[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04K 1/00
G09C 1/00

[12] 发明专利说明书

[21] ZL 专利号 97195668.5

[45] 授权公告日 2004 年 4 月 14 日

[11] 授权公告号 CN 1146178C

[22] 申请日 1997.6.18 [21] 申请号 97195668.5
[30] 优先权
[32] 1996.6.20 [33] SE [31] 9602475-7
[86] 国际申请 PCT/SE1997/001089 1997.6.18
[87] 国际公布 WO97/49211 英 1997.12.24
[85] 进入国家阶段日期 1998.12.18
[71] 专利权人 普罗特格里特 诺狄克股份公司
地址 瑞典哥德堡
[72] 发明人 沃夫·达尔
审查员 李 明

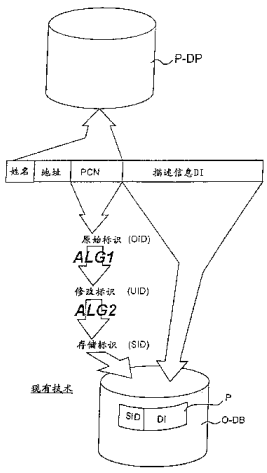
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 吴丽丽

权利要求书 2 页 说明书 13 页 附图 4 页

[54] 发明名称 用于数据处理的方法和装置

[57] 摘要

本发明涉及一种用于处理将受到保护的数据的方法和装置。 数据以编码后的数据元素值(DV)的形式存储在第一数据库(O-DB)的记录(P)中，其中每个数据元素值均被链接到相应的数据元素类型(DT)上，在第二数据库(IAM-DB)中，存储了一个数据元素保护目录(DC)，其中在该目录中为每个单独数据元素类型(DT)包含一个或多个描述数据元素值(DV)处理规则的保护属性，其中在第一数据库(O-DB)中数据元素值被链接到单独数据元素类型(DT)上。 在每个目的在于处理第一数据库(O-DB)中的给定数据元素值(DV)的用户-初始方法中，首先一个强制性调用被发送给数据元素保护目录，以选择与相应数据元素类型相干的保护属性/属性组。 根据所选择的保护属性/属性组，用户对于给定数据元素值的处理被强行地控制。



ISSN1008-4274

1. 一种用于处理将被保护的数据的方法，包括把数据以编码后的数据元素值（DV）的形式存储在第一数据库（O-DB）的记录（P）中的方法，其中每个数据元素值均被链接到相应的数据元素类型（DT）上，该方法的特征在于包括以下步骤：

在第二数据库（IAM-DB）中存储一个数据元素保护目录（DC），其中 DC 中为每个单独数据元素类型（DT）包括一个或多个描述数据元素值（DV）处理规则的保护属性，其中在第一数据库（O-DB）中的数据元素值被链接到所述各数据元素类型（DT）上，

对于每个目的在于处理第一数据库（O-DB）中一给定数据元素值（DV）的用户激活方法来讲，首先生成一个对于数据元素保护目录的强制性调用，以选择与相应的数据元素类型相关的保护属性/属性组，并

根据所选择的保护属性/属性组，强制性地控制用户对于给定数据元素值的处理。

2. 如权利要求 1 所述的方法，还包括把数据元素保护目录（DC）中的保护属性/属性组以编码后的形式存储在第二数据库（IAM-DB），并且当从数据元素保护目录（DC）中选择保护属性/属性组时将其解码的方法。

3. 如权利要求 1 或 2 中所述的方法，其中在第一数据库（O-DB）的每个记录（P）中均有一个记录标识符，并且该方法还包括把记录标识符以编码后的形式（SID）存储在第一数据库（O-DB）中的方法。

4. 如权利要求 1 或 2 所述的方法，其中第一数据库（O-DB）和第二数据库（IAM-DB）中的数据的编码根据具有浮动存储标识的 PTY 原则进行。

5. 如权利要求 1 或 2 所述的方法，其中数据元素类型的保护属性/属性组包括用于描述规则的属性，用于对第一数据库（O-DB）

中相应的数据元素值进行编码。

6. 如权利要求 1 或 2 所述的方法，其中数据元素类型的保护属性/属性组中包括描述规则的属性，其中规则用于决定那个程序/程序组或程序版本被允许用来管理第一数据库（O-DB）中相应的数据元素值。

7. 如权利要求 1 或 2 所述的方法，其中数据元素值的保护属性/属性组中包括描述规则的属性，其中规则用于对第一数据库（O-DB）中的相应的数据元素值进行事件记录。

8. 一种用于处理将被保护的数据的装置，包括一个第一数据库，用于把作为编码后的数据元素值（DV）的所述数据存储在记录（P）中，每个数据元素值均被链接到相应的数据元素类型（DT）上，其特征在于，包括

第二数据库(IAM-DB)，用于存储数据元素保护目录（DC），其中该目录为每个单独数据元素类型（DT）包括一个或多个描述数据元素值（DV）的处理规则的保护属性，其中在第一数据库（O-DB）中的数据元素值被链接到所述各数据元素类型（DT）上，

适用于在每个目的在于处理第一数据库（O-DB）中的给定数据元素值（DV）的用户-激活方法中的装置，该装置初始地生成对数据元素保护目录的强制性调用，从而选择与相应的数据元素类型相关的保护属性/属性组，

适用于根据所选择的属性/属性组来控制用户对于给定数据元素值的处理强制性控制的装置。

用于数据处理的方法和装置

技术领域

本发明涉及计算机辅助信息管理的技术领域，尤其是涉及一种用于将被保护的数据处理的方法和装置，以加强保护数据免受未授权处理。

背景技术

在计算机辅助信息管理领域中，强烈要求增强保护数据记录免受未授权访问，尤其是要求当建立和保持私人记录即包括个人信息的记录时，保护个人的完整性免受侵犯。特别是，存在对私人记录的链接和匹配进行限制和禁止的规则。并且在其他领域中，例如工业，国防，银行，保险等领域中，也要求对用于管理和存储敏感信息的工具，数据库，应用等，保护它们免受未经授权的访问。

