(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111597535 B
(45)授权公告日 2023.07.18

(21)申请号 202010425693.4
(22)申请日 2016.05.02
(65)同一申请的已公布的文献号
申请公布号 CN 111597535 A
(43)申请公布日 2020.08.28
(30)优先权数据
2015-093729 2015.04.30 JP
(62)分案原申请数据
201680038418.9 2016.05.02
(73)专利权人 德山真旭
地址 日本东京
(72)发明人 德山真旭
(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
专利代理师 宋融冰
(51)Int.Cl.
G06F 21/32(2013.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)
H04L 9/08(2006.01)
H04L 9/14(2006.01)
(56)对比文件
CN 102415049 A,2012.04.11
CN 103455764 A,2013.12.18
CN 103354925 A,2013.10.16
审查员 于彬

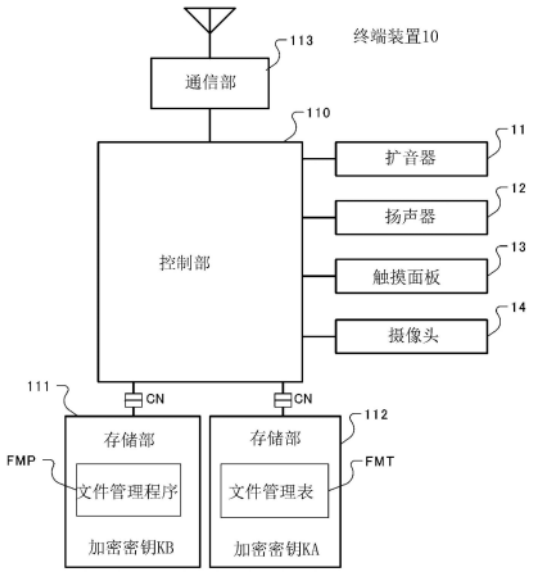
权利要求书2页 说明书11页 附图17页

(54)发明名称

终端装置及存储介质

(57)摘要

本申请提供一种终端装置及存储介质，其中，如果指定保存对象的文件，则控制部(110)通过执行文件管理程序，从而将保存对象的文件分割，利用与分割文件的逻辑地址对应的加密密钥进行加密，并保存于与逻辑地址对应的存储目的地中，生成将逻辑地址、加密密钥、以及保存目的地物理地址对应的表。如果指定读取对象文件，则控制部(110)从理论地址中确定对应的分割文件，参照表确定分割文件的保存目的地的物理地址和加密密钥，并从确定的物理地址中读取分割文件，利用确定的加密密钥进行解码。



CN 111597535 B

1.一种终端装置,其特征在于,具备:

分割单元,其将保存对象的文件分割,并生成分割文件;

选择单元,其选择多个加密方法和多个存储目的地中的各一个;

保存单元,其利用所述选择单元所选择的加密方法,对所述分割单元所生成的分割文件加密,并将所述加密的分割文件保存于所述选择单元所选择的存储目的地中;

对应单元,其将确定所述分割文件的信息、所述加密方法、以及保存目的地的地址相对应;以及

获取单元,其获取生物体信息,

所述选择单元基于所述获取单元所获取的生物体信息,选择多个加密方法中的一个,或所述选择单元基于所述获取单元所获取的生物体信息,选择多个存储目的地中的一个。

2.根据权利要求1所述的终端装置,其特征在于,

在所述生物体信息中包含多个种类的生物体信息,

所述选择单元根据所述多个种类的生物体信息分别选择所述加密方法,

所述保存单元使用所述选择单元所选择的加密方法加密所述分割文件。

3.根据权利要求1或2所述的终端装置,其特征在于,

所述选择单元基于所述获取单元所获取的生物体信息,从多个加密密钥或加密算法中选择一个。

4.根据权利要求1或2所述的终端装置,其特征在于,

所述选择单元基于所述获取单元所获取的生物体信息,选择键盘数据的配置位置,

所述分割单元为了使得分割后的数据为预定大小,在所述选择单元所选择的位置配置键盘数据。

5.根据权利要求1或2所述的终端装置,其特征在于,

所述选择单元基于所述获取单元所获取的生物体信息,选择分割文件的存储目的地,

所述保存单元将分割文件存储于所述选择单元所选择的存储目的地中。

6.根据权利要求1或2所述的终端装置,其特征在于,

所述保存单元将所述加密的分割文件与所述对应单元保存于不同的存储目的地中。

7.根据权利要求1或2所述的终端装置,其特征在于,

所述终端装置还包括:

分割文件确定单元,其确定与读取对象文件对应的所述分割文件;

确定单元,其参照所述对应单元确定所述分割文件的保存目的地的地址和所述加密方法;以及

再生单元,其从所述确定单元所确定的地址中读取所述分割文件,并根据确定的所述加密方法进行解码。

8.根据权利要求1或2所述的终端装置,其特征在于,

所述分割文件由一个簇的数据构成。

9.根据权利要求1或2所述的终端装置,其特征在于,

所述多个存储目的地的至少一个能够拆装地安装。

10.根据权利要求1或2所述的终端装置,其特征在于,

所述多个存储目的地的至少一个配置于云上。

11.一种存储介质,其特征在于,其存储有计算机程序,

所述计算机程序用于使计算机作为权利要求1所述的终端装置发挥功能。

终端装置及存储介质

[0001] 本申请为2017年12月28日提交的申请号为201680038418.9且发明名称为“终端装置及计算机程序”的专利申请的分案申请。

技术领域

[0002] 本发明涉及具有数据加密功能的终端装置及存储介质。

背景技术

[0003] 数据的安全的要求正在提高。为了保持安全，提出了各种方案(例如，参照专利文献1)。专利文献1公开了将保存的数据双重加密地进行保护。

[0004] 现有技术文献

[0005] 专利文献

[0006] 专利文献1:日本特开2015-1800号公报

发明内容

[0007] 发明要解决的问题

[0008] 专利文献1中所记载的技术是，如果密钥泄露，则全部的信息能够再生。

[0009] 本发明的目的在于提供一种终端装置，其能够更安全地保护数据。

[0010] 用于解决问题的方案

[0011] 为了解决上述问题，本发明所涉及的终端装置具备：

[0012] 分割单元，其将保存对象的文件分割，并生成分割文件；

[0013] 选择单元，其选择多个加密方法和多个存储目的地中的各一个；

[0014] 保存单元，其利用所述选择单元所选择的加密方法，对所述分割单元所生成的分割文件加密，并将所述加密的分割文件保存于所述选择单元所选择的物理性的存储目的地中；以及

[0015] 表，其将确定所述分割文件的信息、所述加密方法、以及保存目的地的物理地址对应地进行存储。

[0016] 所述保存单元还可以构成为：将确定所述加密方法的信息保存于所述物理性的存储目的地中，并将所述分割单元所生成的分割文件和确定对该分割文件加密的加密方法的信息保存于不同的存储目的地中。

