如果异或结果为1，则在该字符后面生成2个增补空格。例如，a[0]＝1与字符“严”的二进制码的末位数字1进行异或运算，异或结果为0，则在该字符“严”后面生成0个增补空格，即不增补空格。

[0068] 需要说明地是，从信息文本的M个字符中选择连续的20个字符中，非空格字符之间最多包含一个空格。如果从数据库中获取的信息文本中包含连续的两个或两个以上的空格，则首先对信息文本执行去空格处理，以使信息文本的非空格字符之间最多包含一个空格。

[0069] 步骤S27：将转换后的信息文本返回给调用者。

[0070] 完成信息文本的转换之后记录相关日志，然后将转换后的信息文本以Json报文的形式返回给调用者以便展示。

[0071] 步骤S28：从返回给调用者的信息文本中提取调用者的唯一序号。

[0072] 由于转换后的信息文本中的增补空格是根据调用者的唯一序号的二进制数表示的每位二进制数与对应的字符的二进制码的末位数字之间执行异或运算而生成的，且在各字符后面生成的增补空格的数量与异或运算结果相关，因此，根据经转换的信息文本中增补空格的数量以及已知的相应字符的二进制码，可以通过上述转换处理的逆向处理来还原调用者的唯一序号。例如，假设经转换的信息文本中，第一个字符后面为一个增补空格，并且该字符非空格，则表示调用者的唯一序号的二进制数表示中第一个二进制数与该字符的二进制码的末位数字异或结果为1，即上述末位数字与上述第一个二进制数不同，那么，根据任何二进制数与1异或，结果都是与该二进制数相反的二进制数的原理，将该字符的二进制码的末位数字与1异或，得出的异或结果即为调用者的唯一序号的二进制数表示中第一个二进制数的具体数值，以此类推，可以确定调用者的唯一序号的二进制数表示中每位二进制数的具体数值，从而还原出调用者的唯一序号。

[0073] 下面介绍提取调用者的唯一序号的具体方法。首先，获取返回给调用者的信息文本(即经转换的信息文本)，去除经转换的信息文本中的增补空格，其中，如果经转换的信息文本中非空格字符后面为一个空格，则该空格被识别为增补空格，如果经转换的信息文本中包含两个或三个连续的空格，则其中第一个空格被识别为转换之前信息文本原文中包含的空格，另外的一个或两个空格被识别为增补空格。

[0074] 然后，根据相应字符后面被去除的增补空格的数量，将这些字符的二进制码的末位数字与预设二进制数字执行异或运算。具体地，可预先从经转换的信息文本中选取包含所有增补空格的文本段，并将该文本段按照字符存储在数组b[p](0＝<p＝<59)中，将该文本段去除增补空格之后的字符顺序存储在数组c[q](0＝<q＝<19)中，假设调用者的唯一序

号的二进制数表示存储在数组a[20]中，遍历数组b[p](0＝<p＝<59)，其中：

[0075] 当b[0]非空格时，

[0076] 如果b[1]不为空格，则将b[0]对应的c[0]用UTF8编码表示，并将该UTF8编码的二进制码的末位数字与0进行异或，结果为0时，则a[0]为0，结果为1时，则a[0]为1；

[0077] 如果b[1]为空格，则将b[0]对应的c[0]用UTF8编码表示，并将该UTF8编码的二进制码的末位数字与1进行异或，结果为0时，则a[0]为0，结果为1时，则a[0]为1；

[0078] 当b[0]为空格时，

[0079] 如果b[1]为空格而b[2]非空格，则将b[0]对应的c[0]用UTF8编码表示，并将该UTF8编码的二进制码的末位数字与0进行异或，结果为0时，则a[0]为0，结果为1时，则a[0]为1；

[0080] 如果b[1]和b[2]均为空格，则将b[0]对应的c[0]用UTF8编码表示，并将该UTF8编码的二进制码的末位数字与1进行异或，结果为0时，则a[0]为0，结果为1时，则a[0]为1；