与本申请具有同一申请人的申请 WO95/15628 公开了一种用于存储数据的方法，该方法可不必降低完整性，而提高链接和匹配的可能性。在附图的图 1 和图 2 中所示的方法涉及信息的存储，其中该信息一方面包括识别信息或原始标识 OID，例如私人代码序号 Pcn，另一方面包括描述信息 DI。根据以下原则，信息 OID+DI 作为记录 P 被存储在数据库 O-DB 中：

步骤 1：通过一个第一算法，最好是非可逆算法 ALG1，OID 被编码成更新标识 UID;

步骤 2：通过一个第二可逆算法 ALG2，UID 被编码成存储标识 SID;

步骤 3：SID 和 DI 作为记录 P 被存储在数据库 O-DB 中，SID 作为记录标识符;

步骤 4：在预定时间，通过解码算法 ALG3 把记录中的 SID 解码成 UID，从而实现对所有的或所选择记录 P 中的 SID 的转换，此后 UID 通过一种改进的第二可逆算法或 ALG2'被编码成一种新的存储

标识 SID’，SID’作为新的记录标识符被放在相关记录 P 中，以作为先前 SID 的替代。这一步骤导致记录的 SID 的增强性安全“浮动(floating)”转换。

对于这种编码和存储方法的细节和优点的进一步的描述，可参看 WO95/15628，其中可认为 WO95/15628 构成当前描述的一部分。根据上述步骤 1-4 的存储原则，以下均称其为 PTY，其中 PTY 为概念 PROTEGRITY 的缩写，其中 PROTEGRITY 表示“保护和完整性”。

在由 Leif Jonson 所著的“PROTEGRITY（ASIS）Study 2”，Ver，1.2，1996 年月月，中提供了对于 PTY 的详细的技术描述。也可认为该文献构成当前描述的一部分。

然而，在所讨论的技术领域中，外壳保护为目前主要的保护方法。外壳保护一方面包括外部安全（假设），另一方面包括一个使用用户口令来控制访问的授权检查系统 ACS。ACS 作为主机，客户/服务器系统和 PC 的外壳保护，但是它并不能提供全面的保护，并且争论中的信息也常常相对容易地易受到未授权访问。由于在扩展领域中，存储了“敏感”信息，因此这种保护越来越不令人满意了，其中“敏感”信息必须要求允许通过分布式进行管理，在动态变化的环境中进行存储和处理，其中动态变化的环境尤其是指从局部分布到个人计算机。在当前的这种发展下，系统的限制将越来越模糊并且由外壳保护所提供的作用也将不再适用。

发明内容

鉴于上述原因，本发明的一个目的在于提供一种用于处理信息的改进方法，通过该方法有可能提高使敏感信息免受未授权访问的保护。

本发明的另一个特殊的目的在于提供一种用于数据处理或管理的技术，该技术使得负责系统的人，组织的管理者等可以容易地建立并不断的适应用户对将受到保护的存储信息的各种可能的处理。

本发明的另一个目的在于提供一种用于数据处理的技术，该技术用于通过未确认软件来提供一种保护，以防止试图对数据进行未授权的数据处理。

本发明的另一个目的在于根据上述目的提供一种用于数据处理

的技术，该技术可与上述 PTY 原则联合使用，以提供一种具有极高保护级别的安全系统。

因此，本发明提供了一种用于处理将受到保护的数据的方法，其中该方法包括用于把数据以记录的编码后的数据元素值的形式存储在第一数据库（O-DB）中的方法，其中每个数据元素值均被链接到相应的数据元素类型上。

本发明的方法的特征在于下述采取的措施:

在第二数据库（IAM-DB）中存储了一个数据元素保护目录，其中数据元素保护目录为每一个单独数据元素类型包含一种或多种保护属性，以描述对于数据元素值的处理规则，其中在第一数据库中数据元素值被链接到各数据类型上。

在每一个目的在于处理第一数据库中给定数据元素值的用户-激活方法中，首先生成一个对数据元素保护目录的强制性调用，以选择与相应的数据元素类型相关的保护属性/属性组，并根据所选择的保护属性/属性组，强行地控制对于给定数据元素值的处理。

在本申请中用到了下述定义:

.“处理”可能包括各种处理措施，其中各种指对将由本发明的方法进行保护的数据的各种形式的读取，打印，修改，编码，移动，拷贝等。

.“数据元素类型”涉及具有公认意义的数据的特定类型。

.“数据元素值”涉及在给定记录中指定数据元素类型的值。

.“记录”涉及许多放在一起的数据元素值，其中这些数据元素值均被链接到各自的数据元素类型上，并且记录中还可以包括记录标识符，通过它可识别记录。例子:

	数据元素类型	
记录 ID	社会津贴	汽车
XXXX XXXXX	编码后的数据元素值	编码后的数据元素值
YYYY YYYYY	编码后的数据元素值	编码后的数据元素值

“表示处理规则的保护属性”可涉及

-存储在数据元素保护目录中，并提供有关规则或规则组的全部信息的数据，其中规则或规则组应用于对相应数据元素的处理，和/或

-存储在数据元素保护目录中，并要求另外调用存储在其他地方的信息的数据，可与描述处理规则的保护属性一起指定所涉及的处理规则。

“保护属性的选择”可涉及：

-选择以存储在数据元素保护目录中的形式的保护属性，和/或

-选择由保护属性恢复的数据，例如通过解码。

“编码”可涉及任何形式的编码，三元码，把明文数据代码转换成不可解释（编码后）数据的转换，尤其涉及包括散列的转换方法。

本发明的方法提供了一种新的保护类型，这种保护类型实质上与现有技术中的外壳保护方法不同，并且这种保护类型在元组或数据元素层作用。每个用于第一数据库的记录中的数据元素类型均与一个或多个保护属性相关，其中保护属性存储在独立的数据元素保护目录中，并且保护属性描述了如何处理相应的数据元素值的规则。特别应指出的是，对于数据元素保护目录的调用是强制性的。即，在一个实施根据本发明的方法的系统中，假设一个用户，例如想要读取第一数据库的某记录中的特定数据元素值，则通过他对数据元素值的访问，会自动地并强制地生成一个对于第二数据库中的数据元素保护目录的系统调用，以选择与相应的数据元素类型相关的保护属性。该系统的下一步处理程序（读取数据元素值）也是根据所选择的保护属性/属性组而被强行地控制，其中所选择的保护属性/属性组应用于相应的数据元素类型。