[0017] 而且，所述终端装置还可以具备：例如，

[0018] 获取单元，其获取用户的生物体信息；以及

[0019] 分割大小设定单元，其根据转换信息，得到所述分割文件的大小，所述转换信息是将所述获取单元所获取的生物体信息转换为该分割文件的大小的信息，

[0020] 所述分割单元生成所述分割大小设定单元所得到的大小的分割文件。

[0021] 所述终端装置可以构成为：

[0022] 在所述生物体信息中包含多个种类的生物体信息，

[0023] 所述分割大小设定单元按照每个所述多个种类的生物体信息，根据所述转换信息得到所述分割文件的大小，

[0024] 所述分割单元将所述保存对象的文件分割，并生成所述分割大小设定单元所得到的大小中的一个或多个分割文件。

[0025] 所述终端装置可以构成为：

[0026] 所述分割大小设定单元是将基于用户的生物体信息的条件和分割文件的大小对应地进行存储的分割大小表，

[0027] 所述选择单元根据所述获取单元所获取的生物体信息，从所述分割大小表中进一步选择所述分割文件的大小，

[0028] 所述分割单元生成所述选择单元所选择的大小的分割文件。

[0029] 所述终端装置可以构成为：

[0030] 还具备：

[0031] 获取单元，其用于获取用户的生物体信息；以及

[0032] 制作单元，其根据所述获取单元获取的生物体信息制作加密密钥，

[0033] 所述保存单元利用所述制作单元所制作的加密密钥加密所述分割文件。

[0034] 所述终端装置可以构成为：

[0035] 在所述生物体信息中包含多个种类的生物体信息，

[0036] 所述制作单元根据所述多个种类的生物体信息分别制作所述加密密钥，

[0037] 所述保存单元使用所述制作单元所分别制作的加密密钥中的一个或多个加密密钥，加密所述分割文件。

[0038] 另外，所述终端装置也可以构成为：

[0039] 还具备：例如，

[0040] 分割文件确定单元，其确定与读取对象文件对应的所述分割文件；

[0041] 确定单元，其参照所述表确定所述分割文件的保存目的地的物理地址和所述加密方法；以及

[0042] 再生单元，其从所述确定单元所确定的物理地址中读取所述分割文件，并根据确定的所述加密方法进行解码。

[0043] 所述分割文件例如由一个簇的数据构成。

[0044] 优选所述多个存储目的地的至少一个能够拆装地安装。

[0045] 或者，优选所述多个存储目的地的至少一个配置于云上。

[0046] 用于使计算机作为上述终端装置发挥功能的计算机程序也包含在发明内。

[0047] 发明效果

[0048] 根据本发明，由于按照每个分割数据更改加密方法和保存目的地，因此解码变得更加困难。由此，能够更安全地保护数据。另一方面，处理负担小。

附图说明

[0049] 图1是本发明的实施方式1所涉及的终端装置的框图。

[0050] 图2A是说明图1的终端装置执行的文件的分割的图。

[0051] 图2B是说明根据实施方式1所涉及的簇的构成的图。

[0052] 图2C是用于说明图1的终端装置执行的加密处理的图。

[0053] 图2D是表示文件管理表的构成例的图。

[0054] 图3是图1的终端装置执行的文件存储处理的流程图。

[0055] 图4是图1的终端装置执行的文件再生处理的流程图。

[0056] 图5是表示电话簿文件的构成例的图。

[0057] 图6是表示日程文件的构成例的图。

[0058] 图7是实施方式1所涉及的终端装置等的变形例的框图。

[0059] 图8是本发明的实施方式2所涉及的终端装置等的框图。

[0060] 图9是表示实施方式2所涉及的文件管理表的示例的图。

[0061] 图10是表示根据实施方式2的分割大小表的示例的图。

[0062] 图11是图8所示的终端装置执行的文件存储处理的流程图。

[0063] 图12是表示图11所示的文件分割处理和加密处理的具体示例的流程图。

[0064] 图13是表示图11所示的分散存储处理的具体示例的流程图。

[0065] 图14是表示图11所示的文件存储处理的实例的图。

[0066] 图15是例示一个扇区的构成的图。

[0067] 图16是表示用于根据生物体信息更改加密密钥的加密密钥表的示例的图。

[0068] 图17A是表示用于根据生物体信息更改存储目的地的存储目的地表的示例的图。

[0069] 图17B是表示用于根据生物体信息更改存储目的地的存储目的地表的其他示例的图。

[0070] 图18A是表示用于根据生物体信息更改加密所使用的生物体信息的生物体信息选择表的示例的图。

[0071] 图18B是表示用于根据生物体信息更改加密所使用的生物体信息的生物体信息选择表的其他示例的图。

[0072] 图19是表示用于根据生物体信息更改键盘数据的位置的键盘数据位置选择表的示例的图。

[0073] 图20A是例示根据图19的键盘数据位置选择表而实现的一个扇区的构成的图。

[0074] 图20B是例示根据图19的键盘数据位置选择表而实现的一个扇区的构成的其他图。

具体实施方式

[0075] (实施方式1)

[0076] 下面参照附图,对本发明的实施方式1所涉及的终端装置进行说明。

[0077] 本实施方式的终端装置10是所谓的智能手机,具有将数据加密且分散保存的功能。

[0078] 如图1所示,终端装置10具备:控制部110、以及与控制部110连接的扩音器11、扬声器12、触摸面板13、摄像头14、存储部111、112、通信部113。

[0079] 扩音器11是利用语音通话拾取用户的声音的装置。扬声器12利用语音通话输出接收的声音。触摸面板13由触摸传感器和显示装置叠层而构成。触摸传感器判别用户的操作位置。显示装置按照控制部110的控制显示各种信息。

[0080] 摄像头14配置于终端装置10的正面，拍摄被摄体。

[0081] 控制部110由处理器、RAM(Random Access Memory)等构成，执行存储于存储部111、112的应用程序。应用程序包括文件管理程序、邮件程序、日程管理程序等。控制部110通过执行文件管理程序，将各种文件(数据)分散且加密地保存，并从多个位置读取数据，将原始数据解码。

[0082] 存储部111和112是作为辅助存储装置利用的非易失性存储器，由闪速存储器等构成。存储部111中存储有文件管理程序FMP，存储部112中存储有文件分配表(文件管理表)FMT。而且，存储部111、112将所谓的电话簿数据、日程数据等机密性高的信息分散地存储。而且，存储部111、112分别可拆装地与终端装置10连接。具体而言，存储部111、112安装在形成于终端装置10的壳体上的槽等内，并通过连接器CN与控制部110连接。

[0083] 通信部113按照控制部110的控制，与基站、附近的接入点之间进行无线通信，进行语音通话、邮件通信、数据通信等。

[0084] 接下来，参照图2对控制部110通过执行文件管理程序FMP而执行的文件存储处理进行说明。

[0085] 如图2A所示，一个文件被分割为簇，所述簇是计算机的桌面访问的最小单位。一个簇中所包含的扇区的数量是任意的，但在以下的说明中，如图2B所示，设为8个。在本实施方式中，将一个扇区设为512字节。因此，一个簇具有4,096字节(约4K字节)的大小。

