(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117099147 A
(43)申请公布日 2023.11.21

(21)申请号 202180096065.9
(22)申请日 2021.03.22
(85)PCT国际申请进入国家阶段日
2023.09.20
(86)PCT国际申请的申请数据
PCT/JP2021/011664 2021.03.22
(87)PCT国际申请的公布数据
WO2022/201235 JA 2022.09.29
(71)申请人 日本电信电话株式会社
地址 日本东京都
(72)发明人 高桥慧 千田浩司 市川敦谦
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 王瑞
(51)Int.Cl.
G09C 1/00(2006.01)

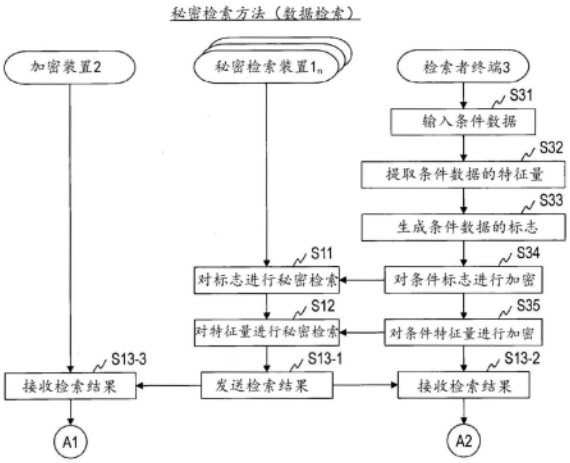
权利要求书2页 说明书9页 附图6页

(54)发明名称

秘密检索方法、秘密检索系统、秘密检索装置、加密装置、检索者终端以及程序

(57)摘要

本发明高效地进行基于秘密计算的数据检索。检索者终端(3)取得条件数据(S31)。检索者终端(3)从条件数据提取特征量(S32)。检索者终端(3)根据条件数据的特征量来生成标志(S33)。检索者终端(3)对条件数据的标志进行加密(S34)。检索者终端(3)对条件数据的特征量进行加密(S35)。秘密检索装置(1_n)在隐匿了对象标志和条件标志的状态下,取得表示与条件标志一致的对象标志对应的对象特征量的密文的中间检索结果(S11)。秘密检索装置(1_n)在隐匿了对象特征量和条件特征量的状态下,取得表示中间检索结果所表示的对象特征量中的与条件特征量类似的特征量对应的对象数据的密文的检索结果(S11)。秘密检索装置(1_n)将检索结果发送到加密装置(2)和检索者终端(3)(S13-1)。



CN 117099147 A

1.一种秘密检索方法,是由包括至少1台秘密检索装置、加密装置和检索者终端的秘密检索系统所执行的秘密检索方法,

所述加密装置的对象特征量加密部对从作为检索对象的对象数据提取到的对象特征量进行加密,

所述加密装置的对象标志加密部对表示所述对象数据的属性的对象标志进行加密,

所述检索者终端的条件特征量加密部对从作为检索条件的条件数据提取到的条件特征量进行加密,

所述检索者终端的条件标志加密部对表示所述条件数据的属性的条件标志进行加密,

所述秘密检索装置的标志检索部使用所述对象标志的密文和所述条件标志的密文,在隐匿了所述对象标志和所述条件标志的状态下,取得表示与所述条件标志一致的所述对象标志对应的所述对象特征量的密文的中间检索结果,

所述秘密检索装置的特征量检索部使用所述中间检索结果所表示的所述对象特征量的密文和所述条件特征量的密文,在隐匿了所述对象特征量和所述条件特征量的状态下,取得表示与所述条件特征量类似的所述对象特征量对应的所述对象数据的密文的检索结果。

2.如权利要求1所述的秘密检索方法,其中,

所述对象特征量的密文以及所述条件特征量的密文是通过能够进行秘密计算的第一加密方式而被加密的密文,

所述加密装置的对象数据加密部通过与所述第一加密方式不同且为了解密而需要解密密钥的第二加密方式来对所述对象数据进行加密,

所述加密装置的解密密钥发送部向所述检索者终端发送表示用于解密所述检索结果所表示的所述对象数据的密文的解密密钥的信息,

所述检索者终端的加密数据解密部使用所述解密密钥来对所述检索结果所表示的所述对象数据的密文进行解密并取得原始对象数据。

3.如权利要求1所述的秘密检索方法,其中,

所述对象数据是监视相机拍摄到的影像中包含的图像数据,

所述条件数据是特定的人物的面部被拍摄的图像数据,

所述对象标志表示所述对象数据中映现的人物的属性,

所述条件标志表示所述条件数据中映现的人物的属性。

4.一种秘密检索系统,是包括至少1台秘密检索装置、加密装置和检索者终端的秘密检索系统,

所述加密装置包括:

对象特征量加密部,对从作为检索对象的对象数据提取到的对象特征量进行加密;以及

对象标志加密部,对表示所述对象数据的属性的对象标志进行加密,

所述检索者终端包括:

条件特征量加密部,对从作为检索条件的条件数据提取到的条件特征量进行加密;以及

条件标志加密部,对表示所述条件数据的属性的条件标志进行加密,

所述秘密检索装置包括：

标志检索部，使用所述对象标志的密文和所述条件标志的密文，在隐匿了所述对象标志和所述条件标志的状态下，取得表示与所述条件标志一致的所述对象标志对应的所述对象特征量的密文的中间检索结果；以及

特征量检索部，使用所述中间检索结果所表示的所述对象特征量的密文和所述条件特征量的密文，在隐匿了所述对象特征量和所述条件特征量的状态下，取得表示与所述条件特征量类似的所述对象特征量对应的所述对象数据的密文的检索结果。

5.一种秘密检索装置，是权利要求4所记载的秘密检索系统中使用的所述秘密检索装置。

6.一种加密装置，是权利要求4所记载的秘密检索系统中使用的所述加密装置。

7.一种检索者终端，是权利要求4所记载的秘密检索系统中使用的所述检索者终端。

8.一种程序，用于使计算机执行权利要求1至权利要求3中任一项所记载的秘密检索方法的各步骤。

秘密检索方法、秘密检索系统、秘密检索装置、加密装置、检索者终端以及程序

技术领域

[0001] 本发明涉及秘密计算技术,尤其涉及在隐匿了检索对象的数据的状态下检索与检索条件的数据类似的数据的技术。

背景技术

[0002] 近年来,监视相机和IoT(物联网(Internet of Things))技术正在普及,例如监视相机影像这样的个人的隐私数据正在被大量地积蓄。通过应用图像检索技术,能够从积蓄的监视相机影像中提取与作为检索条件而被输入的图像数据类似的图像数据。这样的技术期待在对设施的进出管理、在发生了事件或事故的情况下向调查机关的信息提供等各种各样的领域的活用。然而,检索对象的图像数据是个人的生活数据本身,需要被恰当地管理以不发生隐私数据的泄露。