[0081] 当k＝59或q＝19时，整个循环结束，并得到20个异或运算的结果(即数组a[20]中20个数组元素a[0]～a[19])，该数组a[20]中存储的20位数组元素构成的二进制序列即为调用者的唯一序号。

[0082] 根据实际应用的需要，可以在执行完步骤S27之后立即执行该步骤S28，以跟踪调用者对信息的调用情况，也可以在达到特定条件时执行该步骤S28，特定条件例如调用者泄漏了转换后的信息文本的情况。当调用者泄漏了转换后的信息文本时，若该转换后的信息文本未经去空格等处理，通过执行步骤S28可以有效地追踪到泄密者的身份，从而准确地确定敏感信息的泄密源，使得对企业内部员工造成一定的威慑力，有效地遏制内部员工将企业敏感信息外泄。

[0083] 图3是根据本发明实施例的敏感信息提供和跟踪装置的主要模块示意图。

[0084] 如图3所示，本发明实施例的敏感信息提供和跟踪装置30主要包括：接收模块31、验证模块32、转换模块33、返回模块34、提取模块35。

[0085] 其中，接收模块31用于接收调用者对敏感信息的调用请求，该调用请求具有该调用者的身份认证数据；验证模块32用于根据身份认证数据验证调用者的权限，当调用者具备相应的权限时，产生该调用者的唯一序号，并确定调用请求所请求的信息文本；转换模块33用于转换信息文本，使得把唯一序号以密文的形式包含在经转换的信息文本中而不影响信息文本的阅读；返回模块34用于返回转换的信息文本给调用者；提取模块35用于在转换的信息文本提取相应调用者的唯一序号。

[0086] 身份认证数据例如调用者的身份ID，接收模块31在接收到调用者对敏感信息的调用请求之后，根据该调用请求中的身份认证数据向验证模块32发起权限验证的请求，并且该请求可以Json的格式报文发送，其中包含有该调用者的身份认证数据。

[0087] 调用者的唯一序号的二进制数表示的长度是N，并且N是正整数。

[0088] 转换模块33还可以用于：

[0089] 选择信息文本的文本段，该文本段包括连续N个字符，使得按顺序唯一序号的二进制数表示的每位二进制数对应该文本段的一个字符，对唯一序号的二进制数表示的每位二进制数，执行该二进制数与对应的字符的二进制码的末位数字的第一逻辑运算，并且根据运算结果在该字符后面增补空格，所增补空格的数量与该运算结果相对应。

[0090] 其中，文本段中每个字符的二进制码可以为该字符的UTF8编码所对应的二进制码。

[0091] 并且，第一逻辑运算可以为异或运算，根据运算结果在该字符后面增补空格，具体可以包括：

[0092] 当字符非空格时，

[0093] 如果运算结果为0，则在该字符后面生成0个增补空格；

[0094] 如果运算结果为1，则在该字符后面生成1个增补空格；

[0095] 当字符为空格时，

[0096] 如果运算结果为0，则在该字符后面生成1个增补空格；

[0097] 如果运算结果为1，则在该字符后面生成2个增补空格。

[0098] 提取模块35还可以用于：

[0099] 去除转换的信息文本中包括所选择文本段的部分的增补空格，然后根据相应字符后面被去除的增补空格的数量，将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算，得到N个运算结果，根据运算结果组成的二进制序列得到调用者的唯一序号。

[0100] 并且，第二逻辑运算可以为异或运算，并且，根据相应字符后面被去除的增补空格的数量，将这些字符的二进制码的末位数字与预设二进制数字执行第二逻辑运算，具体可以包括：

