(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 102016862 B
(45)授权公告日 2015.08.05

(21)申请号 200980115549.2
(22)申请日 2009.04.29
(30)优先权数据
0807753.9 2008.04.29 GB
(85)PCT国际申请进入国家阶段日
2010.10.29
(86)PCT国际申请的申请数据
PCT/GB2009/050438 2009.04.29
(87)PCT国际申请的公布数据
WO2009/133397 EN 2009.11.05
(73)专利权人 科里普托马迪克公司
地址 英国剑桥郡
(72)发明人 迈克尔·邦德
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王玮
(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/32(2013.01)
(56)对比文件
US 6049612 A,2000.04.11, 说明书摘要,说明书第1-7栏,附图1-6.
CN 1790359 A,2006.06.21,
JP 特开2007-65860 A,2007.03.15,
US 6577735 B1,2003.06.10, 全文.
审查员 田民丽

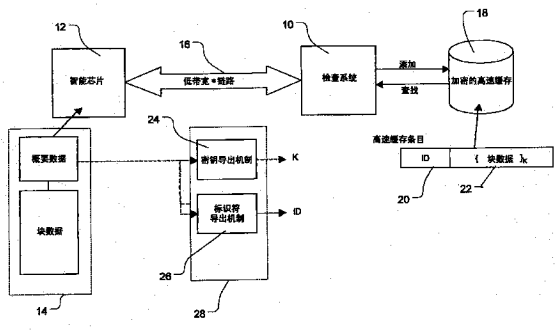
权利要求书2页 说明书7页 附图6页

(54)发明名称

安全数据高速缓存

(57)摘要

本发明总体涉及用于对数据进行安全高速缓存的方法、设备和计算机程序代码,具体而言用于对智能卡系统上存储的数据,如在符合ICAO的EU电子护照中使用的数据进行高速缓存的方法、设备和计算机程序代码。一种高速缓存系统,用于向电子文档中存储的数据提供安全数据高速缓存,所述高速缓存系统包括:输入,接收要高速缓存的数据;处理器,被配置为:使用所接收的数据的全部或部分来计算所述数据的唯一密码密钥;使用所述唯一密码密钥对所述数据的全部或部分进行加密;以及在加密之后丢弃所述唯一密码密钥;以及输出,向数据高速缓存器发送所加密的数据,其中,对所加密的数据进行解密需要根据所述电子文档来重新计算所述唯一密码密钥,从而所述数据高速缓存器是安全的。使用这种高速缓存,除了在首次检查期间以外,通过避开完全读取数据的需要,显著加快了检查过程。



CN 102016862 B

1. 一种用于从安全数据高速缓存器中检索电子文档上的数据的方法，该电子文档包括第一数据部分和第二数据部分，其中该第二数据部分被加密并被存储在所述安全数据高速缓存器中，其中该第二数据部分已经使用唯一密码密钥进行加密，所述唯一密码密钥是根据所述电子文档中的第一数据部分计算的并且在加密之后被丢弃，所述用于从安全数据高速缓存器中检索电子文档上的数据的方法包括：

读取所述电子文档上的所述第一数据部分；

使用所读取的所述电子文档的所述第一数据部分来重新计算所述唯一密码密钥；以及

通过使用重新计算的唯一密码密钥对所述安全数据高速缓存器中储存的所述电子文档的已加密的所述第二数据部分进行解密，从所述安全数据缓存器中检索所述电子文档的所述第二数据部分。

2. 根据权利要求 1 所述的方法，其中，所述电子文档是包括生物统计数据的电子标识文档，所述方法包括：检索所述生物统计数据。

3. 根据权利要求 2 所述的方法，其中，所述电子文档包括概要数据，所述方法包括：使用所述概要数据的全部或部分来计算所述生物统计数据的唯一密码密钥。

4. 根据权利要求 3 所述的方法，其中，所述生物统计数据包括面部信息，所述方法包括：使用所述概要数据的全部或部分来计算所述面部信息的唯一密码密钥。

5. 根据权利要求 3 所述的方法，其中，所述概要数据包括数字签名的数据以及所述生物统计数据是图像形式的生物统计数据，所述方法包括：使用所述图像的部分和所述数字签名的数据来计算所述图像的唯一密码密钥。

6. 根据权利要求 2 所述的方法，其中，所述生物统计数据包括图像，所述方法包括：使用所述图像的部分来计算所述图像的唯一密码密钥。

7. 根据权利要求 6 所述的方法，其中，所述图像是指纹数据。

8. 根据权利要求 1 所述的方法，还包括以匿名标识符将所加密的数据存储在所述高速缓存器中，从而所述数据在所述高速缓存器中是不能进行个人标识的。

9. 根据权利要求 1 所述的方法，其中所述用于从安全数据高速缓存器中检索电子文档上的数据的方法是在处理器上执行的，所述安全数据高速缓存器对于所述处理器而言是远程的，并且所述处理器被配置为与所述安全数据高速缓存器之间通过无线连接来通信。

10. 一种用于验证电子文档的方法，所述方法包括：

通过下述方式创建安全数据高速缓存器：

从所述电子文档中读取数据，该电子文档包括第一数据部分和第二数据部分；

仅使用所述电子文档的所述第一数据部分来计算唯一密码密钥；

使用所述唯一密码密钥对所述电子文档的所述第二数据部分进行加密；

在加密之后丢弃所述唯一密码密钥；以及

将所加密的第二数据部分高速缓存在安全数据高速缓存器中；

通过下述方式验证所述文档：

从所述电子文档中读取所述第一数据部分；

使用所读取的所述电子文档的所述第一数据部分来重新计算所述唯一密码密钥；

使用重新计算的唯一密码密钥来对所述安全数据高速缓存器中储存的所述电子文档的已加密的所述第二数据部分进行解密；以及

使用所解密的所述电子文档的所述第二数据部分来验证所述电子文档。

11. 一种用于验证电子文档的设备，所述设备包括：

用于创建安全数据高速缓存器的装置，其包括：

用于从所述电子文档中读取数据的装置；该电子文档包括第一数据部分和第二数据部分；

用于仅使用所述电子文档的所述第一数据部分来计算唯一密码密钥的装置；

用于使用所述唯一密码密钥对所述电子文档的所述第二数据部分进行加密的装置；

用于在加密之后丢弃所述唯一密码密钥的装置；以及

用于将所加密的第二数据部分高速缓存在安全数据高速缓存器中的装置，以及

用于验证所述文档的装置，其包括：

用于从所述电子文档中读取所述第一数据部分的装置；

用于使用所读取的电子文档的所述第一数据部分来重新计算所述唯一密码密钥的装置；

用于使用重新计算的唯一密码密钥来对所述安全数据高速缓存器中储存的所述电子文档的已加密的所述第二数据部分进行解密的装置；以及

用于使用所解密的所述电子文档的所述第二数据部分来验证所述电子文档的装置。

12. 根据权利要求 11 所述的设备，其中，所述电子文档是包括生物统计数据的电子标识文档，所述设备包括：用于检索所述生物统计数据的装置。

13. 根据权利要求 12 所述的设备，其中，所述电子文档包括概要数据，所述设备包括：用于使用所述概要数据的全部或部分来计算所述生物统计数据的唯一密码密钥的装置。