[0086] 应用程序利用逻辑地址来管理扇区和簇。

[0087] 簇由n比特的逻辑地址的上位n-3比特指定。簇内的各扇区由逻辑地址的下位3比特指定。

[0088] 在以下的说明中，关于簇的逻辑地址是指n比特的逻辑地址整体的上位(n-3)比特。

[0089] 存储于存储部111中的文件管理程序FMP在将文件存储于存储部时，如图2C所示，对分配有奇数的逻辑地址((n-3)比特)的簇(以下称为奇数逻辑地址簇)和分配有偶数的逻辑地址的簇(以下称为偶数逻辑地址簇)进行不同的处理。

[0090] 首先，文件管理程序FMP对分配有奇数逻辑地址的簇进行基于加密密钥KA的加密处理，并存储于存储部111上的任意的物理地址PA中。加密密钥KA存储于存储部112上。另一方面，文件管理程序FMP对分配有偶数逻辑地址的簇进行基于加密密钥KB的加密处理，并存储于存储部112上的任意的物理地址PB中。加密密钥PB存储于存储部111上。

[0091] 文件管理程序FMP在进行了上述处理后，生成如图2D所示的文件管理表FMT。这表示由逻辑地址Li确定的簇存储于物理地址PAi(或PBi)中，并利用密钥KA(或KB)加密。文件管理表存储于控制部110内。另外，从逻辑地址Li中确定密钥，因此可以不存储密钥KA或KB。

[0092] 接下来，对如上所述，加密并分散地存储的文件的再生的处理进行说明。

[0093] 文件管理程序FMP如果接受到从应用程序发送的访问文件的请求，则求出构成访问对象的文件的簇的逻辑地址(如前文所述，n-3比特)。

[0094] 文件管理程序FMP如果接收到从应用程序发送的访问文件的请求，则求出构成访问对象的文件的第一个簇的逻辑地址。访问的请求包含例如第一个扇区的逻辑地址。文件管理程序FMP从第一个扇区的逻辑地址求出第一个簇的逻辑地址。文件管理程序FMP如果确定了第一个簇的逻辑地址，则参照文件管理表FMT，求出对应的物理地址，进而确定加密密

钥。接下来，文件管理程序FMP从对应的物理地址中读取数据，使用确定的加密密钥进行编码，并发送至应用。

[0095] 文件管理程序FMP如果在后续的簇中执行同样的动作，将全部的簇解码，并发送至应用程序，则处理结束。

[0096] 接下来，参照图3所示的流程图对控制部110所进行的文件存储处理进行说明。首先，如果应用程序请求保存文件，则控制部110开始图3所示的文件存储处理。

[0097] 首先，控制部110执行文件管理程序FMP，确定构成保存对象的文件的第一个簇的逻辑地址Li，并判别其为奇数还是偶数(步骤S11)。如果逻辑地址Li为奇数(步骤S11:是)，则如图2C所示，利用加密密钥KA将处理对象的簇加密(步骤S12)。控制部110将加密的簇存储于存储部111上的空闲区域中(步骤S13)。

[0098] 接着，如图2D所示，控制部110将处理的簇的逻辑地址Li、存储的区域的物理地址PAi、以及加密密钥KA对应地注册于文件管理表FMT中(步骤S14)。

[0099] 接着，控制部110判别文件的保存是否结束(步骤S15)，如果未结束(步骤S15:否)，则将逻辑地址Li进行+1(步骤S18)。接着，处理返回至步骤S11，处理下一个簇。

[0100] 另一方面，在步骤S11中，如果判别处理对象的簇的逻辑地址为偶数(步骤S11:否)，则如图2C所示，利用加密密钥KB将处理对象的簇加密(步骤S16)。控制部110将加密的簇存储于存储部112上的空闲区域中(步骤S17)。

[0101] 接着，如图2D所示，控制部110将处理的簇的逻辑地址Li、存储的区域的物理地址PBi、以及加密密钥KB对应地注册于文件管理表FMT中(步骤S14)。

[0102] 接着，控制部110判别文件的保存是否结束(步骤S15)，如果未结束(步骤S15:否)，则将逻辑地址Li进行+1(步骤S18)。接着，处理返回至步骤S11，处理下一个簇。

[0103] 在步骤S15中，如果判别文件的保存结束(步骤S15:是)，则文件存储处理结束。

[0104] 接下来，参照图4所示的流程图，对控制部110所进行的文件再生处理进行说明。如果应用程序请求读取文件，则控制部110开始图4所示的文件再生处理。

[0105] 另外，从应用中例如以构成文件的第一个扇区的逻辑地址和数据量的形式确定读取对象。

[0106] 首先，控制部110求出第一个簇的逻辑地址，参照文件管理表FMT，确定将处理对象的簇加密的加密密钥和存储位置的物理地址(步骤S21)。

[0107] 接下来，控制部110从在步骤S21中确定的物理地址中读取簇(步骤S22)。接下来，控制部110利用在步骤S21中确定的加密密钥将读取的簇解码(步骤S23)，并发送至应用程序。

[0108] 接着，判别文件的读取是否结束(步骤S24)，如果未结束(步骤S24:否)，则返回至步骤S21，对下一个簇继续进行同样的文件再生处理。

[0109] 在步骤S24中，如果判别文件的读取结束(步骤S24:是)，则文件再生处理结束。

[0110] 根据这样的构成，一个文件分散地存储于存储部111和112中。而且，存储于存储部111中的簇利用加密密钥KA加密，加密密钥KA存储于存储部112中。另外，存储于存储部112中的簇利用加密密钥KB加密，该加密密钥KB存储于存储部111中。因此，即使一方的存储部111或112的数据泄露到外部，数据的复原也困难。

[0111] 另外，由于文件管理程序FMP自动地进行加密处理，因此控制负担小。

[0112] 由此，即使将如图5所示的所谓的地址簿、如图6所例示的日程数据等保存于终端装置10内，信息泄露的危险也小。

[0113] 另外，本发明不限定于上述实施方式，能进行各种变形及应用。例如，在上述实施方式中，将存储部111和112设为可拆装，可以设为仅一方可拆装，也可以设为两方固定。