[0003] 设想上述这样的利用方式,作为在确保数据的机密性的同时进行检索的技术,考虑应用秘密计算技术。此外,在专利文献1中,公开了如下的技术:通过将从监视相机影像等提取到的访问者的特征部分进行秘密共享等来进行隐匿化,对隐匿化后的信息进行检索,由此来进行访问者的人物对照。

[0004] 现有技术文献

[0005] 专利文献

[0006] 专利文献1:日本特开2016-71639号公报

发明内容

[0007] 发明要解决的课题

[0008] 然而,在应用秘密计算技术的情况下,直接输入图像数据并通过秘密计算来进行检索需要庞大的计算成本,是不现实的。在专利文献1中记载的现有技术中,在对图像数据进行特征量变化的基础上通过秘密计算进行检索,因此与单纯地对图像数据进行秘密检索相比是高效的。然而,对作为检索对象的全部特征量进行秘密检索,因此根据秘密计算的算法,处理时间对于检索对象的数据件数呈指数函数地增大。

[0009] 鉴于上述这样的技术性课题,本发明的目的在于高效地进行基于秘密计算的数据检索。

[0010] 用于解决课题的手段

[0011] 本发明的一个方式的秘密检索方法由包括至少1台秘密检索装置、加密装置和检索者终端的秘密检索系统所执行的秘密检索方法,加密装置的对象特征量加密部对从作为检索对象的对象数据提取到的对象特征量进行加密,加密装置的对象标志加密部对表示对象数据的属性的对象标志进行加密,检索者终端的条件特征量加密部对从作为检索条件的条件数据提取到的条件特征量进行加密,检索者终端的条件标志加密部对表示条件数据的属性的条件标志进行加密,秘密检索装置的标志检索部使用对象标志的密文和条件标志的

密文,在隐匿了对象标志和条件标志的状态下,取得表示与条件标志一致的对象标志对应的对象特征量的密文的中间检索结果,秘密检索装置的特征量检索部使用中间检索结果所表示的对象特征量的密文和条件特征量的密文,在隐匿了对象特征量和条件特征量的状态下,取得表示与条件特征量类似的对象特征量对应的对象数据的密文的检索结果。

[0012] 发明效果

[0013] 根据本发明,能够高效地进行基于秘密计算的数据检索。

附图说明

[0014] 图1是例示秘密检索系统的功能结构的图。

[0015] 图2是例示秘密检索装置的功能结构的图。

[0016] 图3是例示加密装置的功能结构的图。

[0017] 图4是例示检索者终端的功能结构的图。

[0018] 图5是例示秘密检索方法(数据注册)的处理过程的图。

[0019] 图6是例示秘密检索方法(数据检索)的处理过程的图。

[0020] 图7是例示秘密检索方法(数据检索)的处理过程的图。

[0021] 图8是例示计算机的功能结构的图。

具体实施方式

[0022] 本发明为了实现将机密性高的数据作为对象的安全的检索系统,应用秘密计算技术。为了即使在使用计算成本大的秘密计算的情况下也高效地进行检索,构成为在检索系统的外部(例如,如果作为检索对象的原始数据是监视相机影像,则是监视相机自身或者在监视相机和检索系统之间设置的中间服务器),事先根据原始数据生成表示特征量和原始数据的属性的标志,对该特征量和标志进行加密并注册到检索系统。检索系统首先利用标志的密文通过秘密计算筛选对象数据,利用被筛选的对象数据的特征量的密文进行基于秘密计算的数据检索。在利用了特征量的数据检索中需要计算特征量间的类似度,但利用了标志的筛选仅进行值的比较。因此,如果最初利用标志进行对象数据的筛选,能够降低数据检索整体的处理成本。例如,如果根据检索对象的数据和检索条件的数据分别生成表示拍摄到的人物的性别的标志,在进行了基于性别的筛选的基础上进行使用了特征量的检索,则能够将处理成本降低大约50%。

[0023] 以下,对本发明的实施方式详细地进行说明。另外,在附图中,对具有相同的功能的结构部赋予相同的序号,并省略重复说明。

[0024] [实施方式]

[0025] 本发明的实施方式是在将各数据进行隐匿的状态下,通过秘密计算从作为检索对象而被积蓄的数据中检索与作为条件被输入的数据类似的数据的秘密检索系统以及方法。在本实施方式中,设想如下的利用方式:将由监视相机拍摄到的监视相机影像中包含的图像数据作为检索对象,将特定的人物所映现的图像数据作为检索条件,将作为检索对象而被积蓄的图像数据中的、检索条件的图像数据中映现的人物所映入的图像作为检索结果输出。其中,在本发明中,作为检索对象的数据不限定于图像数据。例如,如果是声音数据或文本数据等能够提取某种特征量的数据,则无论是何种数据都能够作为检索对象。

[0026] 如图1所示,实施方式的秘密检索系统100包含N(≥1)台秘密检索装置$1_1,\cdots,1_N$、加密装置2、检索者终端3、以及存储装置4。加密装置2以及检索者终端3也可以分别被包含多台。C(≥1)台监视相机$5_1,\cdots,5_C$通过有线或者无线接口连接到加密装置2。在包含多台加密装置2的情况下,与各加密装置2连接的监视相机5_c(c∈=1,…,C)的台数C也可以互相不同。通过将存储装置4应具备的功能安装在秘密检索装置$1_1,\cdots,1_N$的任一个中,存储装置4能够省略。

[0027] 秘密检索装置$1_1,\cdots,1_N$、加密装置2、检索者终端3、以及存储装置4分别连接到通信网9。通信网9是构成为所连接的各装置能够相互通信的线路蒋欢方式或者分组交换方式的通信网,例如能够使用互联网或LAN(局域网(Local Area Network))、WAN(广域网(Wide Area Network))等。

[0028] 在秘密检索装置1_n(n∈{1,…,N})是多台的情况(即,N≥2的情况)下,秘密检索装置1_n例如使用基于沙米尔秘密共享或复制秘密共享等的秘密共享的秘密计算方式来与其他秘密检索装置$1_{n'}$(n'∈{1,…,N}且n≠n')协作地进行检索。在秘密检索装置1_n是1台的情况(即,N=1的情况)下,秘密检索装置1_n例如使用基于同态加密等的加密的秘密计算方式来执行检索。

[0029] 如图2所示,秘密检索装置1_n(n=1,…,N)例如具备加密标志存储部10-1、加密特征量存储部10-2、标志检索部11、特征量检索部12、以及检索结果发送部13。如图3所示,加密装置2例如具备:解密密钥存储部20、对象数据取得部21、对象特征量提取部22、对象标志生成部23、对象标志加密部24、对象特征量加密部25、对象数据加密部26、以及解密密钥发送部27。如图4所示,检索者终端3例如具备条件数据输入部31、条件特征量提取部32、条件标志生成部33、条件标志加密部34、条件特征量加密部35、加密数据取得部36、以及加密数据解密部37。