14. 根据权利要求 13 所述的设备，其中，所述生物统计数据包括面部信息，所述设备包括：用于使用所述概要数据的全部或部分来计算所述面部信息的唯一密码密钥的装置。

15. 根据权利要求 12 所述的设备，其中，所述电子文档包括数字签名的数据和图像形式的生物统计数据，所述设备包括：用于使用所述图像的部分和所述数字签名的数据来计算所述图像的唯一密码密钥的装置。

16. 根据权利要求 12 所述的设备，其中，所述生物统计数据包括图像，所述设备包括：用于使用所述图像的部分来计算所述图像的唯一密码密钥的装置。

17. 根据权利要求 15 或权利要求 16 所述的设备，其中，所述图像是指纹数据。

18. 根据权利要求 11 所述的设备，还包括：用于以匿名标识符将所加密的数据存储在高速缓存器中的装置，从而所述数据在高速缓存器中是不能进行个人标识的。

安全数据高速缓存

技术领域

[0001] 本发明总体涉及用于对数据进行安全高速缓存的方法、设备和计算机程序代码，具体地，用于存储私有和 / 或安全敏感数据（如来自电子标识文档的生物统计数据）的方法、设备和计算机程序代码。

背景技术

[0002] 电子标识文档是以电子存储的信息增强的物理 ID 文档，例如以具有接触式或非接触式接口的智能卡芯片增强的物理 ID 文档。示例包括电子护照、国家 ID 卡、驾驶执照和健康卡。智能卡芯片可以执行多种功能，包括：认证用户标识、提供防伪和存储数据。关键是，许多电子标识方案使用具有存储器的智能卡芯片，作为标识卡持有者的个人和生物统计数据的分布式数据库。每个卡可以存储多至 80KB 数据。

[0003] 国际民航组织 (ICAO) 已经制定了一组规范，用于在机器可读旅行文档 (MRTD) 上存储生物统计数据，依照使用来自发布权威机构的数字签名来保护其完整性的方式格式化生物统计数据。所存储的数据和关联的元信息的格式包括 ICAO“逻辑数据结构”(LDS)。

[0004] 尽管使用智能卡系统作为分布式数据库具有许多优点，但是也有缺点。具体地，由于非接触式接口的带宽限制，从智能卡芯片读取数据较为耗时。从电子标识文档中读取生物统计数据组可能要花费超过 10 秒。如果使用匹配不佳的芯片和读取器软件，则可能花费超过 20 秒。甚至对智能卡的接触式接口也不支持特别高的数据速率，并且，随着不同的生物统计方案（指纹、虹膜等等）竞争以便成为实现，可能需要存储的个人和生物统计数据的量正在快速增长。

[0005] 基于智能芯片、用于标识文档的方案的备选方案是维持数据的集中存储。公开密钥技术直接应用于任一场景中以允许验证者检查从中心存储器检索的数据的完整性。然而，对于存储器自身而言，存在大量安全和私密问题。此外，当必须在远程环境中验证标识文档时，或者在中心数据库受到通信故障的影响时，还要考虑连接问题。

[0006] 这种数据库的内容将需要受制于数据保护法，并容易受到目的的滥用和曲解（针对与原先收集内容的原始原因不同的目的而合法使用）。尽管各国自由追求其自身的中心生物统计收集项目，但是 EU 已经要求，成员国从 EU 护照中检索的敏感生物统计数据不得由检查系统存储。

[0007] 从 WO98/47259 和 US6577735 已知用于创建数据的加密存储的方法。

发明内容

[0008] 根据本发明的一方面，提供了一种对电子文档中存储的数据进行安全高速缓存的方法，所述方法包括：从所述电子文档中读取数据，使用所述数据的全部或部分来计算所述数据的唯一密码密钥；使用所述唯一密码密钥对所述数据的全部或部分进行加密；在加密之后丢弃所述唯一密码密钥，并将所加密的数据高速缓存在数据高速缓存器中，其中，对所加密的数据进行解密需要有所述电子文档存在，以根据所述电子文档来重新计算所述唯一

密码密钥。

[0009] 根据本发明的另一方面，提供了一种高速缓存系统，用于向电子文档中存储的数据提供安全数据高速缓存，所述高速缓存系统包括：输入，接收要高速缓存的数据；处理器，被配置为：使用所接收的数据的全部或部分来计算所述数据的唯一密码密钥；使用所述唯一密码密钥对所述数据的全部或部分进行加密；以及在加密之后丢弃所述唯一密码密钥；以及输出，向数据高速缓存器发送所加密的数据，其中，对所加密的数据进行解密需要有所述电子文档存在，以根据所述电子文档来重新计算所述唯一密码密钥，从而所述数据高速缓存器是安全的。

[0010] 所述电子文档可以是包括生物统计数据的电子标识文档，所述方法可以包括：对所述生物统计数据的全部或部分进行读取、加密和高速缓存。使用这种高速缓存，除了在首次检查期间以外，通过避开完全读取数据的需要，显著加快了检查过程。上述方法和高速缓存系统创建了生物统计数据的加密的高速缓存，其中，每个条目仅在其所源自的原始标识文档存在的情况下才能够被访问。使用这种加密的高速缓存表示了不存储数据的完全分布式方案与集中存储所有数据的完全集中式方案之间的可行的折衷。对于已经从标识文档中读取的数据，可以在本地、国家或者甚至国际级别进行数据的本地高速缓存。

[0011] 可以以假名或匿名标识符来将数据存储在高速缓存器中，从而所述数据在高速缓存器中是不能够进行个人标识的。标识符可以被认为是对数据的查找键值，在于：它使得检查系统能够查找数据，但是标识符不预期是密码密钥。可以在高速缓存器中存储数据的仅一部分，例如可以省去每个数据文件的头部。按照这种方式，在不访问原始文档的情况下，不可能检索数据。

[0012] 所述电子文档可以包括概要数据，即，对其中存储的数据进行概括的文件。所述概要数据可以包括所存储的其他数据的密码散列，或者，数字签名和所述概要数据的全部或部分可以用于计算所述生物统计数据的唯一密码密钥。例如，可以将密钥导出函数应用于该概要数据来产生用于对来自护照的数据进行加密的安全密钥。仅当电子文档存在时，才能够根据概要数据来重新创建这种密钥。还可以将标识符导出函数应用于该概要数据来产生数据的标识符。

[0013] 所述生物统计数据可以包括面部信息和 / 或指纹数据，所述概要数据的全部或部分（例如数字签名）可以用于计算所述生物统计数据的唯一密码密钥。

[0014] 例如，电子标识文档可以是符合 ICAO 的 EU 电子护照，该 EU 电子护照可以包含 16 个不同数据组的生物统计（例如面部、指纹和 / 或虹膜信息）、传记和附加信息，如签名数据。可以对任何和 / 或全部这些数据组进行高速缓存。这种护照还包括“文档安全对象 (SO_D)”形式的概要数据，SO_D是一种包含数字签名的“概要文件”。SO_D保护在电子护照上存储的信息的完整性，并且是在从电子护照中读取任何大数据组之前读取的。SO_D包含较高熵的不可预测数据，因此，可以根据文档安全对象，例如根据数字签名，来导出唯一密码密钥。