[0114] 另外，示出了将数据分割地存储于两个存储部111、112中的示例，但是存储部的数量是任意的。另外，分割数也是任意的。加密密钥的数量也是任意的。

[0115] 利用簇单位确定存储目的地和加密密钥，但以何种大小为单位是任意的，考虑处理负担和安全性而设定。

[0116] 而且，也可以使数据(分割文件)的存储目的地为通过网络连接的外部的服务器、数据库等。

[0117] 示出了通过使加密密钥不同而更改加密方法的示例，但也可以使加密算法自身不同。

[0118] 另外，如图7所示，也可以将文件管理表FMT存储于控制部110内的闪速存储器等非易失性存储器中。

[0119] 另外，如图7所示，也可以通过网络NW将存储部111和112配置于外部装置中。

[0120] 在上述实施方式中，将加密所使用的加密密钥设为两个，但也可以设为三个以上。另外，将文件的存储位置设为两个，但也可以设为三个以上。例如，在将加密密钥的数量设为M(3以上的整数)个、存储位置设为N(3以上的整数)个的情况下，控制部110将簇的逻辑地址除以M(3以上的整数)，并利用由其余数mod(M)确定的加密密钥将簇加密，将簇的逻辑地址除以N(3以上的整数)，将加密的簇存储在由其余数mod(N)所确定的存储位置。控制部110将簇的逻辑地址、加密密钥以及存储位置的物理地址对应地存储于文件管理表FMT中。另外，由于能够从逻辑地址中确定加密密钥，因此也可以省略加密密钥。

[0121] (实施方式2)

[0122] 接下来，参照附图对根据本发明的实施方式2的终端装置进行说明。

[0123] 在实施方式2中提供一种终端装置，其根据用户以不同的方式分散地保存文件，由此不给用户带来负担，并安全地保存数据。另外，对与实施方式1所涉及的终端装置具备的构成同等的构成标以相同的附图标记。

[0124] 如图8所示，本实施方式的终端装置10A通过网络与云CL上的存储装置210、220连接。终端装置10A具有下述功能：获取用户的生物体信息，并根据该生物体信息将文件FI分割、加密，并发送至存储装置210、220。另外，在本实施方式中，作为生物体信息，以指纹、声纹、虹膜为例进行说明。

[0125] 终端装置10A具备：控制部110、以及与控制部110连接的扩音器11、扬声器12、触摸面板13、摄像头14、存储部111、通信部113。

[0126] 扩音器11拾取用户的声音，发送至控制部110。扬声器12按照控制部110的指示向用户提供基于声音的信息。触摸面板13通过触摸传感器获取用户的指纹，并发送至控制部110。摄像头14按照控制部110的指示，获取用户的虹膜画像，并发送至控制部110。

[0127] 控制部110由处理器、RAM(Random Access Memory)等构成，执行存储于存储部111的应用程序和文件管理程序FMP。

[0128] 控制部110通过执行文件管理程序FMP，从而获取用户的生物体信息，并根据该生

物体信息将各种文件FI分割且加密，并发送至存储装置210、220以进行保存。另外，控制部110通过执行文件管理程序FMP，从而获取用户的生物体信息，并根据该生物体信息从存储装置210、220读取数据，并将原始数据解码。

[0129] 在存储部111中，除了文件管理程序FMP、文件管理表FMT以外，还存储有分割大小表DST和加密密钥KF、KV、KI。

[0130] 如图9所示，本实施方式中的文件管理表FMT包括数据管理表DMT和簇管理表CMT。

[0131] 数据管理表DMT将保存对象的文件FI分割而得到的数据的数据编号i、加密后大小、以及加密所使用的加密密钥对应地进行存储。

[0132] 另一方面，簇管理表CMT将簇编号j、存储目的地的物理地址、以及该簇中包含的数据的数据编号i对应地进行存储。

[0133] 存储于存储部111中的分割大小表DST是存储规定分割存储对象的文件FI的大小的信息的表。在本实施方式中，分割大小根据用户的生物体信息而发生变化。因此，如图10所示，分割大小表DST将生物体信息、该生物体信息应满足的条件、满足该条件时选择的分割大小相对应。

[0134] 在图10所示的分割大小表DST中，对于指纹信息而言，设定指纹的端点的数量与分支点的数量的大小关系作为条件，对于声纹信息而言，设定音量最大的频率f_{top}与第二大的频率f_{second}的大小关系作为条件，对于虹膜信息，设定虹膜编码中的1的数量N_1与0的数量N_0大小关系作为条件。

[0135] 如图8所示的通信部113与云CL上的存储装置210、220进行通信。

[0136] 接下来，参照图11～14对控制部110通过执行文件管理程序FMP而执行的文件存储处理进行说明，

[0137] 本实施方式中的文件存储处理是将文件FI分割为基于用户的生物体信息的大小的数据，并根据该生物体信息将分割的文件FI进行加密、分散并保存的处理。

[0138] 如果用户或应用软件请求保存文件FI，则控制部110开始如图11所示的文件FI存储处理。

[0139] 首先，控制部110向用户请求输入生物体信息(指纹信息、声纹信息、虹膜信息)(步骤S10)。具体而言，控制部110在触摸面板13的显示装置上显示如下内容，指示将手指肚放在触摸传感器上、向扩音器11发出预定的语言、注视摄像头14等。

[0140] 接着，控制部110指示分别向触摸面板13、扩音器11、摄像头14获取生物体信息，并判断是否获取到这些生物体信息(步骤S20)。控制部110为待机状态，直至获取到请求的全部生物体信息为止(步骤S20;否)。另一方面，如果控制部110判断获取到请求的全部生物体信息(步骤S20;是)，则从获取的生物体信息中提取这些特征信息(步骤S30)。

[0141] 控制部110例如提取指纹中所含的端点与分支点的各自的位置作为指纹信息的特征信息。另外，控制部110提取声音频谱上音量为峰的频率和基于该音量的位次作为声纹信息的特征信息。另外，控制部110提取虹膜编码作为虹膜信息的特征信息。

[0142] 控制部110如果从生物体信息中提取特征信息，则执行分割保存对象文件FI的文件分割处理(步骤S40)，并执行将分割的文件FI(数据)分别加密的加密处理(步骤S50)，进而结束将加密的分割文件FI分散地存储于存储部210、220的分割存储处理(步骤S60)。

[0143] 接下来，参照图12～14对在文件存储处理中执行的文件分割处理(步骤S40)～分

散存储处理(步骤S60)进行说明。

[0144] 首先,使用图14所示的分割由“ABCDEFGHIJKL”的文本信息构成的文件FI的示例,对文件分割处理的概要进行说明。

[0145] 控制部110在文件分割处理中,将构成文件FI的数据分割成由生物体信息确定的大小的数据。例如,日语的平假名和汉字在UTF-8(Unicode Transformation Format-8)中,一个文字由三个字节表示。在图14所示的示例中,假设“ABCDEFGHTIJKL”的各文字由三个字节表示。在此,控制部110将文件FI从开头按照生物体信息分割成包含7字节、9字节、4字节、・・・这样的被3除不尽的大小(字节数)的数据。由此,“C”、“E”、“I”、“K”的各个文字表示的编码在中途被分割。由此,即使数据1～6的一部分泄露,解读文件FI也会变得困难。在本实施方式中,如此地分割文件FI。

[0146] 接下来,对文件分割处理(步骤S40)和加密处理(步骤S50)的具体顺序进行说明。

[0147] 如图12所示,控制部110开始文件分割处理,首先根据在步骤S30中提取的特征信息,参照存储于存储部111的分割大小表DST,求出基于指纹信息的分割大小S_F、基于声纹信息的分割大小S_V、基于虹膜信息的分割大小S_I这3种分割大小S(步骤S41)。