[0030] 秘密检索系统100中包含的秘密检索装置$1_1,\cdots,1_N$、加密装置2、检索者终端3、以及存储装置4互相协作,并进行图5-7所示的各步骤的处理,由此实现实施方式的秘密检索方法。实施方式的秘密检索方法由将作为检索对象的数据注册到秘密检索系统100的数据注册处理、和通过秘密计算检索作为检索对象的数据中的与作为检索条件的数据类似的数据的数据检索处理这两个阶段构成。图5是例示数据注册处理的过程的流程图,图6-7是例示数据检索处理的过程的流程图。另外,图6所示的附加了A1、A2的圆形的块表示对图7所示的附加了A1、A2的圆形的块继续处理。

[0031] 秘密检索系统100中包含的各装置或终端例如是对具有中央运算处理装置(CPU:中央处理单元(Central Processing Unit))、主存储装置(RAM:随机存取存储器(Random Access Memory))等的公知或专用的计算机读入特别的程序而构成的特别的装置。各装置或终端例如在中央运算处理装置的控制下执行各处理。被输入到各装置或终端的数据或通过各处理得到的数据例如被储存在主存储装置中,主存储装置中储存的数据根据需要被读出到中央运算处理装置而被利用于其他处理。各装置或终端的各处理部也可以是至少一一部分由集成电路等的硬件构成。各装置或终端所具备的各存储部例如能够通过RAM(随机存取存储器(Random Access Memory))等主存储装置、由硬盘、光盘或者闪存(Flash Memory)这样的半导体存储器元件构成的辅助存储装置、或者关系数据库或键值存储器等中间件构成。

[0032] 具体地,秘密检索装置1_n以及加密装置2是塔型或机架型服务器计算机等的具备数据通信功能的信息处理装置。具体地,检索者终端3是台式或者膝上型的个人计算机或者智能手机或平板电脑这样的移动终端等的具备数据通信功能的信息处理装置。具体地,存储装置4是连接大容量存储装置的塔型或机架型的服务器计算机或者内藏大容量存储装置的网络连接储存器等的具备数据通信功能以及数据存储功能的信息处理装置。

[0033] 监视相机5_c例如是具有拍摄作为被摄体的人或物体的运动图像的摄像机的拍摄装置。例如,可拍摄的分辨率或影像的记录介质、麦克风的有无、数字模拟的区别等,监视相机5_c所应具有的功能没有限制,如果是一般的能够拍摄运动图像的拍摄装置,则能够使任意的装置。

[0034] 参考图5,对由实施方式的秘密检索系统100执行的秘密检索方法中的、数据注册时的处理过程进行说明。

[0035] 在步骤S21中,加密装置2的对象数据取得部21取得作为检索对象的数据(以下称为“对象数据”)。对象数据例如是监视相机5_c所拍摄的监视相机影像中包含的图像数据。此时,也可以对对象数据附加关于拍摄场所或拍摄日期时间等的信息的标签。对象数据取得部21将获取到的对象数据输出到对象特征量提取部22以及对象数据加密部26。

[0036] 在步骤S22中,加密装置2的对象特征量提取部22从对象数据取得部21受理对象数据,从该对象数据提取特征量(以下,称为“对象特征量”)。对象特征量提取部22将提取出的对象特征量输出到对象标志生成部23以及对象特征量加密部25。

[0037] 特征量的提取方法能够按照对象数据的种类而任意地决定。例如,在设想将对象数据作为不特定的多个人物所映入的影像中包含的图像数据、并从该对象数据检索特定的人物的面部的利用方式的情况下,通过以下的2个步骤提取特征量即可。首先,从监视相机5_c拍摄到的图像数据提取成为检索对象的区域(例如,人物的面部)(步骤1)。区域提取例如使用主成分分析等的一般的方法即可(参考参考文献1)。接着,将提取到的面部图像数据变换为特征量(步骤2)。面部图像数据的特征量变换例如可以将图像的每个像素的像素值直接作为特征量而采用,也可以使用一般的边缘提取方法,将每个像素的变化量作为特征量而采用(参考参考文献2)。

[0038] 〔参考文献1〕Mante Opel、“主成分分析を用いた顔認識”、[online]、[令和2年3月9日検索]、インターネット<URL:https://qiita.com/manteopel/ite ms/703e9946e1903c6e2aa3>

[0039] 〔参考文献2〕SUNSHINE、“「画像認識」の「特徴量」(2):「エッジ検出」とは?どんな仕組み?「空間フィルタ」とは?どう使っているの?についてまとめました”、[online]、[令和2年3月9日検索]、インターネット<URL:https://it-mint.com/2018/11/05/feature-value-in-image-recognition-whats-edge-detection-and-spatial-filter-1839.html>

[0040] 在对象数据是声音数据的情况下,提取公知的音响特征量即可。在对象数据是文本数据的情况下,提取公知的单词嵌入向量等的特征量即可。

[0041] 在步骤S23中,加密装置2的对象标志生成部23从对象特征量提取部22受理对象特征量,基于该对象特征量生成表示对象数据的属性的标志(以下,称为“对象标志”)。对象标志生成部23将生成的对象标志输出到对象标志加密部24。

[0042] 标志的生成方法能够按照对象数据的种类而任意地决定。例如,在设想将对象数

据作为不特定的多个人物所映入的影像中所包含的图像数据、并以人物的性别以及年龄段来锁定对象数据的情况下,如以下这样生成表示性别以及年龄段的属性标志即可。首先,从对象数据提取面部图像。接着,例如通过参考文献3中记载的方法,从该面部图像估计性别以及年龄。然后,将被估计的性别以及年龄变换为表示性别以及年龄段的符号(例如,如果是性别,男性为1、女性为0等。如果是年龄段,若为20岁～29岁则记为20、若为30岁～39岁则记为30、……等)。

[0043] 〔参考文献3〕和泉恭子,伊賀亮達,林尚典,深野元太郎,大谷哲也,“顔画像における複数特徴量を用いた性別・年齢推定手法”,情報処理学会第65回全国大会,2003年

[0044] 在步骤S24-1中,加密装置2的对象标志加密部24从对象标志生成部23受理对象标志,对该对象标志进行加密。对象标志加密部24使用能够进行秘密计算的任意的加密方式或者秘密共享方式,对对象标志进行加密。具体地,作为能够进行秘密计算的加密方式可举出同态加密等,作为能够进行秘密计算的秘密共享方式可举出沙米尔秘密共享、复制秘密共享等。如果是加密方式则生成的密文是1个密文,如果是秘密共享方式则生成的密文是多个份额构成的分散值。对象标志加密部24将对象标志的密文发送到各秘密检索装置1_n。这里,“将密文发送到各秘密检索装置1_n”,如果该密文是基于加密方式的密文,则意味着向1台秘密检索装置1_1发送1个密文,如果该密文是基于秘密共享方式的密文,则意味着以多台秘密检索装置$1_1,\cdots,1_N$各自不重复地保持1个份额的方式来分配分散值。在后续的说明也同样如此。