[0101] 当该字符非空格时，

[0102] 如果去除的增补空格的数量为0，则将该字符的二进制码的末位数字与0进行异或运算；

[0103] 如果去除的增补空格的数量为1，将该字符的二进制码的末位数字与1进行异或运算；

[0104] 当该字符为空格时，

[0105] 如果去除的增补空格的数量为1，则将该字符的二进制码的末位数字与0进行异或运算；

[0106] 如果去除的增补空格的数量为2，则将该字符的二进制码的末位数字与1进行异或运算。

[0107] 本发明实施例的敏感信息提供和跟踪装置30还可以包括处理模块，该处理模块用于对信息文本执行去空格处理，以使信息文本的非空格字符之间最多包含一个空格。

[0108] 图4是根据本发明实施例的敏感信息提供和跟踪的优选系统架构示意图。

[0109] 图4所示的系统架构中，调用者可以通过调用系统提供的信息调用接口发起对敏感信息的调用请求，该调用请求包含该调用者的身份ID和敏感信息ID，调用系统通过其中的接收模块接收该调用请求，并将调用请求以Json报文的形式发送到敏感信息系统，敏感信息系统提取调用请求中的调用者的身份ID，并以Json报文的形式向权限系统发起权限验证请求，该权限验证请求中包含该调用者的身份ID，权限系统中的验证模块验证该调用者是否具备调用敏感信息的权限，如果该验证者具备相应的权限，则根据将敏感信息ID对应的敏感信息的文本返回敏感信息系统，同时向敏感信息系统发送该调用者的唯一序号，敏感信息系统获取到敏感信息文本之后，将敏感信息文本连同该调用者的唯一序号封装在

Json报文中发送到加密系统，以进行敏感信息文本的转换。加密系统中的转换模块对信息文本进行转换，使得把唯一序号以密文的形式包含在经转换的信息文本中而不影响信息文本的阅读，然后将转换后的信息文本以Json报文的形式返回敏感信息系统，敏感信息系统在记录相关日志之后，可通过其中的返回模块将该报文返回调用系统，以便将转换后的信息文本展示给用户。在转换后的信息文本未经去空格等处理的情况下，加密系统可以对该敏感信息的调用情况进行跟踪，具体地，加密系统中的提取模块可以在转换的信息文本提取相应调用者的唯一序号。其中，在上述加密系统中，转换模块对信息文本的转换过程以及提取模块对调用者的唯一序号的提取过程已经在前文做了详细地介绍，此处不再赘述。

[0110] 图4所示的系统架构基于TCP/IP协议实现的敏感信息调用机制，并通过权限系统、加密系统、敏感信息系统、调用系统的信息和数据交互，以及对敏感信息文本的水印加密(信息转换)，并可通过加密系统反编译相关加密的文本，从而能够在不影响阅读的情况下，达到跟踪相关泄密源的效果。

[0111] 根据本发明实施例的技术方案，接收调用者对敏感信息的调用请求，该调用请求具有该调用者的身份认证数据，根据身份认证数据验证调用者的权限，当调用者具备相应的权限时，产生该调用者的唯一序号，并确定调用请求所请求的信息文本，转换信息文本，使得把唯一序号以密文的形式包含在经转换的信息文本中而不影响信息文本的阅读，然后返回转换的信息文本给调用者，其中，在转换的信息文本能够提取相应调用者的唯一序号。使用本发明实施例的技术方案，能够近乎零影响地在敏感信息中加入调用者的相关信息，在不影响敏感信息阅读的情况下，可以跟踪到相关人员对敏感信息的调用情况，使得当有调用者泄漏敏感信息时可以跟踪泄密来源。

[0112] 上述具体实施方式，并不构成对本发明保护范围的限制。本领域技术人员应该明白的是，取决于设计要求和其他因素，可以发生各种各样的修改、组合、子组合和替代。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明保护范围之内。