[0015] 所述唯一密码密钥可以是散列值。对所述数据的全部或部分进行加密可以包括对所述数据进行盐处理 (salting)。导出散列值和进行盐处理是标准的密码技术。散列函数是一种变换，取得输入并返回称为散列值的固定大小的串。散列值可以是其计算所基于的较长消息或文档的简明表示，因此有时被称为“消息摘要”。消息摘要是较大文档的一种数字指纹，这是因为它对于该文档来说是唯一的。在密码学中，盐包括用作对密码运算的输入

之一的随机比特，以增大输入的熵。

[0016] 在电子护照的具体示例中，SO_D包括生物统计数据的散列和数字签名本身。这些散列可以用于计算所述唯一密码密钥，例如可以对一半散列值进行盐处理，然后使用标准的最优密码技术来对该其进行散列处理。

[0017] 电子文档中存储的一些数据可以受到其他机制的保护，以防止对这种数据的非授权访问。相应地，使用概要信息来计算唯一密码密钥可能是不够的，这是因为这种信息有效地对数据的授权访问的结果进行高速缓存。在这种情况下，数据自身的一部分（例如数据的实际文件的头部）可以用于创建数据的唯一密码密钥。按照这种方式，文档发布者可以始终撤销对访问受控数据的访问（假定文档发布者有效地核查了安全数据高速缓存是适当实现的）。

[0018] 例如，经由 EAC 套件中称为“终端认证”的安全机制来保护 EU 护照中的指纹数据免受非授权访问，终端认证要求检查系统表明其被授权恢复数据。如果 SO_D中存储的指纹数据的散列用于计算唯一密码密钥，则该散列始终可用于电子护照检查器而无需经过终端认证过程。因此，仅使用电子签名来存储指纹数据有效地对终端认证的（成功）结果进行高速缓存。因此，即使从检查系统撤回终端认证，仍能够访问指纹数据。在本示例中，生物统计数据（即指纹数据）具有图像的形式，并且，可以使用所述图像的部分单独地或与所述电子签名相结合来计算所述图像的唯一密码密钥。

[0019] 根据本发明的另一方面，提供了一种用于从使用根据之前任一权利要求所述的方法创建的安全数据高速缓存器中检索电子文档上的数据的方法，所述用于检索数据的方法包括：从所述电子文档读取一些数据；使用所读取的数据的全部或部分来重新计算所述电子文档的所述唯一密码密钥；以及通过使用重新计算的唯一密码密钥对所述安全数据高速缓存器中所述电子文档的加密数据进行解密，检索所述电子文档上的数据。

[0020] 换言之，从安全数据高速缓存器，而不是从文档本身，检索电子文档上的数据（除了创建密钥所需的数据以外）。如上所述，这显著加快了访问文档上的数据所需的时间。除了在首次检查文档期间（即，在创建数据高速缓存器期间）以外，可以避开读取所有数据的需要。

[0021] 所述电子文档可以是包括生物统计数据的电子标识文档，所述方法可以包括：检索所述生物统计数据。上述这种文档的特征也适用于本发明的其他方面。

[0022] 根据本发明的另一方面，提供了一种用于验证或检查电子文档的方法，所述方法包括：创建如上所述的安全数据高速缓存器；从所述电子文档中读取部分数据，使用所读取的数据的全部或部分来重新计算所述电子文档的所述唯一密码密钥；使用重新计算的唯一密码密钥来对所述安全数据高速缓存器中所述电子文档的加密数据进行解密，并使用所解密的数据来验证所述电子文档及其持有者。

[0023] 根据本发明的另一方面，提供了一种用于从由根据权利要求 13 至 16 中任一项所述的高速缓存系统创建的安全数据高速缓存器中检索电子文档上的信息的数据检索系统，所述数据检索系统包括：检查系统，用于从所述电子文档中读取一些数据；以及处理器，被配置为：使用所读取的数据的全部或部分来重新计算所述数据的所述唯一密码密钥；以及使用重新计算的唯一密码密钥来对所述安全数据高速缓存器中的加密数据进行解密，从而从所述安全数据高速缓存器中检索所述电子文档上的数据。

[0024] 根据本发明的另一方面，提供了一种用于验证电子文档的验证系统，所述验证系统包括：如上所述的安全数据高速缓存器；输入，从所述电子文档接收数据；以及处理器，被配置为：使用所接收的数据的全部或部分来重新计算所述数据的所述唯一密码密钥；使用重新计算的唯一密码密钥来对所述安全数据高速缓存器中的加密数据进行解密，并使用所解密的数据来验证所述电子文档及其持有者。

[0025] 所述验证系统可以与仅由所述验证系统自身知道的秘密密码密钥相关联，该秘密密码密钥可以结合进计算中以导出数据的唯一密码密钥。

[0026] 本发明还提供了处理器控制代码，以在例如通用计算机系统上或者在数字信号处理器 (DSP) 上实现上述方法。可以在载体（如盘、CD-ROM 或 DVD-ROM）、编程的存储器（如只读存储器（固件））上提供该代码。用于实现本发明实施例的代码（和 / 或数据）可以包括传统编程语言（解释型或编译型）（如 C) 中的源、对象或可执行代码、或者汇编代码、用于设置或控制 ASIC（专用集成电路）或 FPGA（现场可编程门阵列）的代码、或者用于硬件描述语言（如 Verilog（商标）或 VHDL（甚高速集成电路硬件描述语言））的代码。本领域技术人员可以认识到，这种代码和 / 或数据可以分布在多个互相通信的耦合组件之间。

附图说明

[0027] 图 1 是结合了安全数据高速缓存器的检查系统的框图总览；

[0028] 图 2 是用在电子护照应用中所使用的检查系统中的、图 1 的变型；

[0029] 图 3 示意了对图 2 的电子护照中的数据的唯一密码密钥的计算；

[0030] 图 4 是示出了本地、国家和国际检查系统如何与安全数据高速缓存器进行通信的示意图；

[0031] 图 5 示出了图 1 或图 2 的检查系统的组件的示意图；以及

[0032] 图 6 是创建安全数据高速缓存器、从中检索信息并验证文档的步骤的流程图。

具体实施方式

[0033] 图 1 示出了用于检查电子文档的检查系统 10，电子文档包含智能芯片 12，智能芯片 12 上存储有包括概要数据和块数据在内的数据 14。智能芯片 12 可以具有接触式或非接触式接口。检查系统通过标准技术（当前是低带宽链路 16）来访问智能芯片 12 上保持的电子数据。低带宽意味着与必须传输的数据量成比例的低带宽。