[0045] 在步骤S24-2中,各秘密检索装置1_n从加密装置2接收对象标志的密文,将该对象标志的密文存储到加密标志存储部10-1。

[0046] 在步骤S25-1中,加密装置2的对象特征量加密部25从对象特征量提取部22获取对象特征量,对该对象特征量进行加密。对象特征量加密部25所使用的加密方法与加密装置2的对象标志加密部24所使用的加密方法是同样的。对象特征量加密部25将对象特征量的密文发送到各秘密检索装置1_n。

[0047] 在步骤S25-2中,各秘密检索装置1_n从加密装置2接收对象特征量的密文,将该对象特征量的密文存储到加密特征量存储部10-2。

[0048] 在步骤S26-1中,加密装置2的对象数据加密部26从对象数据取得部21获取对象数据,对该对象数据进行加密。对象数据加密部26所使用的加密方法是与对象标志加密部24以及对象特征量加密部25所使用的加密方法不同的加密方法,是如果不使用正当的解密密钥则无法得到原始数据的加密方法。如果是这样的加密方法,则可以是公共密钥加密,也可以是公钥加密。对象数据加密部26将表示对象数据的密文的信息、和表示为了解密该对象数据的密文而所需的解密密钥的信息进行关联,并存储到解密密钥存储部20。表示解密密钥的信息可以是解密密钥本身,也可以是事先在加密装置2和检索者终端3之间以安全的方法交换的能够识别解密密钥的信息。对象数据加密部26将对象数据的密文发送到存储装置4。

[0049] 在步骤S26-2中,存储装置4从加密装置2接收对象数据的密文,存储该对象数据的密文。

[0050] 参考图6-7,对由实施方式的秘密检索系统100执行的秘密检索方法中的、数据检索时的处理过程进行说明。

[0051] 在步骤S31中,检索者终端3的条件数据输入部31取得由使用检索者终端3的检索者向检索者终端3输入的、作为检索条件的数据(以下称为“条件数据”)。条件数据例如是想检索的人物的面部被拍摄而成的图像数据。条件数据输入部31将取得到的条件数据输出到条件特征量提取部32。

[0052] 在步骤S32中,检索者终端3的条件特征量提取部32从条件数据输入部31受理条件数据,从该条件数据提取特征量(以下,称为“条件特征量”)。条件特征量提取部32所提取的特征量与加密装置2的对象特征量提取部22所提取的特征量是同样的。条件特征量提取部32将提取到的条件特征量输出到条件标志生成部33以及条件特征量加密部35。

[0053] 在步骤S33中,检索者终端3的条件标志生成部33从条件特征量提取部32受理条件特征量,基于该条件特征量生成表示条件数据的属性的标志(以下称为“条件标志”)。条件标志生成部33所使用的标志生成方法与加密装置2的对象标志生成部23所使用的标志生成方法是同样的。条件标志生成部33将所生成的条件标志输出到条件标志加密部34。

[0054] 在步骤S34中,检索者终端3的条件标志加密部34从条件标志生成部33受理条件标志,对该条件标志进行加密。条件标志加密部34所使用的加密方法与加密装置2的对象标志加密部24所使用的加密方法是同样的。条件标志加密部34将条件标志的密文发送到各秘密检索装置1_n。

[0055] 在步骤S35中,检索者终端3的条件特征量加密部35从条件特征量提取部32受理条件特征量,对该条件特征量进行加密。条件特征量加密部35所使用的加密方法与加密装置2的对象特征量加密部25所使用的加密方法是同样的。条件特征量加密部35将条件特征量的密文发送到各秘密检索装置1_n。

[0056] 在步骤S11中,各秘密检索装置1_n的标志检索部11从检索者终端3接收条件标志的密文,使用加密标志存储部10-1中存储的对象标志的密文和从检索者终端3接收到的条件标志的密文,通过秘密计算检索与条件标志一致的对象标志。即,在隐匿了对象标志和条件标志的状态下,提取与条件标志一致的对象标志的密文。标志检索部11将与被提取到的对象标志的密文对应的对象特征量的密文从加密特征量存储部10-2中读出,将表示该对象特征量的密文的信息(以下,称为“中间检索结果”)输出到特征量检索部12。

[0057] 基于秘密计算的标志检索能够在将对象标志以及条件标志储存为表形式的基础上通过能够进行秘密计算的加密方式进行加密,例如进行参考文献4中记载的秘密计算上的过滤处理(比较运算)来实现。

[0058] 〔参考文献4〕濱田浩気,五十嵐大,菊池亮,千田浩司,諸橋玄武,冨士仁,高橋克巳,“実用的な高速で統計分析が可能な秘密計算システムMEVAL,”コンピュータセキュリティシンポジウム(CSS),2013年

[0059] 在步骤S12中,各秘密检索装置1_n的特征量检索部12从标志检索部11受理中间检索结果,使用中间检索结果中包含的对象特征量的密文和从检索者终端3接收到的条件特征量的密文,通过秘密计算来检索与条件特征量类似的对象特征量。即,在隐匿了对象特征量和条件特征量的状态下,提取与条件特征量类似的对象特征量的密文。特征量检索部12将表示与被提取到的对象特征量的密文对应的对象数据的密文的信息(以下,称为“检索结果”)输出到检索结果发送部13。

[0060] 基于秘密计算的特征量检索能够通过在秘密计算的基础上,对所有的对象数据计

算与条件数据的欧几里得距离,并将该计算结果与事先设定的阈值进行比较来进行。欧几里得距离如以下这样地计算。被检索数据(对象数据)以及检索数据(条件数据)是n×m像素的图像数据。在将被检索数据的像素值(特征量)设为$x=[x_{ij}]$,将检索数据的像素值设为$y=[y_{ij}]$时(i=1,…,m、j=1,…,n),欧几里得距离D通过下面的式来表示(参照参考文献5)。

[0061] 【数式1】

[0062] $$D=\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij}-y_{ij})}$$

[0063] 〔参考文献5〕井上光平,浦浜喜一,“ユークリッド距離の下限に基づく画像のフィルタリング検索,”映像情報メディア学会誌,Vol.59,No.11,pp.1701-1704,2005年

[0064] 秘密计算上述的欧几里得距离D能够通过活用具有加法同态性的秘密计算而容易地实现。

[0065] 对于所有的对象数据计算欧几里得距离D,通过将该计算结果与规定的阈值进行比较,能够生成检索结果。例如,将欧几里得距离D为规定的阈值以下的对象数据、或者将欧几里得距离D按升序排序时的从开头起规定的件数的对象数据作为检索结果输出即可。秘密计算上的排序计算例如能够使用参考文献6中记载的方法。

[0066] 〔参考文献6〕五十嵐大,濱田浩気,菊池亮,千田浩司,“超高速秘密計算ソートの設計と実装:秘密計算がスクリプト言語に並ぶ日”,コンピュータセキュリティシンポジウム(CSS),2017年