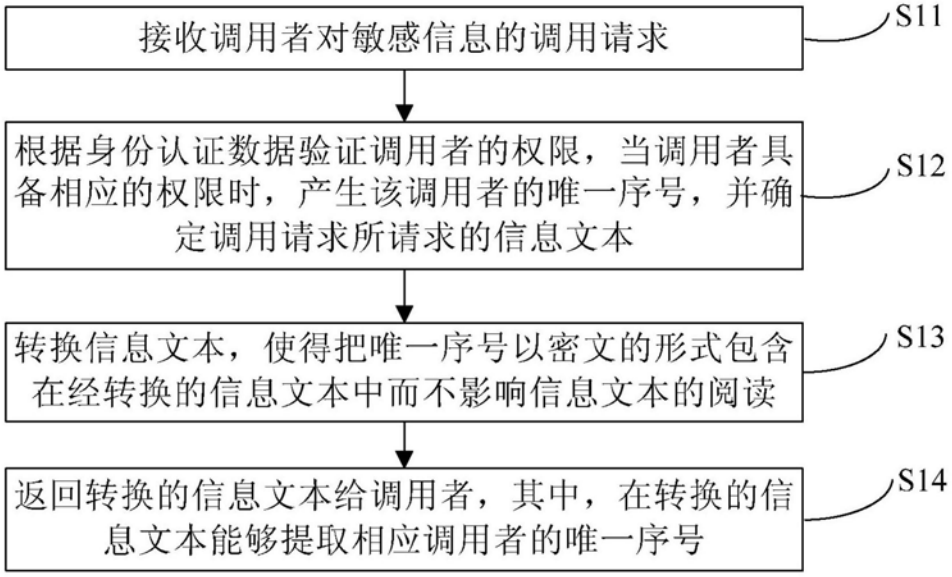

接收调用者对敏感信息的调用请求
S11
根据身份认证数据验证调用者的权限，当调用者具备相应的权限时，产生该调用者的唯一序号，并确定调用请求所请求的信息文本
S12
转换信息文本，使得把唯一序号以密文的形式包含在经转换的信息文本中而不影响信息文本的阅读
S13
返回转换的信息文本给调用者，其中，在转换的信息文本能够提取相应调用者的唯一序号
S14