[0148] 根据图10所示的分割大小表DST,例如,如果将指纹的端点设为4、分支点设为5、声纹的音量最大的频率f_{top}设为300Hz、第二大的频率f_{second}设为400Hz、虹膜编码的1的数量N_1设为1005、0的数量N_0设为1043,则对于指纹,为端点＜分支点,选择503字节作为分割大小S_F,对于声纹,为$f_{top}＜f_{second}$,选择491字节作为分割大小S_V,对于虹膜,成为$N_1＜N_0$,选择479字节作为分割大小S_I。

[0149] 分割大小S设定为小于通常的数据处理的单位即一个扇区(512字节)的大小。而且,设定为质数字节。分割大小S设定为比一个扇区小的大小。

[0150] 具体而言,接着,控制部110在表示数据编号的指示器i中设置初始值“1”(步骤S42)。

[0151] 接下来,求出将值i除以3时的余数Mod(i,3)的值为1、2、0的哪一个。

[0152] 在Mod(i,3)＝1的情况下(步骤S43;是),控制部110从文件FI的残存的数据的开头截取与分割大小S_F相当的量的数据(步骤S44)。控制部110利用加密密钥KF将截取的数据加密(步骤S45)。

[0153] 在Mod(i,3)＝2的情况下(步骤S43;否、S46;是),控制部110从文件FI的残存的数据的开头截取与分割大小S_V相当的量的数据(步骤S47)。控制部110利用加密密钥KV将截取的数据加密(步骤S48)。

[0154] 在Mod(i,3)＝0的情况下(步骤S43;否、S46;否),控制部110从文件FI的残存的数据的开头截取与分割大小S_I相当的量的数据(步骤S49)。控制部110利用加密密钥KI将截取的数据加密(步骤S50)。

[0155] 加密的数据的大小是分散的,在这种状态下,在计算机中的处理困难。因此,如图15所示,控制部110将步骤S45、S48、S50中加密的数据与键盘数据组合,生成一个扇区的数据(步骤S51)。

[0156] 接下来,如图9所示,将数据编号i、数据的加密后的大小、以及密码中所使用的加密密钥注册于数据管理表DMT(步骤S52)中。

[0157] 接着,判别未处理的数据是否为0字节,如果不是0字节(步骤S53;否),则将数据编

号i进行+1(步骤S54),返回至步骤S43,并从保存对象文件FI将数据截取并进行加密。

[0158] 在步骤S53中,如果判别未处理的数据为0字节(步骤S53;是),则处理返回至主流程。

[0159] 如此,在文件分割、加密处理中,控制部110从存储对象文件FI中,按照由指纹确定的分割大小S_F、由声纹确定的分割大小S_V、由虹膜确定的分割大小S_I的顺序,从存储对象文件FI中依次截取数据。控制部110将截取的数据利用加密密钥KF、KV、KI依次加密,并依次生成一个扇区的数据。

[0160] 接下来,参照图13对图11所示的分散存储处理(步骤S60)的详细情况进行说明。

[0161] 依次生成扇区数据,该扇区数据包含通过分割、加密处理加密的数据。生成的扇区数据汇总八个作为簇,存储于存储装置210、220中。

[0162] 因此,控制部110将表示簇的顺序的簇编号j初始化为1(步骤S61)。

[0163] 接下来,将通过分割、加密处理生成的扇区数据依次每八个地组合并生成簇(步骤S62)。

[0164] 接下来,控制部110判别保存对象的簇的簇编号j是奇数还是偶数(步骤S63)。如果簇编号j为奇数(步骤S63:是),则将该簇存储于存储装置210上的空闲物理地址PA(步骤S64)中。

[0165] 接着,如图9所示,控制部110将处理的簇的簇编号j、存储的区域的物理地址PA、以及该簇所包含的数据的数据编号i对应地注册于簇管理表CMT(步骤S66)中。

[0166] 接着,控制部110判别文件FI的保存是否结束(步骤S67),如果未结束(步骤S67:否),则对簇编号j进行+1(步骤S68)。接着,处理返回至步骤S62,处理下一个簇。

[0167] 另一方面,在步骤S63中,如果判别处理对象的簇的簇编号j是偶数(步骤S63:否),则控制部110将该簇存储于存储装置220上的空闲物理地址PB(步骤S65)中。

[0168] 接着,控制部110进入上述步骤S66。

[0169] 在步骤S67中,如果判别文件FI的保存结束(步骤S67:是),则文件存储处理结束。

[0170] 接下来,对控制部110所进行的文件再生处理进行说明。

[0171] 如果解码对象的文件FI被确定,则控制部110读取该文件FI用的簇管理表CMT,确定存储目的地的物理地址,并依次读取簇。

[0172] 接下来,控制部110从读取的簇所包含的各扇区中,按照簇管理表CMT和数据管理表DMT的内容,提取从读取的各簇所包含的扇区中被加密的数据。

[0173] 控制部110根据数据管理表DMT的内容,使用合适的加密密钥将提取的数据解码。

[0174] 接下来,通过连接以数据编号i顺序解码的数据,将原始数据(文件FI)再生。

[0175] 另外,由于文件FI被分割为用户唯一的、且计算机在该状态下不能识别的大小的数据簇,因此,即使万一一部分数据泄露,解读泄露的簇也是困难的,信息泄露的危险小。

[0176] 另外,本发明不限定于上述实施方式,能够进行各种变形及应用。例如,在上述实施方式中,对存储装置210与220是云CL上的装置进行了说明,但是也可以是与终端装置10本地连接的装置。

[0177] 另外,示出了将文件FI分割并存储在两个存储装置210和220中的示例,但存储装置的数量是任意的。另外,分割大小S也是任意的,加密密钥的数量也是任意的。

[0178] 在上述实施方式中,对使用分割大小表求出(算出)文件FI的分割大小的示例进行

了说明，但算出分割大小S的方法不限定于此。利用由任意的函数(转换信息)将控制部110从获取的生物体信息中提取的特征信息进行转换等的方法，从终端装置10获取的生物体信息中得到分割大小S即可。

[0179] 另外，上述转换信息不限定于终端装置10内的存储部111，例如，也可以保存于通过网络与终端装置10连接的服务器等中。终端装置10在计算分割大小S时，可以将保存于服务器的转换信息暂时保存于存储部111中，并将生物体信息转换为分割大小S，也可以使服务器计算分割大小S，并进行下载。

[0180] 另外，作为终端装置10获取的生物体信息，列举有指纹信息、声纹信息、虹膜信息这3种，但也可以构成为利用除此以外的生物体信息。例如，终端装置10也可以学习用户的习惯，以基于用摄像头拍摄的习惯字、绘制在触摸面板13上的习惯字的分割大小S将文件FI分割。