[0067] 在步骤S13-1中,各秘密检索装置1_n的检索结果发送部13从特征量检索部12受理检索结果,将该检索结果发送到检索者终端3。此外,检索结果发送部13将该检索结果和表示检索者终端3的信息发送到加密装置2。

[0068] 在步骤S13-2中,检索者终端3从各秘密检索装置1_n接收检索结果,根据检索结果得到表示对象数据的密文的信息。在特征量检索部12通过基于秘密共享的秘密计算方式来进行检索的情况下,通过复原从各秘密检索装置1_n接收到的检索结果的份额,得到表示对象数据的密文的信息即可。在特征量检索部12通过基于加密的秘密计算方式进行了检索的情况下,通过根据规定的解密方法对从秘密检索装置11接收到的检索结果进行解密来得到表示对象数据的密文的信息即可。检索者终端3将得到的表示对象数据的密文的信息输入到加密数据取得部37。

[0069] 在步骤S13-3中,加密装置2从各秘密检索装置1_n接收检索结果和表示检索者终端3的信息,与检索者终端3同样地,根据检索结果得到表示对象数据的密文的信息。加密装置2将得到的表示对象数据的密文的信息和表示检索者终端3的信息输入到解密密钥发送部27。

[0070] 在步骤S36中,检索者终端3的加密数据取得部36从存储装置4取得被输入的信息所表示的对象数据的密文。加密数据取得部36将取得到的对象数据的密文输出到加密数据解密部37。

[0071] 在步骤S27-1中,加密装置2的解密密钥发送部27从解密密钥存储部20取得用于对被输入的信息所表示的对象数据的密文进行解密的表示解密密钥的信息。解密密钥发送部27将取得到的表示解密密钥的信息发送到检索者终端3。

[0072] 在步骤S27-2中,检索者终端3从加密装置2接收表示解密密钥的信息,取得该解密密钥。检索者终端3将取得到的解密密钥输入到加密数据解密部37。

[0073] 在步骤S37中,检索者终端3的加密数据解密部37从加密数据取得部36受理对象数据的密文,使用被输入的解密密钥来对该对象数据的密文进行解密。加密数据解密部37输出通过解密得到的原始对象数据。在对象数据取得部21对对象数据附加了拍摄场所、拍摄日期时间等的信息的情况下,将这些信息附加到原始对象数据上并输出。

[0074] 通过上述这样地构成,秘密检索装置1_1,…,1_N将作为检索对象的数据筛选为作为检索条件的数据和表示属性的标志所一致的数据的基础上,仅使用特征量来检索被筛选的作为检索对象的数据,因此能够降低基于秘密计算的数据检索的计算成本。此外,检索者终端3能够将作为检索对象的数据中的与作为检索条件的数据类似的原始数据其本身作为检索结果而取得。此时,原始数据通过如果没有解密密钥则无法解密的加密方式而被加密,因此与原始数据有关的信息能够不泄露于秘密检索装置1_1,…,1_N。从而,能够安全地向检索者终端提供原始数据作为检索结果。

[0075] [变形例]

[0076] 在实施方式的秘密检索系统中,加密装置2构成为从多台监视相机5_1,…,5_C拍摄到的图像数据分别提取特征量,对该特征量和原始图像数据进行加密存储为能够从秘密计算装置1_1,…,1_N利用。然而,通过在监视相机5_1,…,5_C本身中安装特征量提取以及加密的功能,能够省略加密装置2。在该情况下,监视相机5_1,…,5_C具备实施方式的加密装置2所具备的解密密钥存储部20、对象特征量提取部22、对象标志生成部23、对象标志加密部24、对象特征量加密部25、对象数据加密部26、以及解密密钥发送部27。即,在变形例的秘密检索系统中,监视相机5_1,…,5_C分别构成为相当于加密装置2。

[0077] 以上,对本发明的实施方式进行了说明,但具体的结构不限于这些实施方式,只要是不脱离本发明的主旨的范围内进行适当设计的变更等,当然也包含于本发明。在实施方式中说明的各种处理不仅按照记载的顺序按时间序列执行,也可以根据执行处理的装置的处理能力或需要并行地或者单独地被执行。

[0078] [程序、记录介质]

[0079] 在通过计算机来实现在上述实施方式中说明的各装置中的各种处理功能的情况下,各装置应具有的功能的处理内容通过程序来记述。而且,使该程序读入到图8所示的计算机的存储部1020,使运算处理部1010、输入部1030、输出部1040等执行操作,由此上述各装置中的各种处理功能在计算机上被实现。

[0080] 记述该处理内容的程序能够记录在计算机可读取的记录介质中。计算机可读取的记录介质例如可以是非暂时性的记录介质,磁记录装置、光盘等。

[0081] 此外,该程序的流通例如通过将记录了该程序的DVD、CD-ROM等可移动型记录介质销售、转让、借出等来进行。进而,也可以构成为将该程序事先储存于服务器计算机的存储装置,经由网络,从服务器计算机向其他计算机转发该程序,从而使该程序流通。

[0082] 执行这样的程序的计算机例如首先将可移动型记录介质中记录的程序或从服务器计算机转发的程序暂时储存到自身的非暂时性的存储装置的辅助记录部1050。而且,处理的执行时,该计算机将储存在自身的非暂时性的存储装置的辅助记录部1050中的程序读入到暂时性的存储装置即存储部1020,根据读入的程序执行处理。此外,作为该程序的其他

执行方式,也可以是计算机从可移动型记录介质中直接地读入程序,执行按照该程序的处理,进而也可以是每当从服务器计算机向该计算机转发程序时,依次执行按照获取到的程序的处理。此外,也可以构成为不进行程序从服务器计算机向该计算机的转发,而利用仅通过其执行指示和结果取得来实现处理功能的所谓ASP(应用服务提供商(Application Service Provider))型的服务,来执行上述的处理。另外,在本方式中的程序中,设为包含供电子计算机用于处理且等价于程序的信息(虽然不是对于计算机的直接的指令,但是具有对计算机的处理进行规定的性质的数据等)。