图1

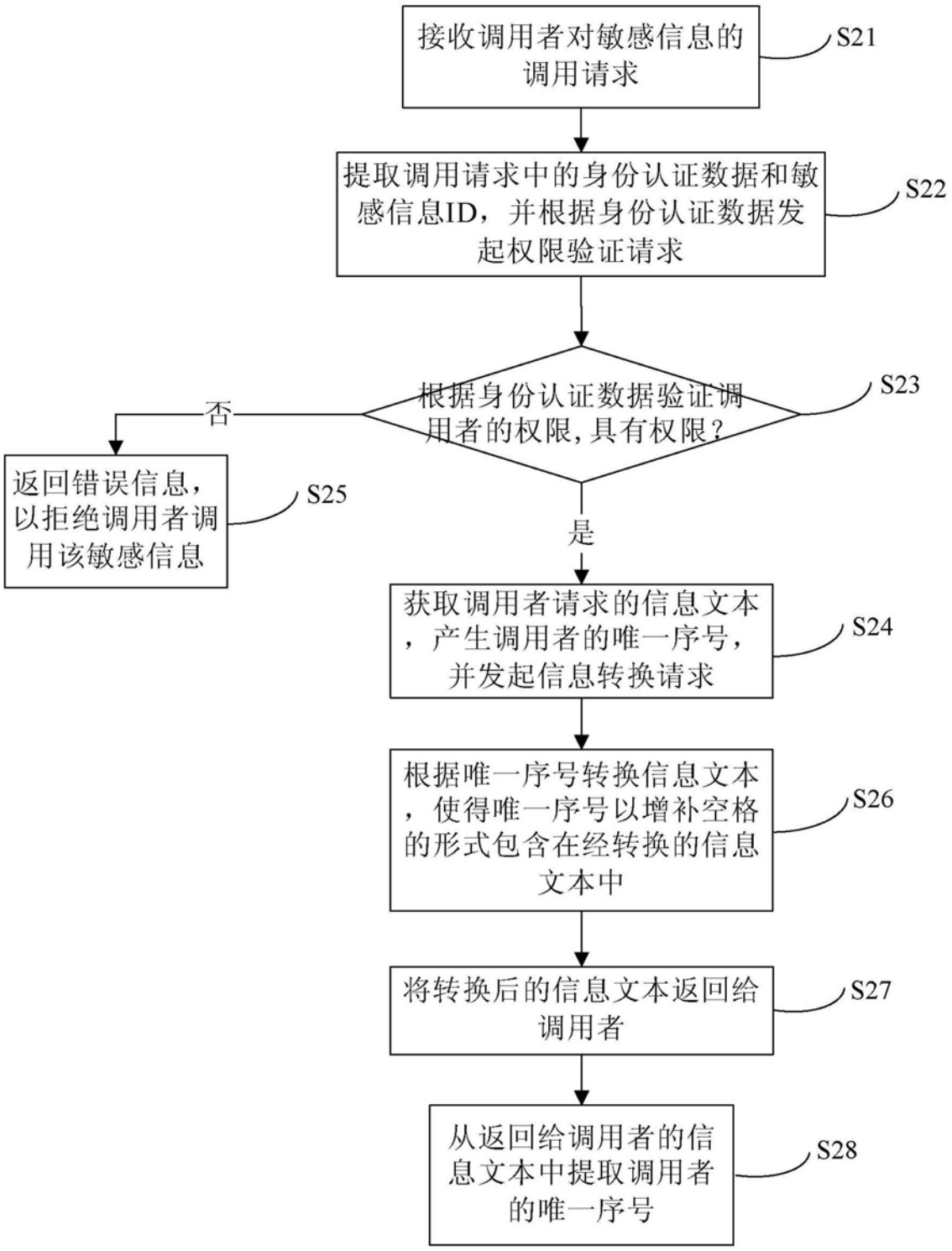

接收调用者对敏感信息的调用请求
S21
提取调用请求中的身份认证数据和敏感信息ID，并根据身份认证数据发起权限验证请求
S22
根据身份认证数据验证调用者的权限，具有权限？
S23
否
返回错误信息，以拒绝调用者调用该敏感信息
S25
是
获取调用者请求的信息文本，产生调用者的唯一序号，并发起信息转换请求
S24
根据唯一序号转换信息文本，使得唯一序号以增补空格的形式包含在经转换的信息文本中
S26
将转换后的信息文本返回给调用者
S27
从返回给调用者的信息文本中提取调用者的唯一序号
S28