[0181] 在上述实施方式中，由从用户的生物体信息中提取的特征信息确定分割大小S，但也可以基于生物体信息，确定包含加密密钥的加密的方法。

[0182] 例如，如图16所示，也可以根据生物体信息应满足的条件预先设定加密密钥，根据生物体信息选择加密密钥。在图16的加密密钥表EKT的示例中，在步骤S45中选择并使用加密密钥KF1和KF2中的一个，在步骤S48中选择并使用加密密钥KV1和KV2中的一个，在步骤S50中选择并使用加密密钥KI1和KI2中的一个。另外，也可以使使用的加密密钥的数量更多。

[0183] 另外，也可以利用函数等将生物体信息或特征量转换为加密密钥。

[0184] 另外，文件FI的存储目的地也可以基于生物体信息确定。例如，如图17A、17B所示，也可以根据生物体信息满足的条件预先设定簇的存储目的地，根据生物体信息选择存储目的地。

[0185] 在实施方式2中，如果数据编号i确定，则为了加密而参照的生物体信息确定，但也可以基于生物体信息，使为了加密而参照的生物体信息变化。

[0186] 例如，如图18A、18B所例示，也可以将某生物体信息应满足的条件与该条件满足时参照的生物体信息(特征量)对应。在图18的示例中，如果根据输入的指纹信息的特征量判别端点≥(分支点+5)，则执行图12所示的处理。另一方面，如果判别端点＜(分支点+5)，则例如在Mod(3)＝2时，参照虹膜信息。因此，在步骤S47中，以与虹膜对应的分割大小S(在图10的示例中为487字节或479字节)截取数据，在步骤S48中，形成基于加密密钥KI的加密。另外，在步骤S48中，也可以变形为使用图16所示的KI1或KI2作为加密密钥。

[0187] 在图15中，为了使截取的大小S的数据为一个扇区的数据，将键盘数据配置在最后，但也可以基于生物体信息更改键盘数据的位置。

[0188] 例如，如图19所示，可以将某生物体信息应满足的条件和该条件满足时的键盘数据的位置对应。在图19的示例中，如果根据输入的虹膜信息的特征量判别N1≥N0，则如图20A所示，键盘数据配置于一个扇区的开头。另外，如果根据输入的虹膜信息的特征量判别N1＜N0，则如图20B所示，从存储对象文件截取的大小S的数据的前100字节配置于一个扇区的开头，接着，键盘数据仅继续(一个扇区的数据大小-S)，然后，配置截取的数据的剩余部分。在这种情况下，优选在数据管理表DMT中注册键盘数据的位置和大小。

[0189] 在上述实施方式中，示出了为了将从输入的生物体信息中提取的特征量加密而参

照的示例，但也可以参照预先注册的生物体信息或特征量。例如，在用户注册时认证用的生物体信息或其特征量，并预先存储于控制部110或存储部111或112中。用户在使用终端装置10或10A时，从扩音器11、触摸面板13、摄像头14输入生物体信息。为了认证用户，将输入的生物体信息与注册的生物体信息或特征量进行对比。用户被认证后，也可以将为了加密、解码而参照的生物体信息或特征量作为注册的生物体信息或特征量。如果设为这样的构成，则存在输入的生物体信息随着终端装置10、10A的使用环境、操作而变动的可能，但由于注册的生物体信息、特征量不变动，因此，能够稳定地进行加密、解码。

[0190] 在实施方式中，示出了几个表，但这些表不需要采取表的形式，只要能够导出需要的信息，则其可以是函数、程序的方式。另外，也可以删除一部分的信息、或注册用于导出该信息的其他信息。例如，由于图2D所示的文件管理表FMT中的加密密钥KA或KB能够从逻辑地址Li中导出，因此可以删除。在该情况下，逻辑地址Li作为确定加密所使用的加密密钥的信息发挥作用。也可以删除图9所示的数据管理表DMT中的加密密钥KF、KV、KI。另外，例如，也可以删除图9所示的簇管理表CMT中的数据编号。在第j个簇中包含数据编号i为8·(j-1)+1～8·j为止的数据。

[0191] 作为为了加密、解码而参照的生物体信息，例示了指纹信息、声纹信息、虹膜信息，但生物体信息的种类不限于这些。例如，除这些以外，也可以导入静脉信息、脸部信息、掌纹信息、签字信息等作为生物体信息，使用的信息的数量也不限于三个，可以为一个、两个，也可以为更多。

[0192] 另外，各装置、部件的配置可以任意地更改。可以将用于使计算机作为终端装置10发挥功能的计算机程序存储并分发至非临时性计算机可读记录介质(CD-ROM等)中，通过将该程序安装于计算机中，构成执行上述处理的终端装置10。

[0193] 在不脱离本发明的广义精神和范围的情况下，本发明可以进行各种实施方式及变形。另外，上述实施方式用于说明本发明，并不用于限定本发明的范围。即，本发明的范围不由实施方式而由权利要求书示出。而且，在权利要求书内及与其同等的发明意义的范围内实施的各种变形视为在本发明的范围内。

[0194] 本发明基于2015年4月30日申请的日本专利申请2015-093729号。日本专利申请2015-093729号的说明书、权利要求书、附图的整体作为参照并入本说明书中。