[0083] 此外,在该方式中,通过在计算机上执行规定的程序来构成本装置,但也可以通过硬件实现这些处理内容的至少一部分。

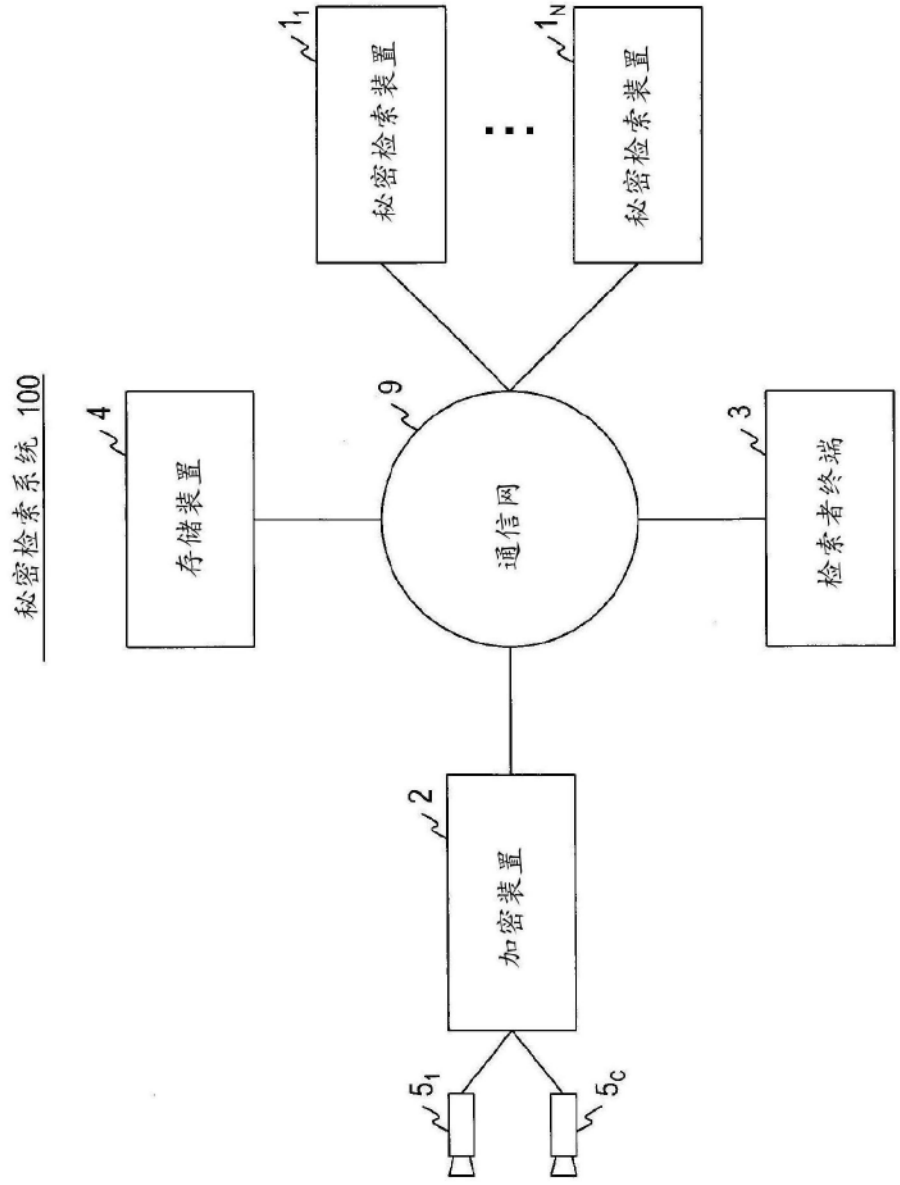


图1

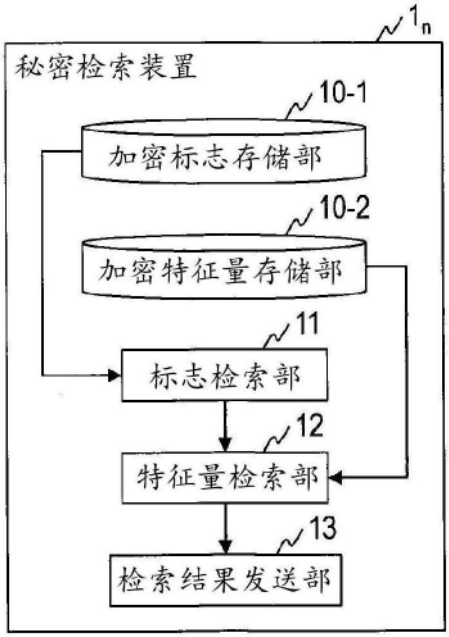

1n
秘密检索装置
10-1
加密标志存储部
10-2
加密特征量存储部
11
标志检索部
12
特征量检索部
13
检索结果发送部

图2

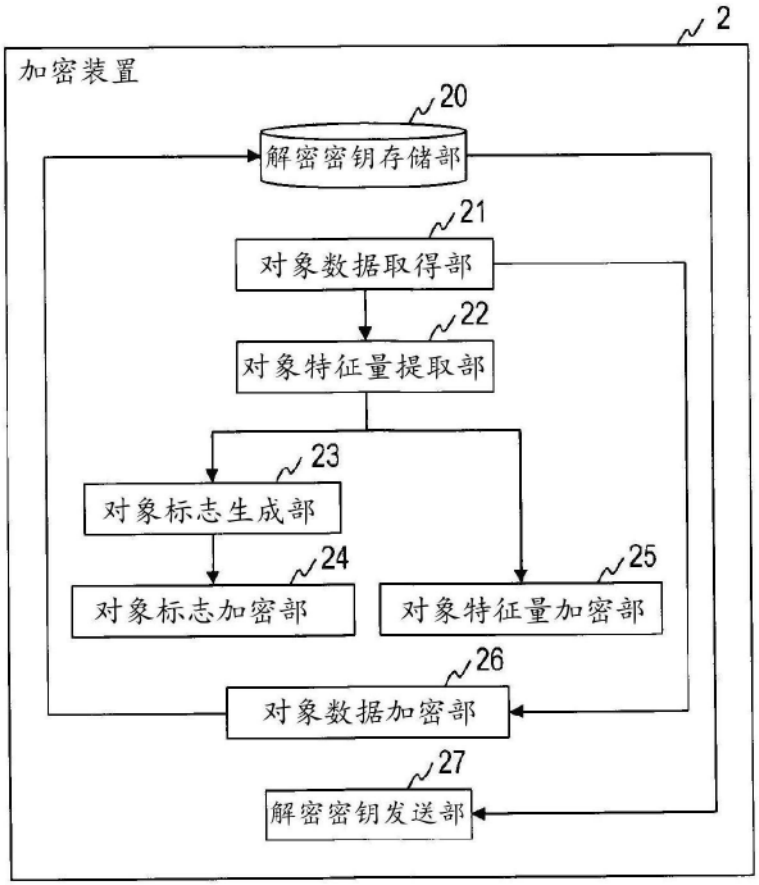

2
加密装置
20
解密密钥存储部
21
对象数据取得部
22
对象特征量提取部
23
对象标志生成部
24
对象标志加密部
25
对象特征量加密部
26
对象数据加密部
27
解密密钥发送部