术语“数据元素保护目录”及根据本发明的对它的使用不应与已知术语“主动字典”相混淆，“主动字典”指除操作数据库外，存在一个特殊的表，该表表示对操作数据库中的数据元素值的不同的定义或选择，例如数据元素值“黄”根据定义，表示在上述参照表中所描述的数字区间中的一个颜色代码。

可选地，由保护属性所描述的处理规则对于用户是不可访问的，

并且所读取或所选择的保护属性只有在由系统内部使用以控制处理时才是可取的。一个给定的用户，例如，如果想要读取存储在第一数据库中的有关某个人的信息，则根本不需考虑某一保护属性已被激活，并已取得了某些不能从例如显示器上获得的有关个人的特定的敏感信息。因此，每个目的在于处理数据元素值的用户激活方法，一方面涉及对于数据元素保护目录的强制性调用，一方面涉及下一步的处理，其中下一步的处理强制地受到由保护属性所描述的处理规则的限制，并且可能存在着处理已完成但用户并未获得有关由哪个规则来控制这一处理的信息的情况，尤其是用户根本不可能访问这些规则的情况。

通过改变，添加并移动数据元素保护目录中的保护属性，负责系统的人或相应的人可容易地为每个单独的数据元素类型确定处理规则，其中处理规则应用于与这种单独的数据元素类型相关的数据元素值，从而可容易地保持系统高度而清晰的安全质量。

根据本发明，单独的数据元素（数据元素类型）而不是整个记录成为了控制单元，以使负责系统的组织，操作员等来决定质量的层次，责任和有关信息管理的安全。

为获得高级别的保护，数据元素保护目录最好进行编码，以防止对它们的未授权访问。

作为优选保护属性，本发明提供了以下几种描述，但是，所提供的几种描述被认为是几种不完全的，示例性的描述：

1. 对使用何种“强度”或“级别”（例如0，1，2...）进行编码的描述，以把相应的数据元素值存储在数据库中。同一个记录中的不同的数据元素值可被编码成具有互异的强度。

2. 如果数据元素值将被发送到网络上，则对于对相应的数据元素值将使用何种“强度”或“层次”（例如空，1，2...）进行编码的描述。

3. 对程序和/或程序的版本的描述，其中程序被授权，以处理相应的数据元素值。

4. 对数据元素类型的“属主”的描述。同一记录中的不同的数据元素值可有不同的属主。

5. 对相应的数据元素值的拣出规则的描述，例如，对从数据库中自动移去相应数据元素值的方法和时间的描述。

6. 当处理相应的数据元素值时，对是否自动进行事件记录的描述。

根据本发明的一个特殊的最佳实施例，上述 PTY 存储方法被用来对所有的数据进行编码，其中所有的数据为将要在数据库中（即数据元素值）和数据元素保护目录中（即保护属性）进行编码的数据。一般情况下，每个记录均有各自的记录标识符（相应于上述的 SID），最好是对记录标识符用 PTY 的方法进行保护。尤其是，根据上述的 PTY 原则，可在所需区间和任意所选定的时间来完成操作数据库和数据元素保护目录中的记录标识符的浮动转换。在最佳实施例中，尤其是用于 PTY 编码的封装处理器也可用于实现对于数据元素保护目录的调用和实现根据所选择的保护属性进行处理的程序。

附图说明

下面将参照附图来更详细地解释本发明，其中附图中图示了在示例性数据系统中所实现的发明原则。

图 1（现有技术）图示了根据 WO95/15628 中的 PTY 原则的数据信息的存储原则。

图 2（现有技术）图示了根据 WO95/15628 中的 PTY 原则生成浮动存储标识符的原则。

图 3 图示了一个用于实现根据本发明的方法的计算机系统。

图 4 图示了根据本发明的强制调用数据元素保护目录的数据处理的原则。

图 5 表示一个用于决定数据元素保护目录中保护属性的显示图像的例子。

具体实施方式

下面，标识 IAM（表示信息资产管理器）将被用于组件和应用程序，其中在该实施例中，组件和应用程序对于实现本发明是必需的。

首先参看图 3，图 3 图示了一个实现本发明的数据管理系统，其中该系统中包括了下述几个数据库以存储信息，在该例中存储有关个人的信息：

一个一般包括可访问数据的开放数据库 P-DB，其中可访问数据

为例如人名，品名，地址等，其中个人代码序号 Pcn 以明文的形式作为记录标识符；

- 一个包括受到保护的数据的操作数据库 O-DB．编码后的标识作为记录标识符（=存储标识 SID），在这种情况下编码后的标识指编码后的个人代码序号。 O-DB 被授权用户用以处理个人记录，例如读取和更新；

- 一个档案数据库 A-DB，该数据库中包括从操作数据库 O-DB 传送（抹出）来的数据，并且该数据库用于静态查询，但是并不是用于直接对个人记录的查询．从 O-DB 到 A-DB 的转移可成批地进行。

- 一个对于实现本发明所必需的数据库 IAM-DB．该数据库中包括具有用于数据元素类型的保护属性的数据元素保护目录，其中数据元素类型与操作数据库 O-DB 中的记录中的数据元素值相关，．数据库 IAM-DB 最好是物理地独立于其他数据库 O-DB 并且对于用户是不可访问的。但是，可有两个或更多个数据元素保护目录集：一方面是初始版本，其中只有一个授权 IAM 操作员对初始版本有访问权，另一方面是复制版本，其中复制版本从初始版本处获得数据元素保护目录，并且复制版本可选地存储在与操作数据库 O-DB 相同的文件存储器中．这两个版本可离的很远，例如，可位于不同的城市．

图 3 中的数据系统还可包括一个硬件组件 10，一个控制模块 20（IAM-API），和一个程序模块 30(PTY-API).下面将详细描述这三个组件的功能．

硬件组件 10

硬件组件 10 作为计算机中硬件组件自身的分布式处理器．它有一个封装，使得它可完全防止窜改，即不可能通过跟踪工具进行检测．

硬件组件 10 可作为至少执行以下功能的独立部件：

- 创建用于 PTY 编码的可变的，可逆的和非可逆的编码算法，并为这些算法提供所需的变量；

- 根据 PTY，开始对存储数据中的存储标识（ SID ）进行修改，其中存储数据一方面为 O-DB 中的数据，另一方面为 IAM-DB 中的数据

元素保护目录中的数据;

- 把用户可访问记录的用户授权存储在 O-DB 中; 和
- 把原始标识 OID 与 O-DB 中的正确记录链接起来.