[0195] 附图标记说明

[0196] 10:终端装置

[0197] 11:扩音器

[0198] 12:扬声器

[0199] 13:触摸面板

[0200] 14:摄像头

[0201] 111、112:存储部

[0202] 113:通信部

[0203] 210、220:存储装置

[0204] CL:云

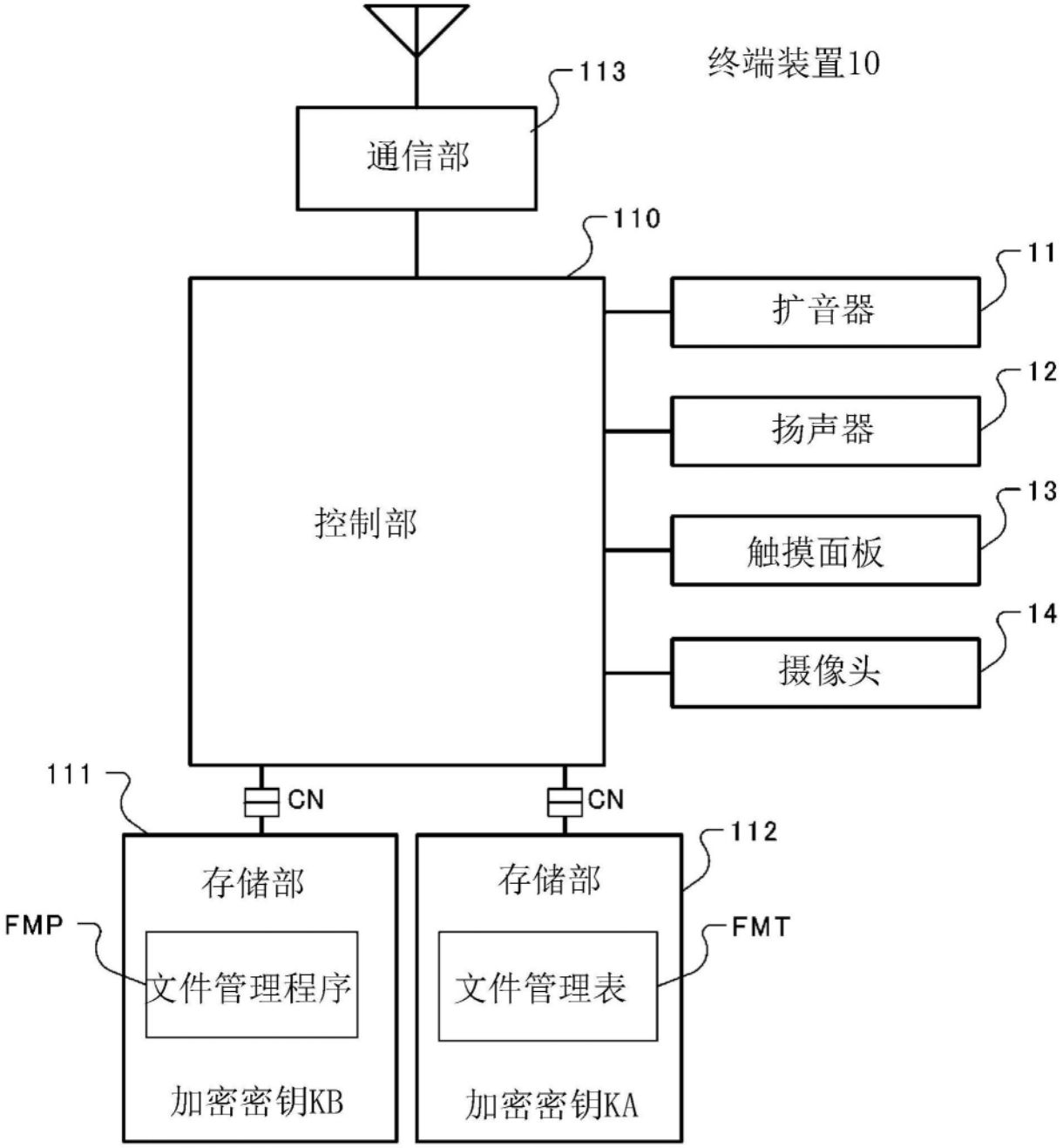

终端装置10
113
通信部
110
11
扩音器
12
扬声器
13
触摸面板
14
摄像头
控制部
111
CN
CN
112
存储部
存储部
FMP
文件管理程序
FMT
文件管理表
加密密钥KB
加密密钥KA

图1

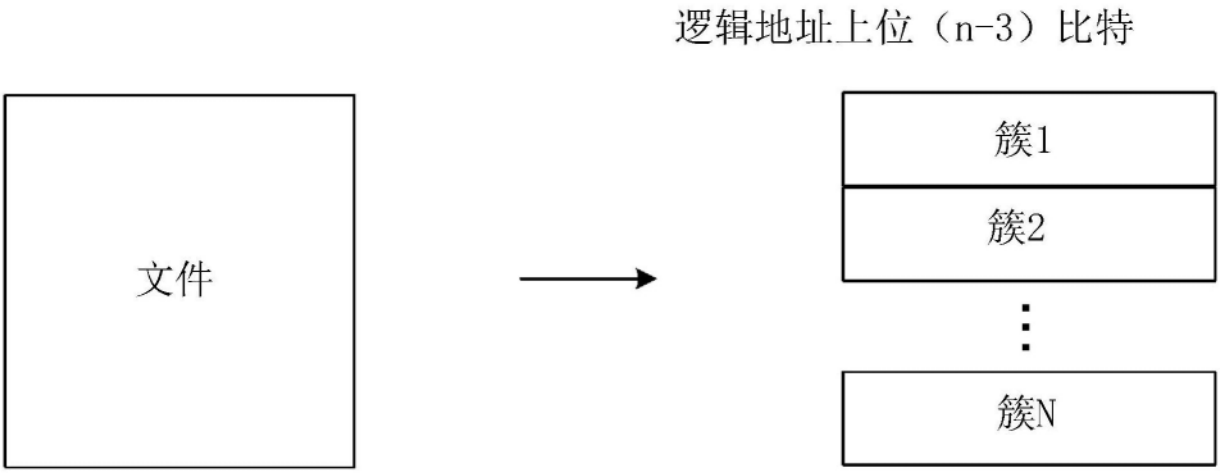

逻辑地址上位（n-3）比特
文件
簇1
簇2
簇N

图2A

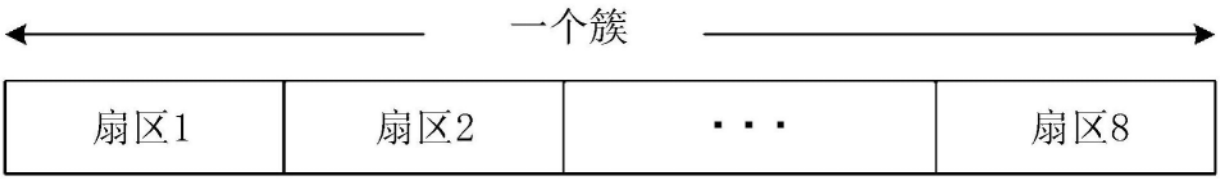

一个簇
扇区1
扇区2
· · ·
扇区8

图2B


奇数逻辑
地址簇
偶数逻辑
地址簇
基于加密密钥
KA的加密
基于加密密钥
KB的加密
物理地址PA
奇数地址簇
物理地址PB
奇数地址簇

图2C

文件管理表FMT

Li	PAi (PBi)	KA (KB)