[0034] 检查系统 10 还连接至安全数据高速缓存器 18，安全数据高速缓存器 18 可以对检查系统而言是本地的，或者可以是例如通过在线连接与检查系统连接的共享高速缓存器。高速缓存器中的每个条目包括标识符 ID 20 和使用唯一密码密钥 K 加密的加密块数据 $\{块数据\}_K$ 22。检查系统 10 与安全数据高速缓存器 18 之间的通信是双向链路，使得检查系统可以向高速缓存器添加条目并查找高速缓存器中存储的信息。

[0035] 如虚线所示，标识符 ID 和用于对数据进行加密的唯一密码密钥 K 都是从智能芯片上保持的概要数据导出的。使用密钥导出机制 24 来导出该密钥，密钥导出机制 24 可以是应用于概要数据的散列函数或其他标准密码函数。类似地，使用标识符导出机制 26 来导出该标识符，标识符导出机制 26 可以向概要数据应用散列函数或其他类似函数。密钥和标识符导出机制都是处理器 28 的一部分，处理器 28 对检查系统而言可以是本地的或者远程的。

[0036] 在图 2 中，针对符合 ICAO 的 EU 电子护照 32，对图 1 的系统进行了适配。这种护照 32 上存储的数据 34 包含 16 个不同组的生物统计、传记和附加信息。要存储在符合 EU 扩展访问控制 (EAC) 的电子护照上的两个较大的生物统计数据组是 ：

[0037] 数据组 2(DG2)- 面部信息

[0038] 数据组 3(DG3)- 指纹信息

[0039] 在从电子护照中读取这些较大数据组之前，首先读取“文档安全对象”(SO_D)。“文档安全对象”(SO_D) 是一种“概要文件”，包含数字签名并保护电子护照上存储的信息的完整性。由于概要文件包含较高熵的不可预测数据，其包括生物统计数据的散列和数字签名本身，因此可以将密钥导出函数应用于该数据以产生用于对来自护照的数据进行加密的安全密钥。仅在拥有概要文件时才能够重新创建这种密钥。

[0040] 在电子护照的具体示例中，可以使用对每个数据组计算的散列值作为密码密钥，以在对数据组块数据进行高速缓存之前对其进行加密。该散列值还可以用作假名或标识符，以防止在数据库中可对数据组进行个人标识。

[0041] 在一个具体示例中，可以通过将数据的散列 H(DG2) 分为两半来安全地存储 DG2。第一半用作对 (非密码) 散列表的标识符 ID = left(H(DG2))，以存储数据组。然后，使用从散列的第二半导出的密码密钥，即 K = right(H(DG2))，来对数据组进行加密。使用标准的最优密码技术来进行该加密，包括盐处理。高速缓存表中的示例行将包含以下查找键值或标识符以及加密数据 ：

[0042]

left(hash(DG2))	encrypt(right(hash(DG2)),salt||DG2)

[0043] 按照这种方式，仅在拥有真实电子护照 (其文档安全对象包含数据组的散列) 时，才能够计算密钥并对数据组进行解密。即使知道制作数据组所基于的公民的身份，也不可能预测生物统计数据组的该散列的值。典型地，该数据是 JPEG 文件、WSQ 图像或类似的图像文件，从语义角度来看，这种图像文件是高度冗余编码。相应地，它们包含许多不可预测的数据，因此具有较高的熵。

[0044] 检查可能想要高速缓存的一些智能卡数据受到访问控制机制的保护。例如，EU 护照中的指纹数据存储在数据组 3(DG3) 中，并且，经由 EAC 套件中称为“终端认证”的安全机制来保护该指纹数据免受非授权访问，终端认证要求检查系统表明其被授权恢复数据。然而，指纹数据的散列可用于文档安全对象中的电子护照检查器，而无需经过终端认证过程。因此，使用上述方案来存储指纹数据有效地对终端认证的 (成功) 结果进行高速缓存。在首次成功访问之后可以绕过访问控制机制的情况下，图 3 示出了密钥导出机制 24 如何导出密钥 K。

[0045] 从文档安全对象可用的数据的散列 H(EF.DG3)32 与实际文件的头部进行组合。包括文件 40 的足够大的头部以将充足的较高熵数据包含在散列中是很重要的。所使用的头部的量必须遍及文件头部 42、生物统计 CBEFF 头部 44 和图像头部 46 以及图像 48 自身的一部分。因此，来自未经访问控制的概要文件的较高熵数据与经过了访问控制的实际文件自身的头部一起用作对密钥导出函数的输入。

[0046] 指纹数据组的前 200 个字节与 DG3 的散列拼接，以形成仅在执行适当的访问控制

过程之后才能重新创建的密钥。因此，文档发布者始终可以撤销另一国家对访问受控数据的访问（假定文档发布者有效地核查了检查器适当实现该方案）。在本示例中，高速缓存表将包含以下形式的行：

[0047]

left(hash(DG3))	encrypt(hash(head(DG3)),salt||DG3)

[0048] 图 4 示意了检查系统 10 如何能够连接至一个或多个安全数据高速缓存器。检查系统可以与嵌入检查系统自身中的本地高速缓存器 101 形式的安全数据高速缓存器进行通信。检查系统可以经由因特网或使用标准技术的专用网，与外部高速缓存器（例如港口或国家高速缓存器 102 或国际高速缓存器 103）进行通信。对于外部高速缓存器 102、103，可以存在网络上的同步以向高速缓存器添加数据。

[0049] 这种高速缓存方案的可行性（尤其对于离线设备）取决于针对从智能芯片中检索的数据的存储要求。为了表明该可行性，以典型地存储在 EU EAC 电子护照上的数据为例：

[0050] 面部图像 20KB

[0051] 指纹图像每幅 15KB（通常为两幅）

[0052] 这给出了针对每个护照持有者典型的最大 50KB 的数据。存储 2 亿名旅行者的加密生物统计数据的数据库将需要 50KB*2 亿＝ 9.3 万亿字节。实际上，护照持有者的旅行频率的分布是相当不均匀的。相应地，可以基于存储价格和运营考虑来选择可用的高速缓存空间，将高速缓存器中的空间分配给最频繁的用户。存在多种合适的高速缓存填充和替换算法。使用网络上的同步，可以在本地检查系统、入境港口、国家区域（或甚至有国际合作）之间执行多层高速缓存。

[0053] 对于不能经由无线连接访问外部高速缓存器的便携式检查系统，可以容易地将最频繁的 100,000 个旅行者的加密生物统计信息的本地高速缓存器 101 加载至 4GB 闪存卡上。

[0054] 再次注意，高速缓存器不包含个人可标识的信息，并且，尽管它包含加密数据，但是一旦丢弃了密钥，则该数据被有效地删除。概念上，一旦 PC 的电源关闭，实际数据就不再保持在系统上，生物统计信息的 RAM 拷贝也不再保持在系统上。