控制模块 20 (IAM-API)

控制模块控制对系统所能提供的数据保护类型的处理.

控制模块执行通过 API (应用程序接口) 程序接口所请求的处理.

程序模块 30 (PTY-API) 30

程序模块 (PTY-API) 30 处理应用程序 40 (包括 ACS) 和硬件组件 10 之间的对话. 该模块还可记录事件, 并控制从操作数据库 O-DB 拣出/移动数据.

现在参看图 4, 图 4 中图示了与图 3 相同的四个数据库 (P-DB, O-D, A-DB, IAM-DB), 并图示了根据本发明各数据元素的处理是如何根据规则而受到控制的, 其中规则由存储在数据库 IAM-DB 中的数据元素保护目录中的保护属性描述.

该例中所要存储的数据涉及特定的个人信息, 且包括: (1) 一般可访问数据例如姓名和地址, (2) 标识信息, 例如个人代码序号 (Pcn), 和 (3) 描述信息 (DI). 一般性可访问数据姓名和地址与个人代码序号 (Pcn) 一起存储在开放数据库 P-DB 中, 由于信息的类型是一般可访问的, 因此所述存储作为明文是可执行的.

然而, 为了存储描述信息 DI 及标识信息, 需遵循以下步骤, 其中在以下步骤中下述标识被用来描述编码和解码算法. 一般地讲, 编码和解码算法可被描述如下:

$F_{类型}$(随机数, 输入数据)=结果

其中:

F 表示一函数.

类型 表示如下函数类型:

F_{KIR}=非可逆性编码算法;

F_{KR} =可逆性编码算法

F_{DKR}=解码算法

随机数

表示包括在函数 F 中的一个或多个常量和/或变量.

输入数据

为将被编码或解码的数据，和

结果

表示对于给定函数的一个唯一的函数值

步骤 1 信息的分离

标识信息从描述信息中分离出来;

步骤 2 准备存储标识 SID

根据标识信息选择出原始标识 OID．这里所选择的 OID 与个人的个人代码序号 PCn 等价．通过非可逆性编码算法 ALG1 OID 被编码成更新标识 UID，其中 ALG1 由硬件组件 10 随机地产生，算法如下:

ALG1： F_{KIR}（随机数， OID ）=UID

如此设计算法 ALG1 是为了在试图把 UID 解码成 OID 时可生成许多标识，从而不可能把特定的 UID 与相应的 OID 相链接.

然后通过可逆性算法 ALG2 UID 被编码成存储标识 SID，其中 ALG2 也由硬件组件 10 随机产生，算法如下:

ALG2： F_{KR}（随机数， UID ）=SID

如此设计算法 ALG2，是为了存在一个相应的解码算法 ALG3，通过 ALG3 可对 SID 进行解码以重建 UID．

如上述步骤 4 所述，当把编码后的数据元素值 DV 存储在操作数据库 O-DB 中时，则存储标识 SID 就会作为编码后的记录标识符.

步骤 3 生成编码后的数据元素值 DV

各个与原始标识 OID 相关的描述信息 DI 被转换成一个或多个与各数据元素类型 DT 相连的编码后的数据元素值 DV．

编码也通过如下描述的可逆性编码函数 F_{KR} 来实现，与上述算法 ALG1 和 ALG2 一样，编码也由硬件组件 10 随机生成．本发明与众不同之处在于发送给数据库 IAM-DB 中的数据元素保护目录的强制性调用从而自动地选择链接到数据元素类型上的保护属性，并且保护属性表示以何

种“强度”或程度对描述数据进行编码，以生成数据元素值 DV。

图 4 中的数据库 IAM-DB 下所图示的表，表示数据元素保护目录的示例性内容，在这里表示为 DC。作为例子，这里可假设保护函数 Func1 相应于“编码的程度”。如果待裁决的描述信息 DT 将作为与特定数据元素类型 DT1 相关的数据元素值存储在数据元素保护目录中，则在这种情况下记录在数据元素保护目录中的保护属性“5”将被自动的选出。待裁决的描述信息 DI 也将被自动并强制地使用强度“5”进行编码，以生成如下的编码后的数据元素值 DV：

F_{KR}（随机数，DI）=编码后的数据元素值 DV

要存储敏感性较弱的数据元素，例如数据元素类型为 DT3 的数据元素，则对于 IAM-DB 中的数据元素保护目录的强制性调用将导致选择保护属性“未”被选择，在这种情况下不会对待裁决的描述数据进行任何编码，从而描述数据可作为明文存储在操作数据库 ODB 中。

步骤 4 把记录存储在操作数据库 O-DB 中

根据步骤 2 所得的编码存储标识 SID，及根据步骤 3 所得的相应的编码后的数据元素值或数据元素值 DV 作为记录被存储在操作数据库 O-DB 中。

如上所述，所存储的信息记录 P 具有以下一般的形式：

	编码后的数据元素值的形式的描述信息			
存储标识（SID）	DV1	DV2	DV3	DV4

原始标识 OID 根据 PTY 原则经过两个步骤进行编码，步骤 1 是非-可逆的，步骤 2 是可逆的。因此不可能同时存储描述信息 DI 与永远不能链接到原始标识 OID 上的存储标识 SID，及生成“浮动”（随时间改变）的存储标识 SID 并可能为特定的初始标识 OID 定位相关的描述信息 DI。根据链接到每个单独数据元素上的保护属性来存储描述数据 DI。这就导致了更高级别的保护和建立规则的高度灵活性，以及敏感数据如何被允许使用和可被使用