图3

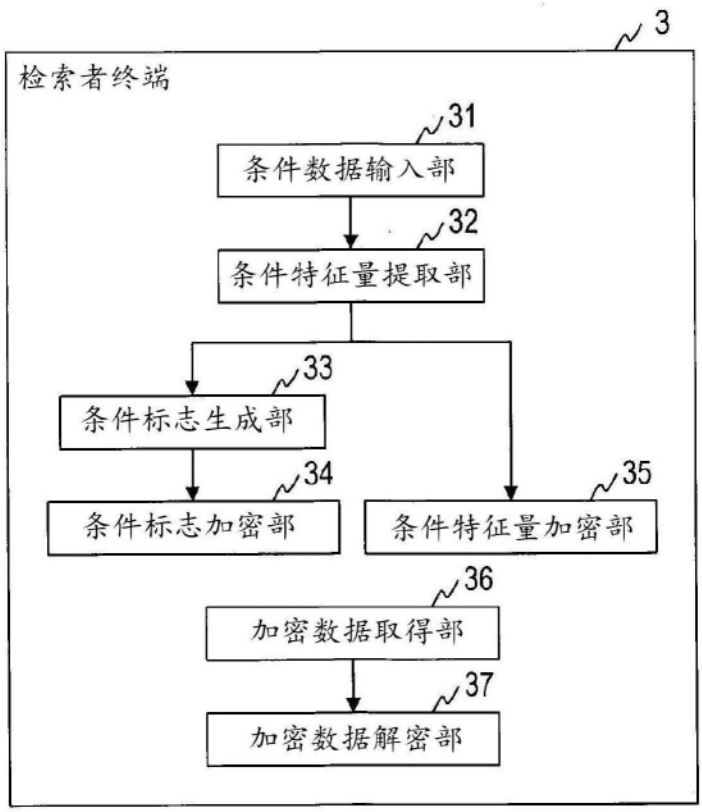

3
检索者终端
31
条件数据输入部
32
条件特征量提取部
33
条件标志生成部
34
条件标志加密部
35
条件特征量加密部
36
加密数据取得部
37
加密数据解密部

图4

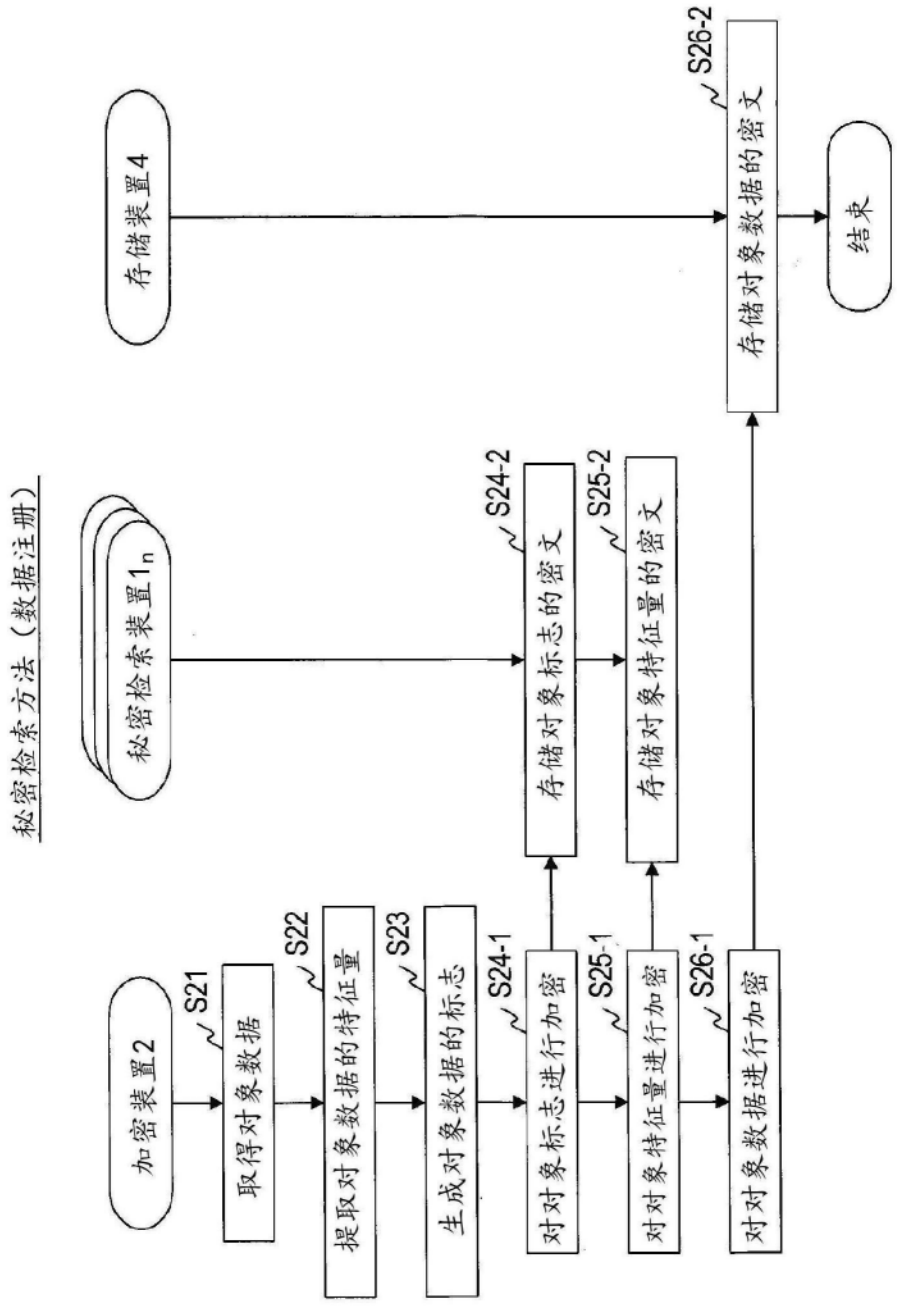

秘密检索方法（数据注册）
加密装置2
S21
取得对象数据
S22
提取对象数据的特征量
S23
生成对象数据的标志
S24-1
对对象标志进行加密
S25-1
对对象特征量进行加密
S26-1
对对象数据进行加密
秘密检索装置1n
S24-2
存储对象标志的密文
S25-2
存储对象特征量的密文
存储装置4
S26-2
存储对象数据的密文
结束