[0055] 可以使用两种另外的机制来降低高速缓存存储要求，并控制高速缓存的分发和使用（如果高速缓存器的创建者不希望共享其高速缓存数据）。首先，由于每个访问受控数据组的头部被读出以包括在存储密钥导出过程中，因此该头部不需要包括在高速缓存条目自身中，从而针对每个生物统计记录节省了数百字节（当存储数十亿护照持有者的记录时，如此小的节省将被放大）。这还表明在不访问原始文档的情况下不可能检索生物统计数据——因为其中一些完全丢失。

[0056] 其次，在构造高速缓存条目期间和在检索时，可以结合仅由有效检查系统知道的秘密密码密钥作为对密钥导出函数的输入。这使得第三方不可能通过在不操作经认可的检查系统的情况下访问高速缓存数据来获得加速。

[0057] 最后，还存在一些问题：如果国家需要移至十指纹生物统计系统，而 DG3 三可以容易地存储更多得多的图像，则对整个数据组而不是对其各个部分进行散列处理。这意味着，如果检查器期望仅从较大集合中读出两个食指指纹，则在不读出整个集合的情况下不能确

保这些图像的完整性。经由非接触式接口读出十指纹集合可能花费超过 60 秒，从而甚至进一步放大了在该环境下进行高速缓存的优点。

[0058] 图 6 示出了检查系统的组件。检查系统 10 包括处理器 50 与代码和数据存储器 52、输入 / 输出系统 54（例如包括对数据高速缓存器的接口和 / 或用于连接至智能芯片上的接口的接口）以及用户接口 56（例如包括键盘和 / 或鼠标）相耦合。存储器 52 中存储的代码和 / 或数据可以在可移除存储介质 58 上提供。在操作中，数据包括从电子标识文档收集的数据，代码包括用于处理该数据以产生数据高速缓存、从高速缓存器检索数据和 / 或根据下述图 6 所示的过程验证文档的代码。

[0059] 图 6 示出了使用上述系统的各种方法的流程图。在步骤 S200，系统检查电子文档，在步骤 202，系统确定是否是首次检查文档。如果系统是首次见到该文档，则如步骤 S204 至 S210 所述创建安全数据高速缓存器。在步骤 S204，读取要存储在数据高速缓存器中的所有数据。在步骤 S206，使用所读取的数据的部分，例如使用文档概要，来创建要存储的数据的唯一密钥。然后在 S208，使用该唯一密钥对要存储的数据进行加密。在步骤 S210，将加密数据存储在数据高速缓存器中，系统丢弃该唯一密钥。如上所述，此后，仅当系统存在原始电子文档时才能够检索高速缓存器中的数据。

[0060] 如果系统先前已经见过该文档（并将来自该文档的信息存储在数据高速缓存器中），则在步骤 S214，从该文档中仅读取重新计算唯一密钥所需的数据。在步骤 S216，根据该所读取的数据来计算唯一密钥，在步骤 S218，使用该密钥对数据高速缓存器中的数据进行解密。因此，从高速缓存器而不是从文档中检索电子文档上的数据，从而更快地访问数据。因此，在步骤 S214 至 218 中阐述了从高速缓存器中检索数据的方法。

[0061] 步骤 S212 和 S220 示出了验证文档及其持有者的步骤，其中，文档是第一次或后续某次被看见的。在步骤 S212，使用从文档自身中读取的数据来验证文档，而相反在步骤 S220，使用来自高速缓存器而不是来自文档自身的数据来验证文档。在这两种情况下，仍需要原始文档作为验证过程的一部分，这是因为在没有原始文档的情况下，不可能访问高速缓存器中的数据以计算唯一密钥。

[0062] 以上描述描述了一种在从智能卡读取存储数据的检查系统中对智能卡数据进行安全高速缓存的机制。使用这种机制，通过将从智能卡的数据传送阶段替换为从高速缓存器中进行查找，显著加快了检查返回文档的速度。由于该机制的具体安全特征，高速缓存器不会造成安全性或私密性风险。这种机制通过以下操作来工作：在从文档上存储的较高熵的数据导出的密钥下对高速缓存的数据进行加密，然后丢弃密钥，使得仅在存在真实文档的情况下才能够对高速缓存条目进行解密。

[0063] 毫无疑问，本领域技术人员可以想到许多其他有效的备选方案。可以理解，本发明不限于所描述的实施例，而是包括落入所附权利要求的精神和范围内的、对本领域技术人员而言显而易见的修改。