的进一步适应，直到数据元素级。

为进一步提高保护的级别，数据元素保护目录 DC 最好根据 PTY 原则以编码后的形式存储在 IAM-DB 中，在这种情况下，例如图 4 中所图示的相应于上述存储标识的数据元素类型和相应于描述性信息或上述数据元素值的保护属性都以编码后的形式存储。这就有效地防止了每一个试图通过对数据元素保护目录中的内容进行未授权访问和解释而想绕过数据元素保护的企图。

在图示的实施例，PTY 可有如下功能:

- 保护以编码后的形式（SID）存储在操作数据库 O-DB 上的原始标识 OID（这一点从上述 WO95/15928 中可知）。

- 保护 IAM-DB 中的信息，尤其是数据元素保护目录中的保护属性和相关的记录标识符，和

- 保护相应数据元素类型的以编码后的数据元素值 DV 的形式存在的描述信息 DI，其中描述信息能得到在数据元素保护目录中所激活并对应于相应保护属性的保护。

功能性保护

在上述用于把数据输入到操作数据库 O-DB 中的处理的实施例中，只有“编码的程度”被作为数据元素保护目录 DC 中的数据元素保护属性进行了讨论。然而，这只是数据元素保护目录中的多个保护属性中的一个例子，其中数据元素保护目录一般为每个数据元素提供多个保护属性。以上的一般性描述中已表示了最佳的保护属性。

一个尤其有趣的保护属性是“被保护程序”。对于这种数据元素保护属性的使用表示数据系统可提供一种新类型的保护，这里称为“功能性保护”，并且其表示在数据处理的系统中只允许使用和可使用已被承认或证实的程序。应当指出的是，根据本发明，这类保护依然是在数据元素级。

为了图示方便，现在假设图 4 中的数据元素保护目录 DC 中的 Func2 对应于这一保护属性，并且数据元素类型分别为 DT1 和 DT2 的数据元素只允许由各自所承认的应用程序或程序 P1 和 P2 进行处理。则应当防止通过例如一个不同的程序 P3，或 P1 的升级版本 P1'来实现对相应数据元

素的未授权处理的情况. 象数据元素保护目录中的保护属性一样, 也需存储标识 P1 和 P2 的数据. 在一个最佳例子中, 基于各自所承认的程序 P1 和 P2, 以本质上已知构成的方式, 建立相应的编码检验和 $P1^*$ 和 $P2^*$. 可认为这些检验和构成所承认程序的唯一指纹, 并且这些指纹可作为保护属性存储在图 4 中所图示的数据元素保护目录中. 然而, 应当指出, 这些所承认程序的检验和也可存储在它们自己的用于记录所承认程序的数据元素保护目录中, 从而从具有编码强度保护属性的数据元素保护目录分离开来.

如果使用了最近提及的保护类型“被保护程序”, 则应当指出, 与目的在于处理给定数据元素的用户-激活措施相关的系统不需对系统所承认的所有程序进行完全检查, 该措施例如是把一新数据元素值输入到一特定记录中. 如果, 例如, 用户试图使用程序 P3, 以把新数据元素值输入到操作数据库 O-DB 中, 则一个强制性调用就被送到与相应的数据元素类型例如 DT1 相关的数据元素保护目录. 然后, 从数据元素保护目录中选择相关的保护属性 $P1^*$, 即这种数据元素值只允许由程序 P1 来存储. 则试图通过程序 P3 来记录数据元素值的企图将失败.

通过定期使用上述功能性保护, 可揭露和/或防止未授权个人(例如“黑客”)通过未承认程序闯入系统并修改和/或添加描述数据以识别记录. 从而不允许识别在操作数据库 O-DB 中的数据元素值.

可跟踪性/事件记录

“事件记录”或“可跟踪性”是根据本发明的另一种保护类型, 该保护类型可与数据元素保护目录中的数据元素类型相连. 如果这种保护因某一数据元素类型而被激活, 则对每个操作数据库 O-DB 中的相应数据元素值的处理将自动, 强制地生成以一种适当的方式所记录的有关处理的信息(“用户”, “日期”, “记录”, “用户程序”等), 使得有可能在以后根据所记录的信息去调查谁处理了所讨论的数据元素值, 什么时候, 通过那个程序等.

从操作数据库 O-DB 读取数据

为实现用户-激活措施需执行以下步骤, 其中用户-激活措施的目的在

于从存储在操作数据库 O-DB 中的记录中读取/修改数据元素值，其中在以下步骤中还包括对于数据元素保护目录的强制性调用和对数据的“拆包”，其中数据由所选择的保护属性自动并强制地进行控制。

步骤 1 通过根据与将要读取的数据元素值 DV 相关的原始标识 OID，（ Pcn ）来生成存储标识 SID，则记录就会被识别。

F_{KR}（ F_{KIR}（ OID ））=SID

步骤 2 当通过 SID 找到记录后，则通过下述解码算法 F_{DKR} 对编码后的数据元素值 DV（即将要读取的编码后的描述数据）进行解码:

F_{DKR}（ DV ）=描述数据（明文）

然而，要执行对数据元素值的解码，则要求首先应当由系统把数据元素的编码控制保护属性从数据元素保护目录 DC 中选择出来，即编码控制保护属性表示以何种强度或何种层次对存储在 O-DB 中的数据元素值 DV 进行编码的属性。如同上述的用于把数据输入到 O-DB 中的程序，当读取数据时，一强制性调用也被送到数据元素保护目录 DC，以选择执行处理所必需的信息，这里的处理指拆包。应当理解，当试图读取时，对于数据元素保护目录的强制性调用可能会造成完全或部分的读取失败，根据与将读取的数据元素值相连的保护属性，这里有几个原因。例如，由于用户试图使用未承认程序和/或由于用户未被授权读取有关项，从而使读取被中断。

如果数据元素保护目录被编码，则解码关键字可存储在从第一和第二数据库分离出的存储区域中。

图 5 表示对话框形式的用户接口的例子，通过该对话框负责 IAM 的人，即负责安全的人可读取和/或修改在数据元素保护目录中所描述的保护属性。在图 5 的例子中，数据元素类型“房屋津贴”和“社会津贴”均被提供以有关编码，搜寻，记录和用户的保护属性。而且，授权用户和与数据元素类型“社会津贴”相连的被保护程序的登录在子菜单中进行。