图2

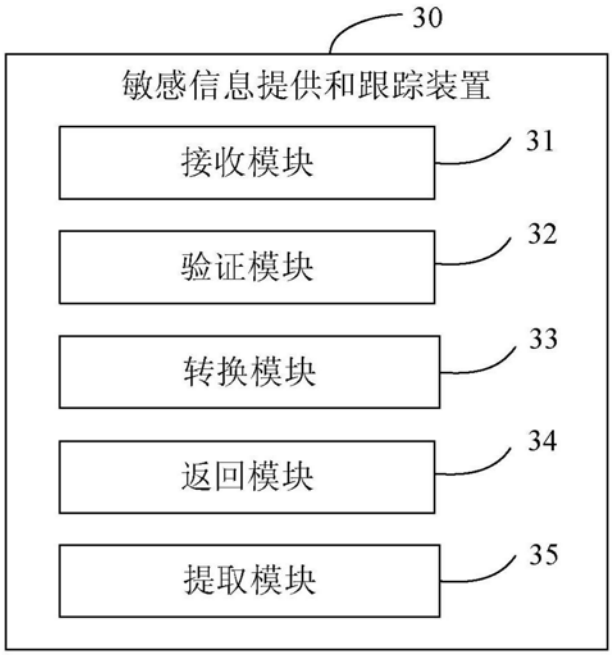

30
敏感信息提供和跟踪装置
接收模块
31
验证模块
32
转换模块
33
返回模块
34
提取模块
35

图3

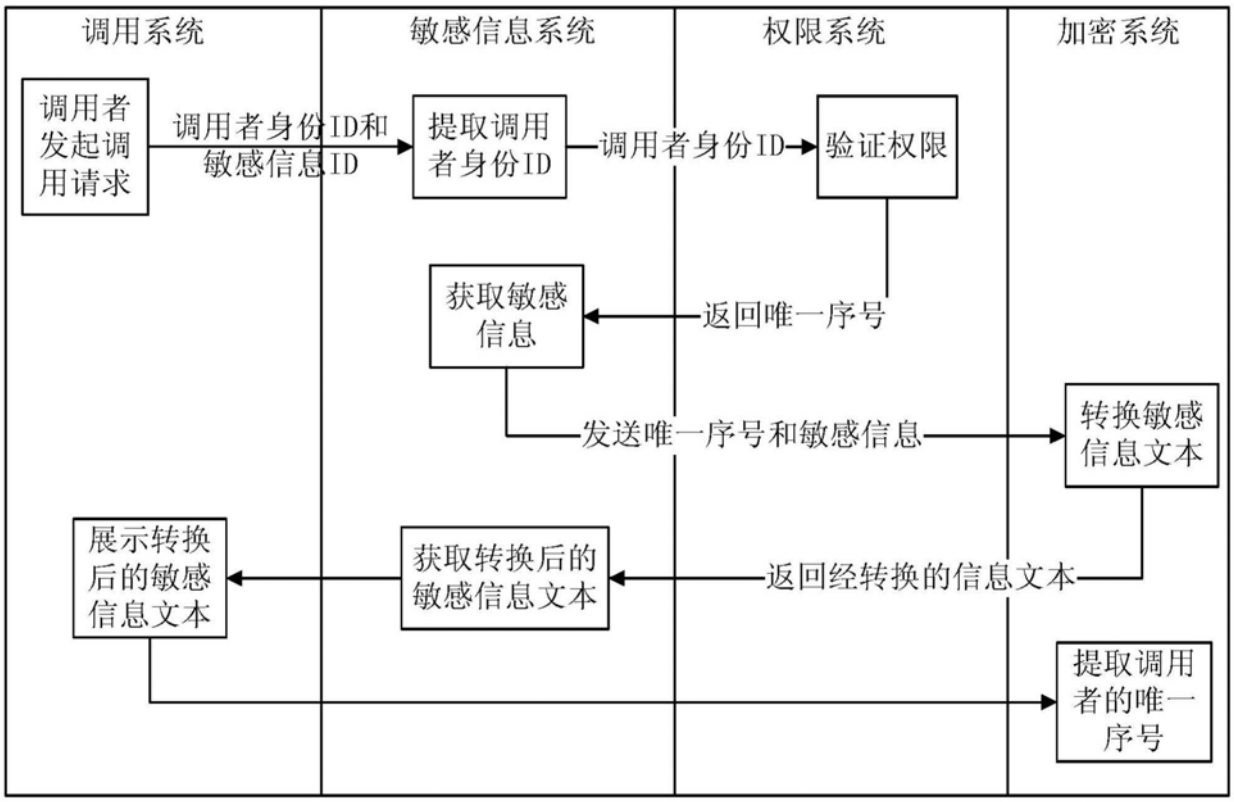

调用系统
敏感信息系统
权限系统
加密系统
调用者发起调用请求
调用者身份ID和敏感信息ID
提取调用者身份ID
调用者身份ID
验证权限
获取敏感信息
返回唯一序号
发送唯一序号和敏感信息
转换敏感信息文本
展示转换后的敏感信息文本
获取转换后的敏感信息文本
返回经转换的信息文本
提取调用者的唯一序号

图4