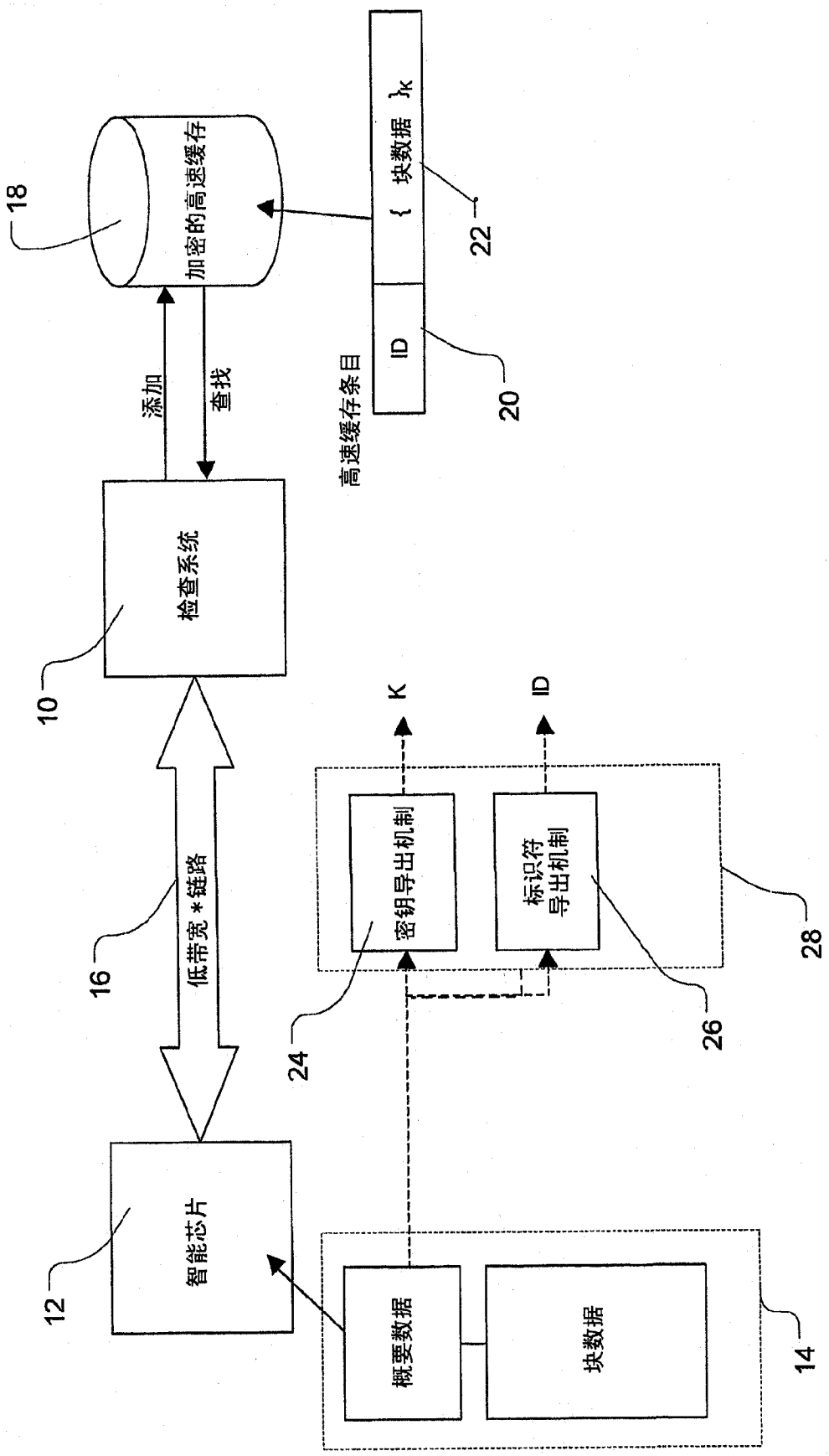

18
加密的高速缓存
{ 块数据 λ_K
22
ID
20
高速缓存条目
添加
查找
检查系统
10
16
低带宽*链路
K
ID
密钥导出机制
标识符
导出机制
28
24
26
12
智能芯片
概要数据
块数据
14

图 1

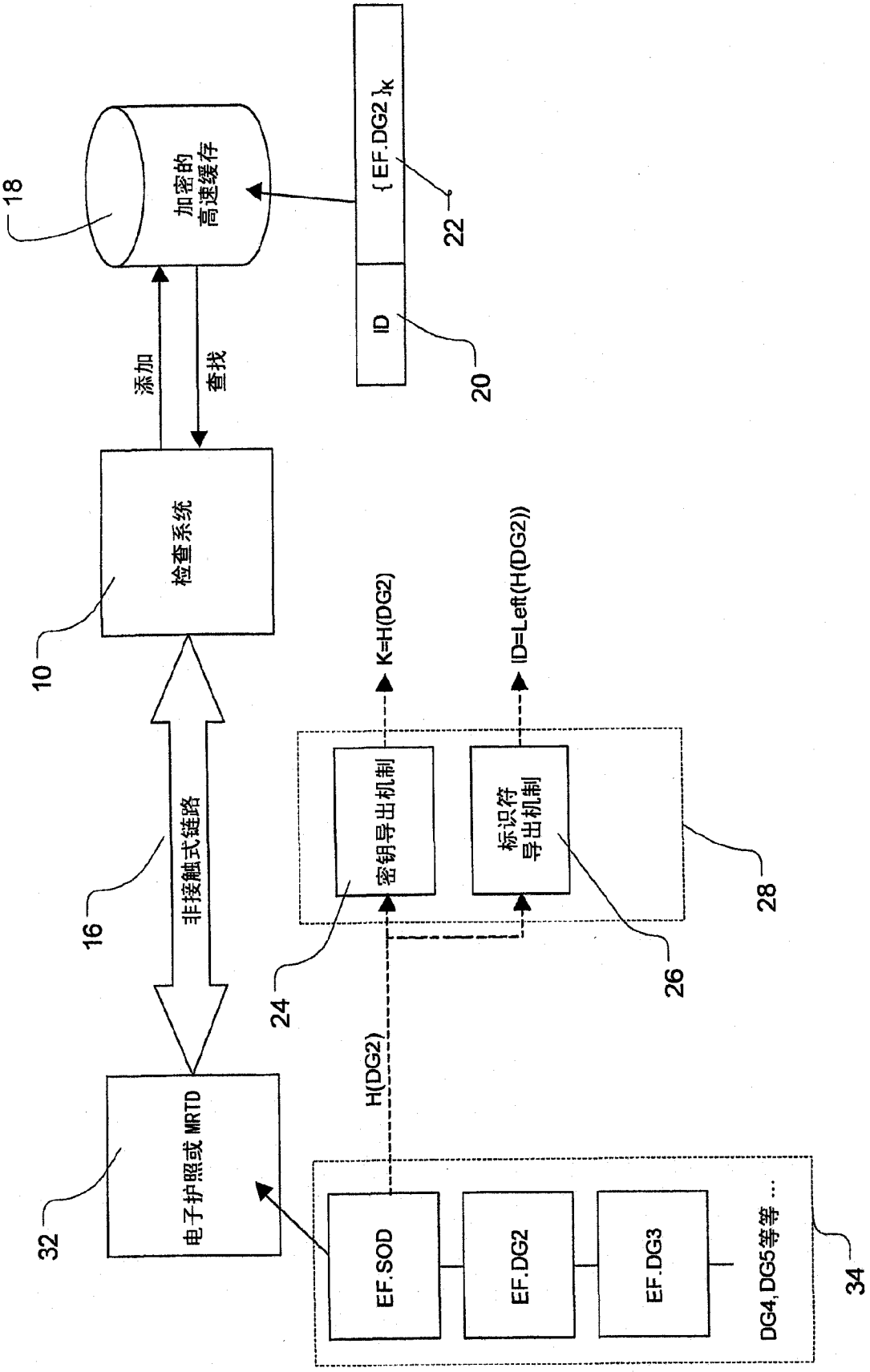

18
加密的
高速缓存
{EF.DG2 λK
22
ID
20
添加
查找
检查系统
10
16
非接触式链路
K=H(DG2)
ID=Left(H(DG2))
密钥导出机制
标识符
导出机制
28
24
26
H(DG2)
32
电子护照或 MRTD
EF.SOD
EF.DG2
EF.DG3
DG4,DG5等等 ...
34