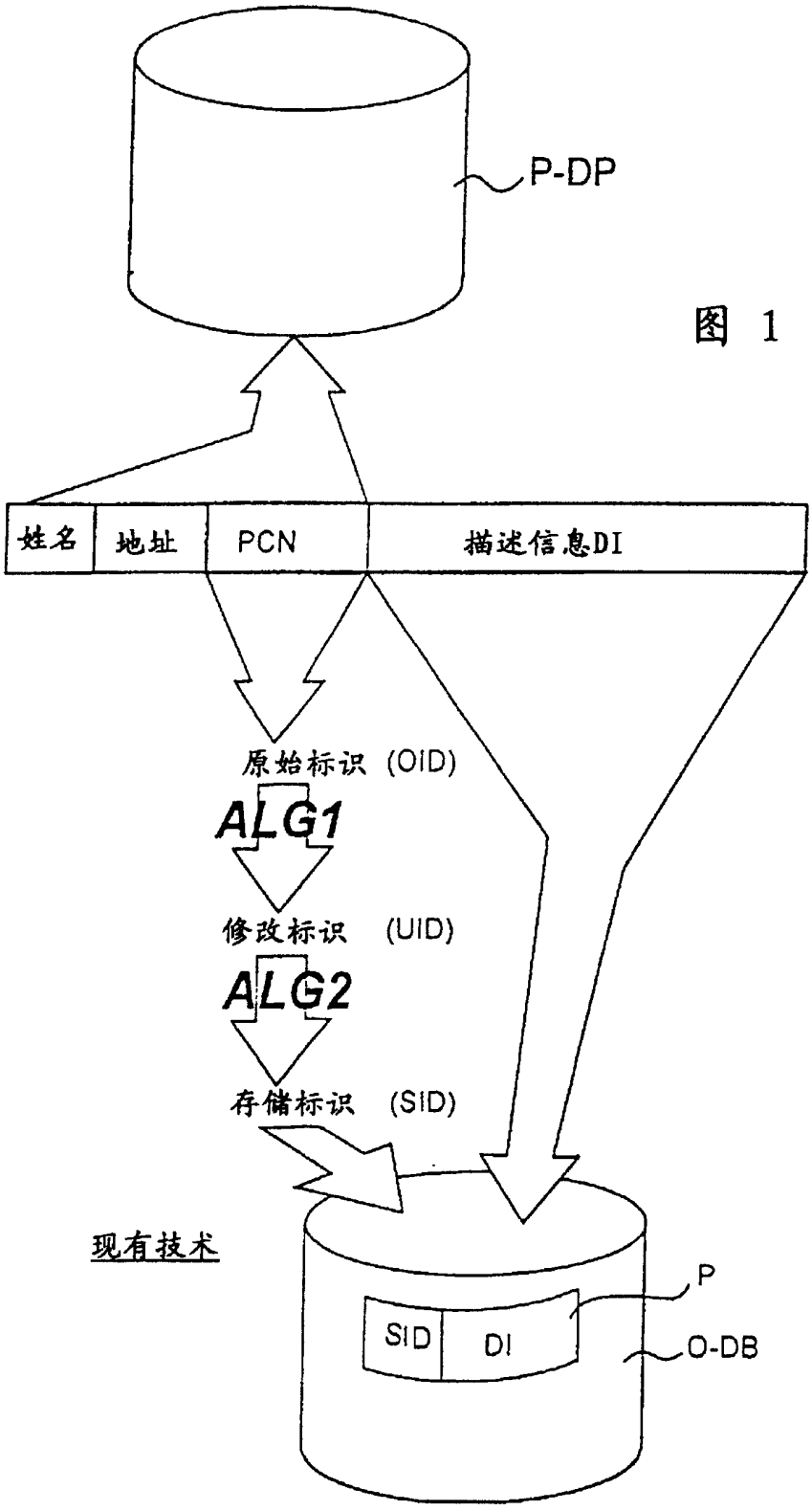

P-DP
姓名
地址
PCN
描述信息DI
原始标识 (OID)
ALG1
修改标识 (UID)
ALG2
存储标识 (SID)
现有技术
P
SID
DI
O-DB