图5

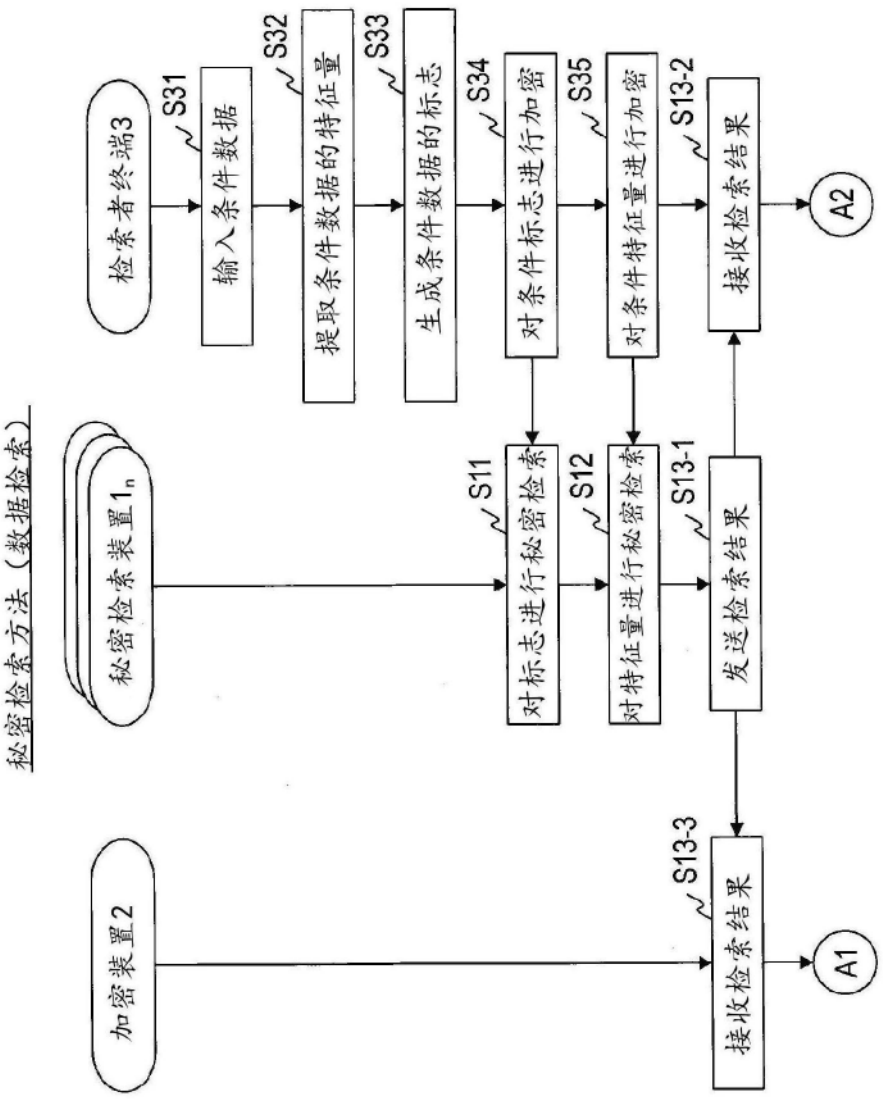

秘密检索方法（数据检索）
检索者终端3
S31
输入条件数据
S32
提取条件数据的特征量
S33
生成条件数据的标志
S34
对条件标志进行加密
S35
对条件特征量进行加密
S13-2
接收检索结果
A2
秘密检索装置1n
S11
对标志进行秘密检索
S12
对特征量进行秘密检索
S13-1
发送检索结果
加密装置2
S13-3
接收检索结果
A1

图6

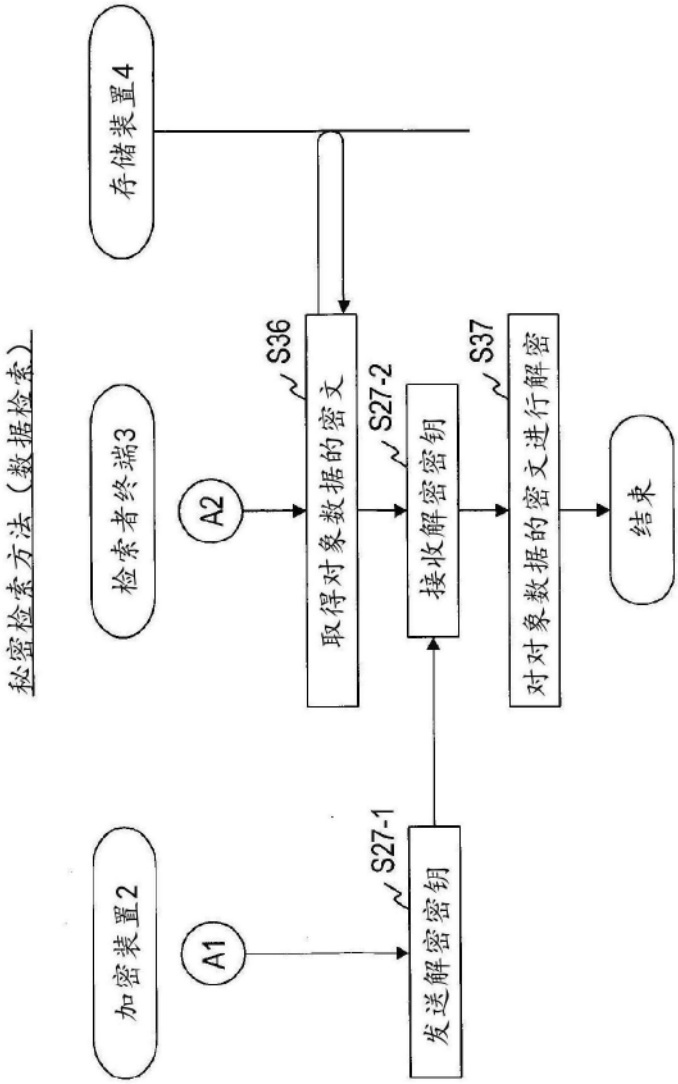

秘密检索方法（数据检索）
存储装置4
检索者终端3
加密装置2
A2
A1
S36
取得对象数据的密文
S27-2
接收解密密钥
S37
对对象数据的密文进行解密
结束
S27-1
发送解密密钥

图7

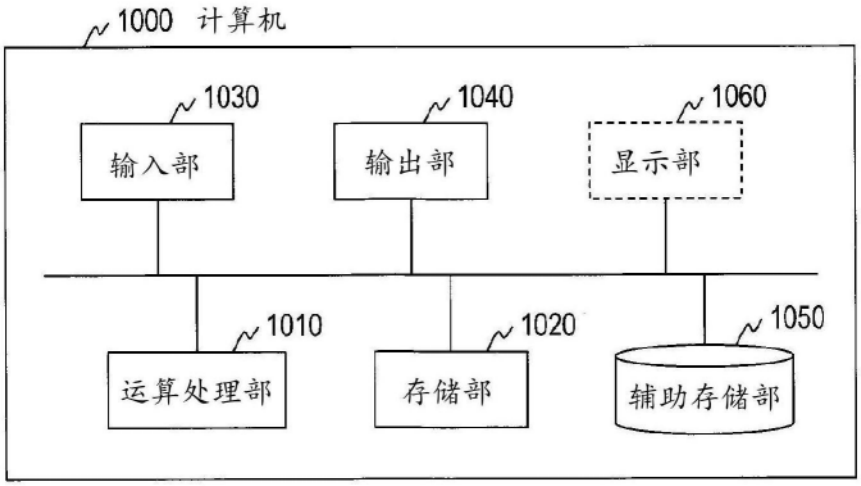

1000 计算机
1030
输入部
1040
输出部
1060
显示部
1010
运算处理部
1020
存储部
1050
辅助存储部

图8