图 2

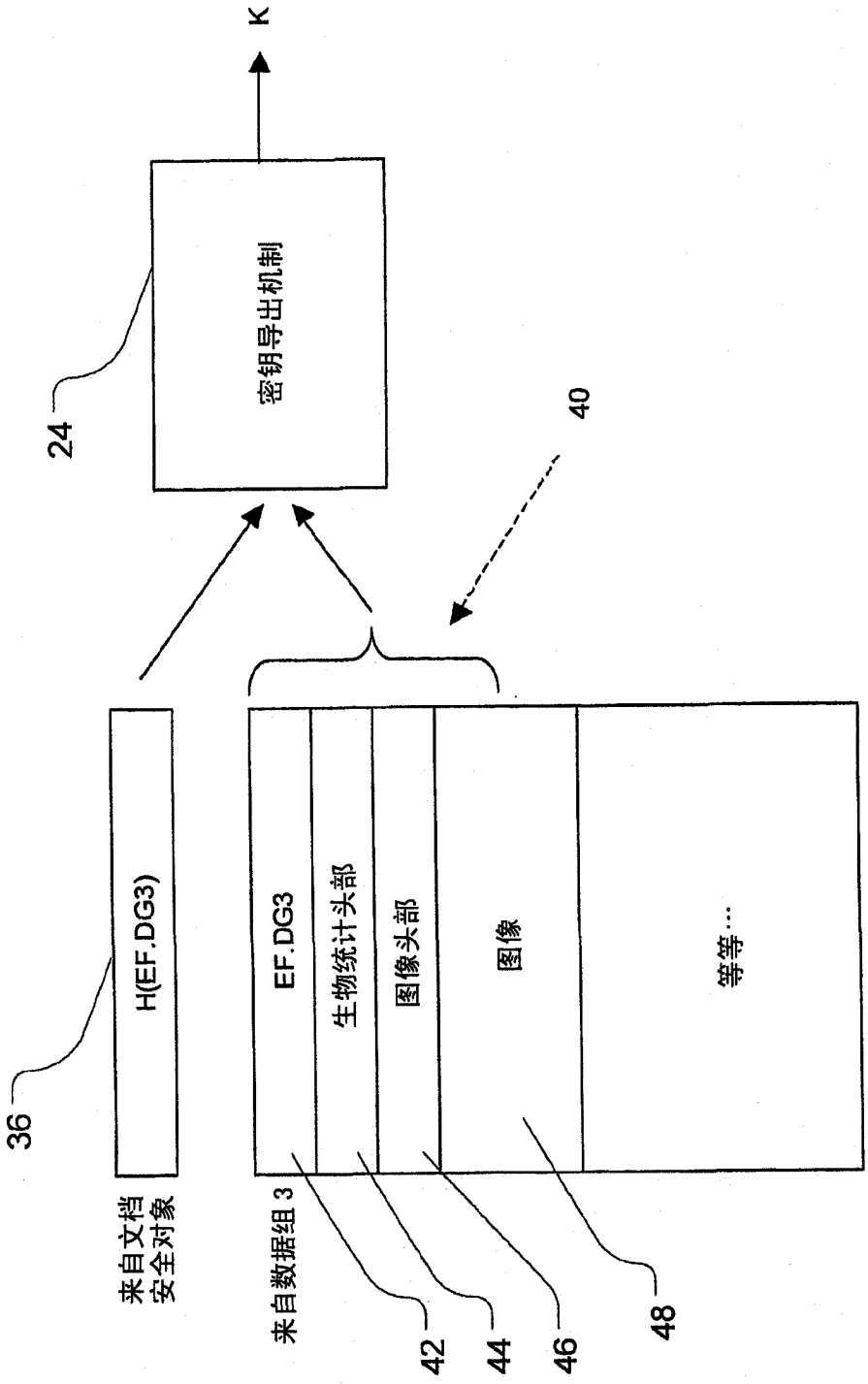

K
密钥导出机制
24
40
H(EF.DG3)
36
来自文档
安全对象
EF.DG3
生物统计头部
图像头部
图像
等等...
来自数据组 3
42
44
46
48