图 1

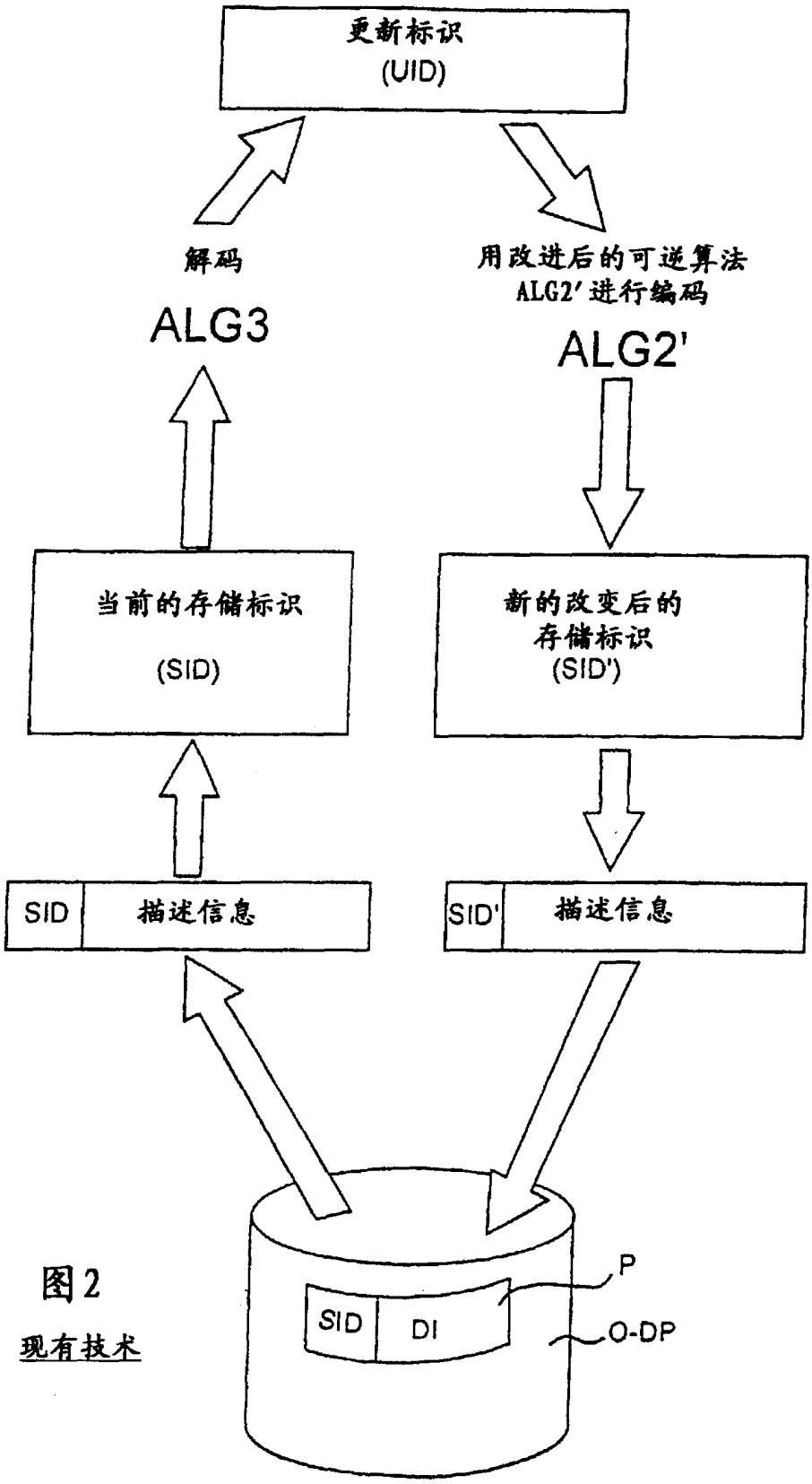

更新标识
(UID)
解码
ALG3
用改进后的可逆算法
ALG2′进行编码
ALG2'
当前的存储标识
(SID)
新的改变后的
存储标识
(SID')
SID
描述信息
SID'
描述信息
SID
DI
P
O-DP

图2

现有技术

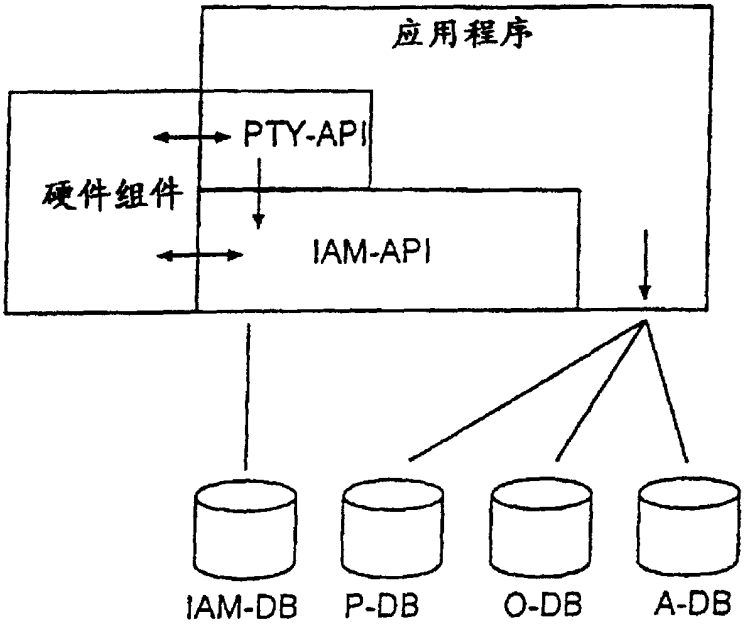

应用程序
PTY-API
硬件组件
IAM-API
IAM-DB
P-DB
O-DB
A-DB

图 3

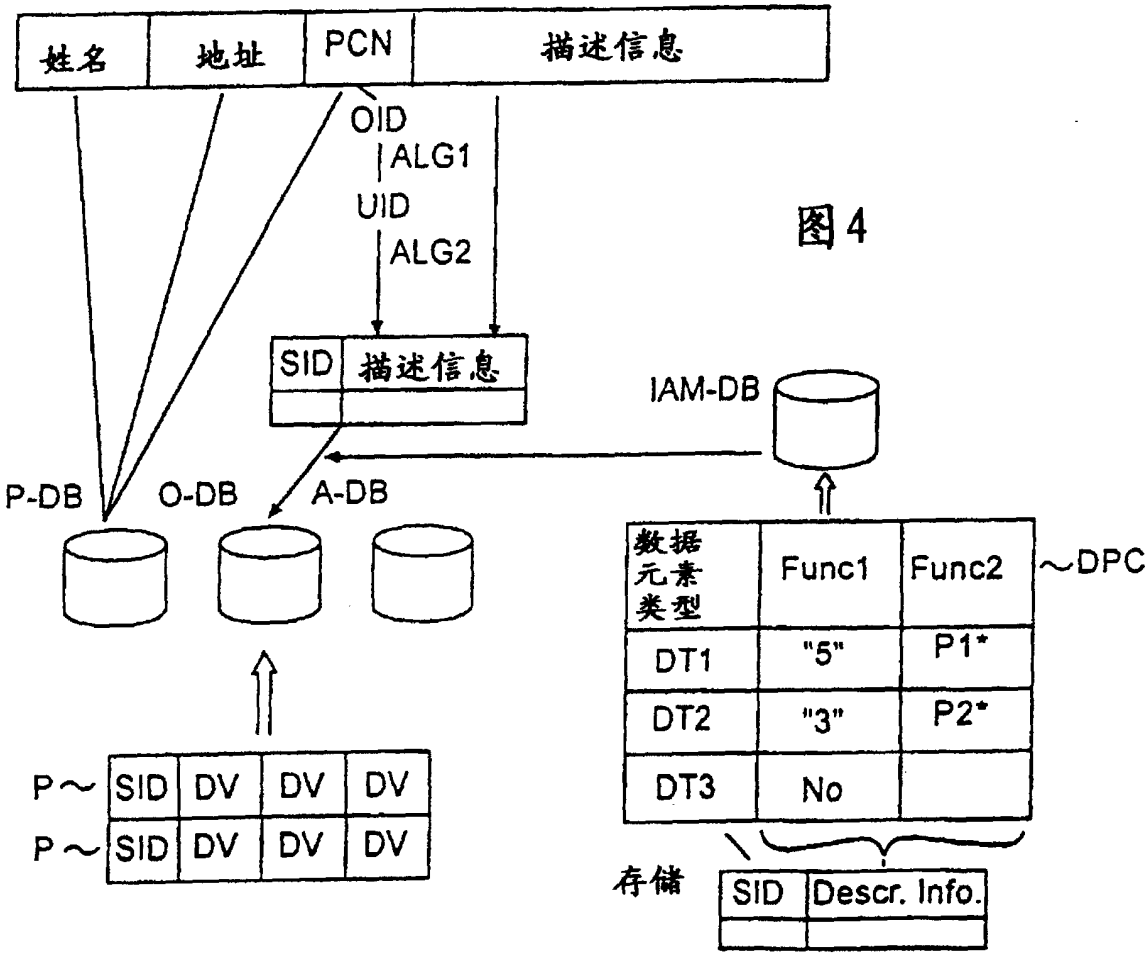

姓名
地址
PCN
描述信息
OID
ALG1
UID
ALG2
SID
描述信息
IAM-DB
P-DB
O-DB
A-DB
数据元素类型
Func1
Func2
~DPC
DT1
"5"
P1*
DT2
"3"
P2*
DT3
No
P~
SID
DV
DV
DV
P~
SID
DV
DV
DV
存储
SID
Descr. Info.

图 4

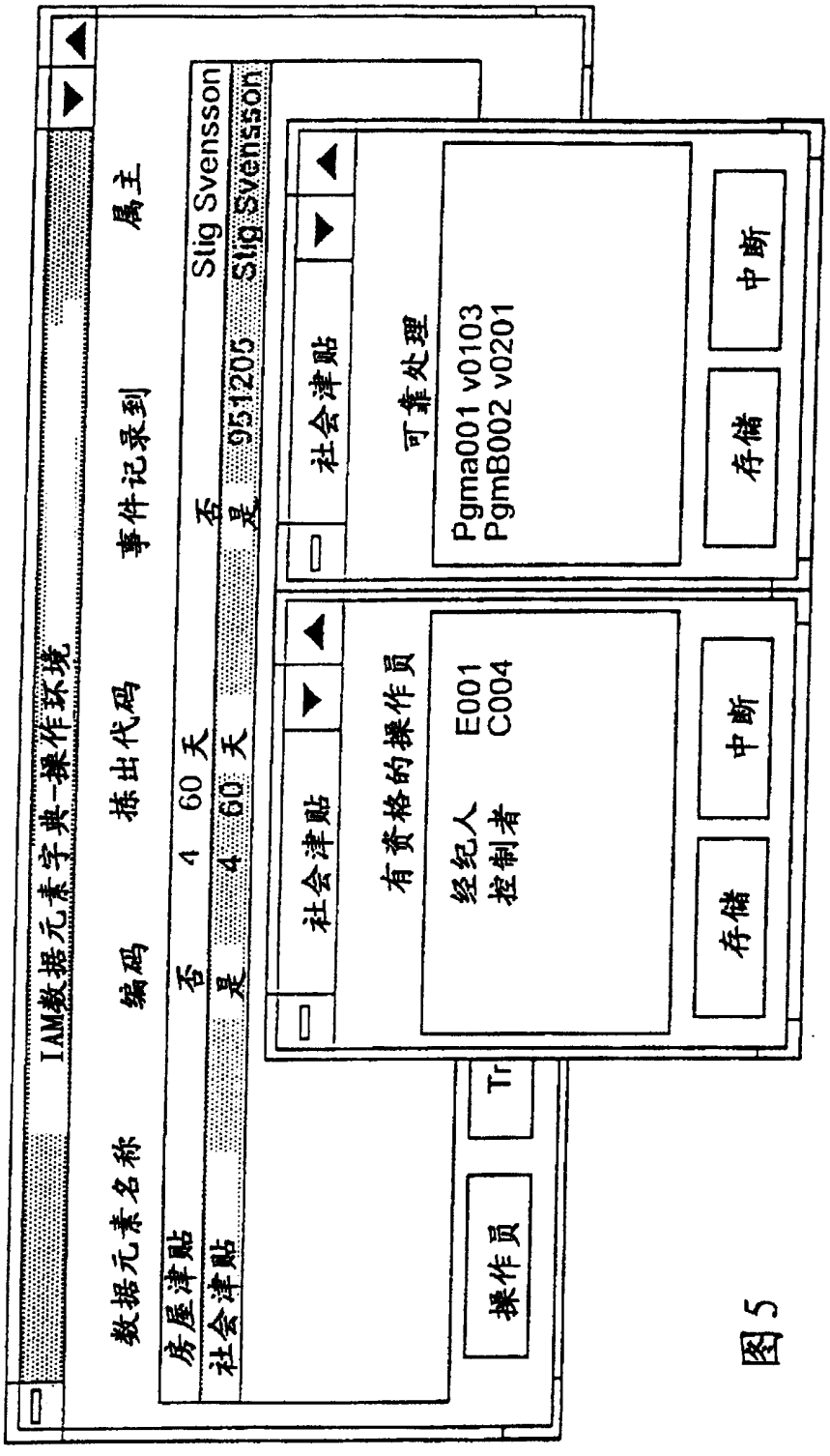

IAM数据元素字典-操作环境
数据元素名称
编码
拣出代码
事件记录到
属主
房屋津贴
否
4
60 天
否
Stig Svensson
社会津贴
是
4
60 天
是
951205
Stig Svensson
操作员
Tr
社会津贴
有资格的操作员
经纪人 E001
控制者 C004
存储
中断
社会津贴
可靠处理
Pgma001 v0103
PgmB002 v0201
存储
中断

图 5