图 3

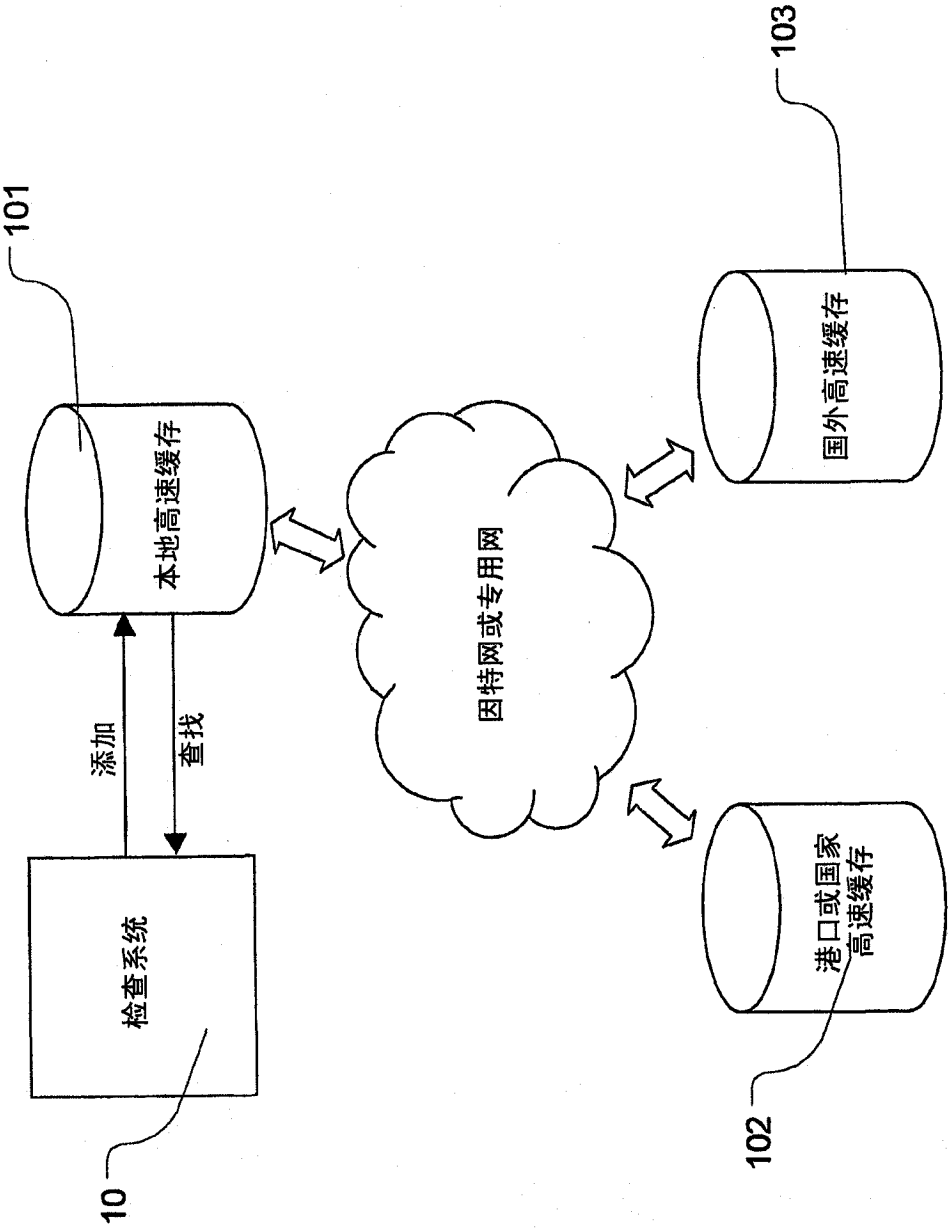


图 4

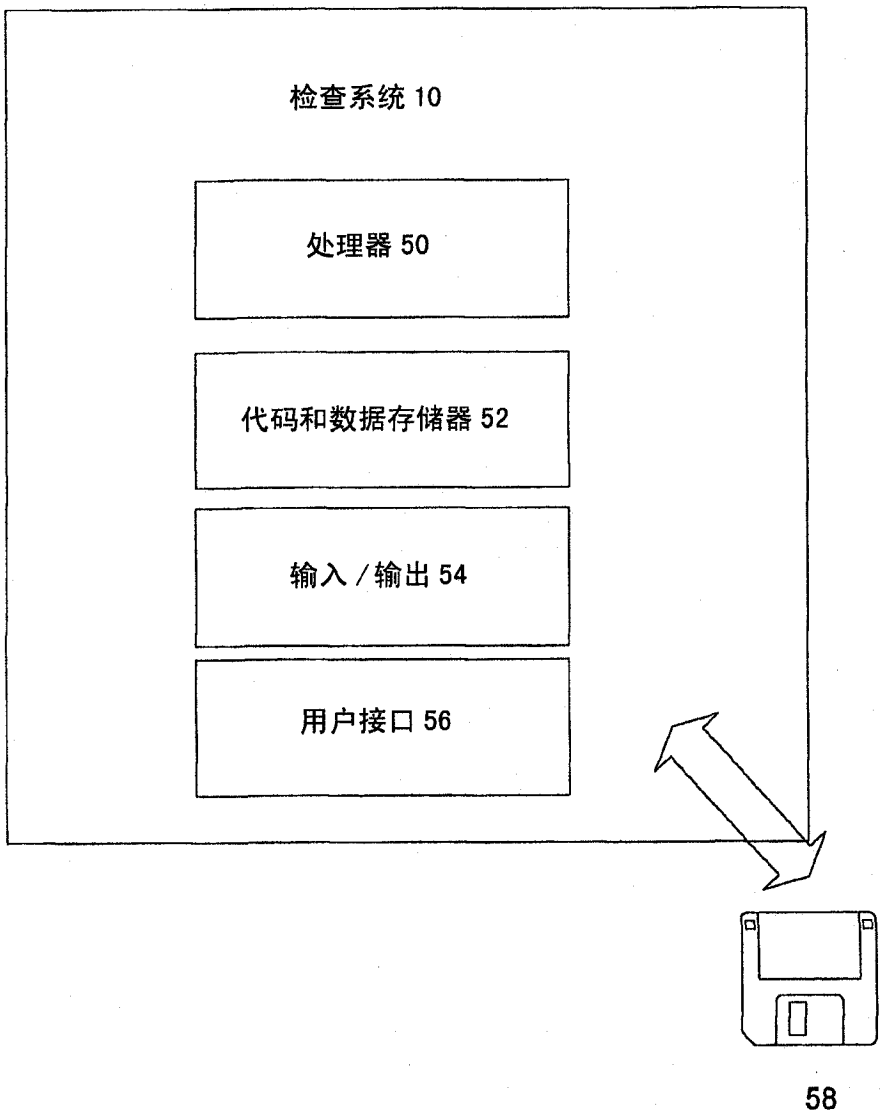


图 5

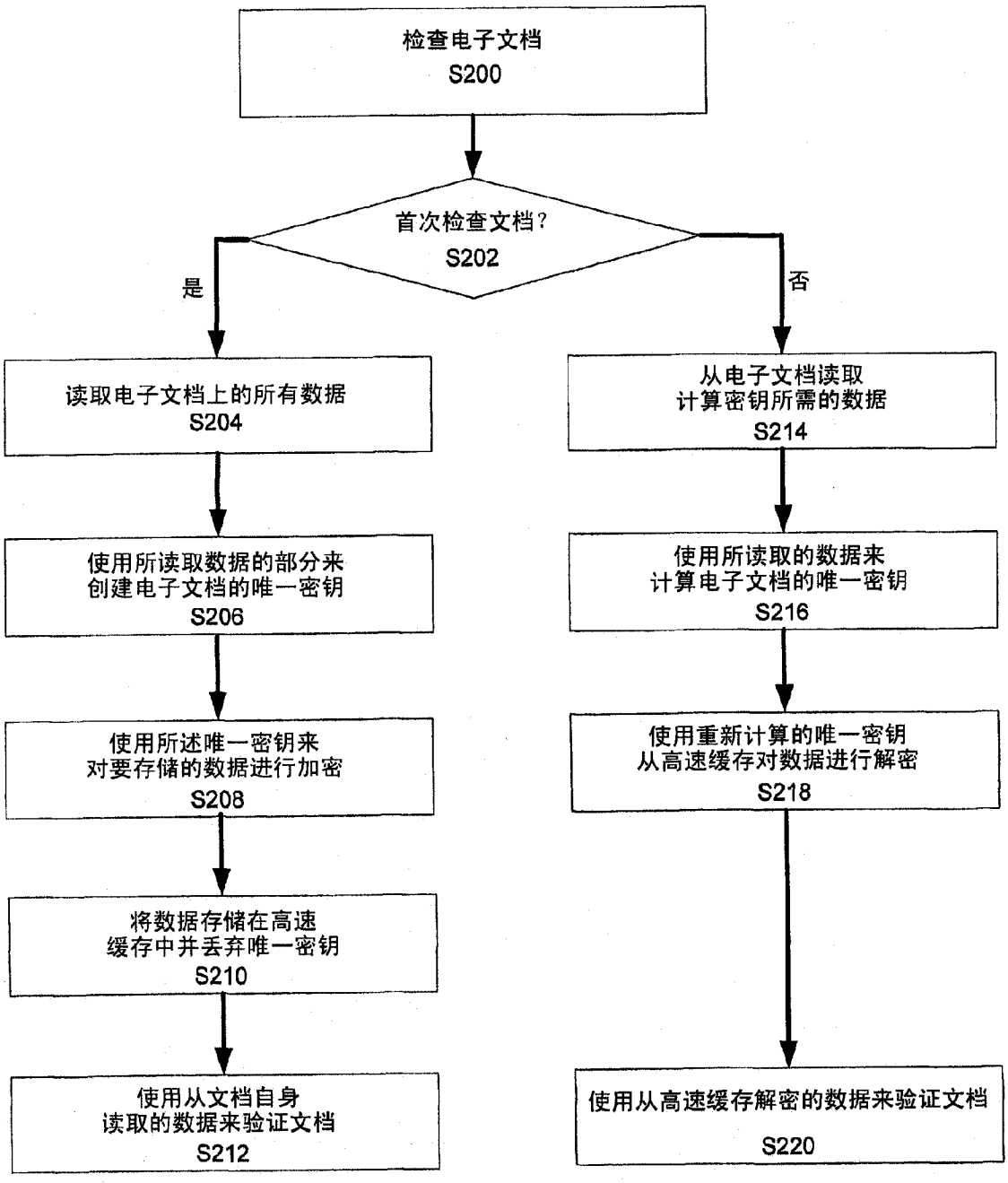

检查电子文档
S200
首次检查文档?
S202
是
否
读取电子文档上的所有数据
S204
使用所读取数据的部分来
创建电子文档的唯一密钥
S206
使用所述唯一密钥来
对要存储的数据进行加密
S208
将数据存储在高速
缓存中并丢弃唯一密钥
S210
使用从文档自身
读取的数据来验证文档
S212
从电子文档读取
计算密钥所需的数据
S214
使用所读取的数据来
计算电子文档的唯一密钥
S216
使用重新计算的唯一密钥
从高速缓存对数据进行解密
S218
使用从高速缓存解密的数据来验证文档
S220

图 6