图2D

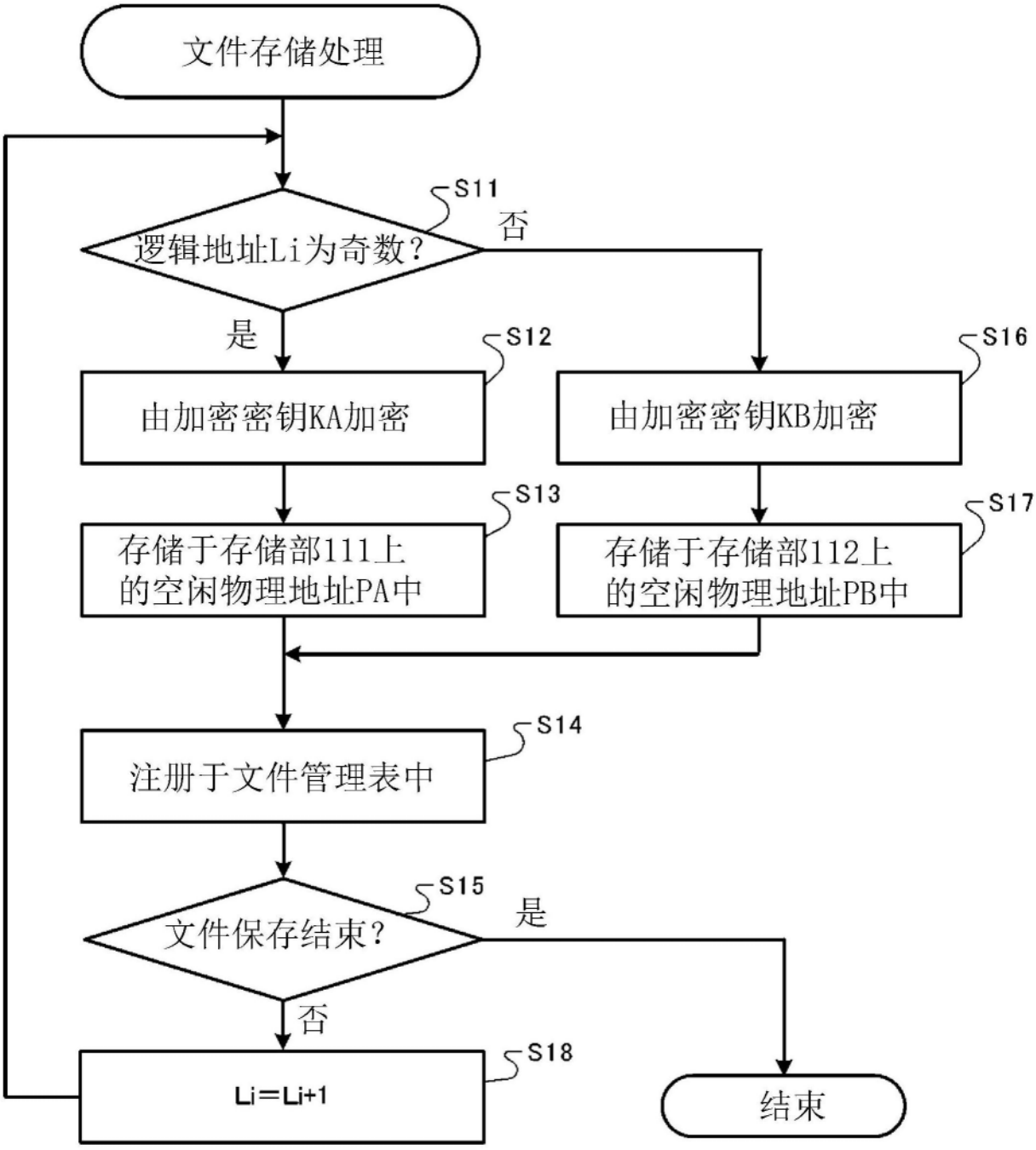


图3

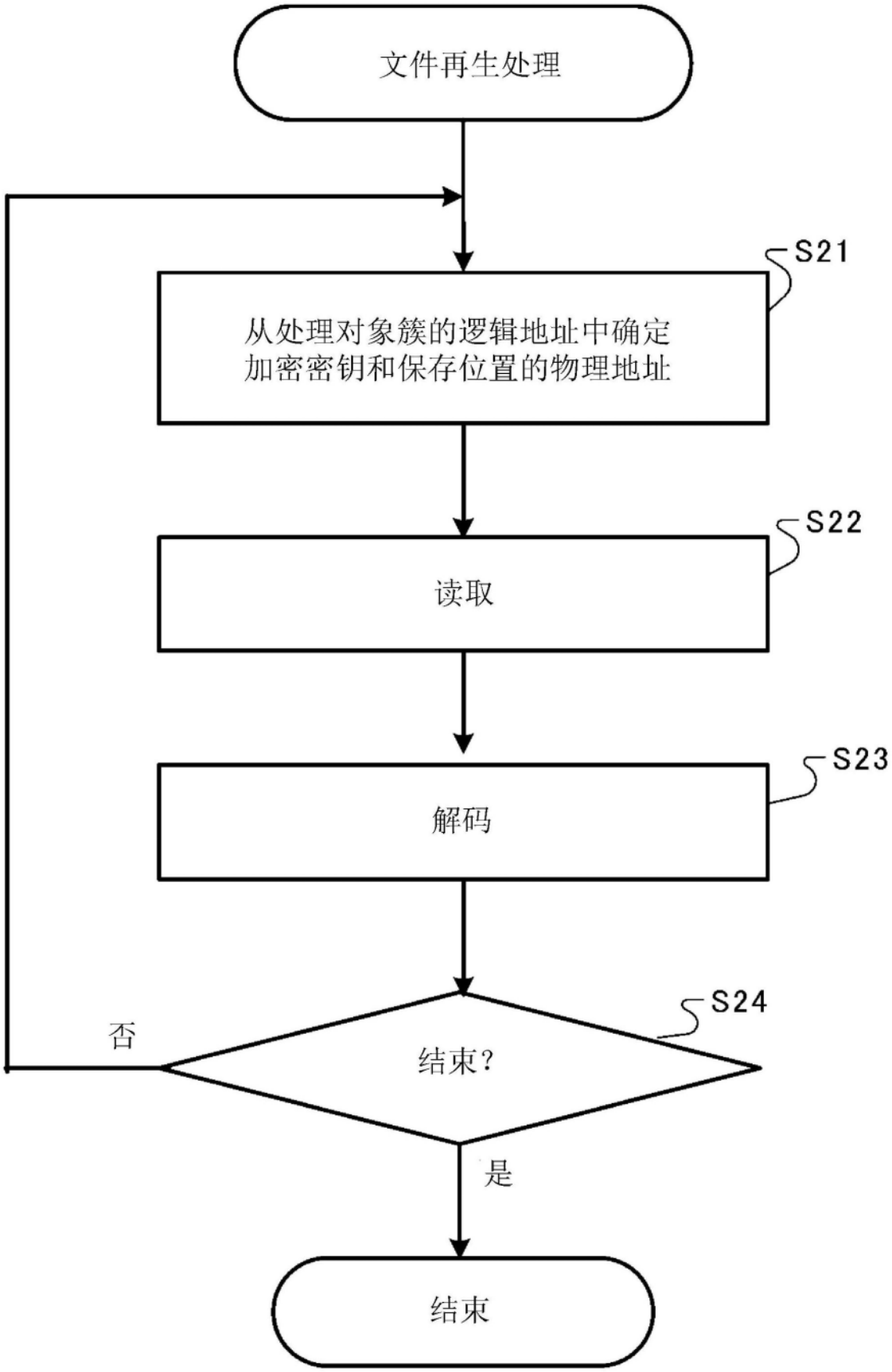

文件再生处理
S21
从处理对象簇的逻辑地址中确定
加密密钥和保存位置的物理地址
S22
读取
S23
解码
S24
结束?
否
是
结束

图4

电话簿文件

姓名	住址	年龄	…	电话号码	邮件地址

图5

日程文件

月日	题目	地点	…	时间	责任人 邮件地址

图6

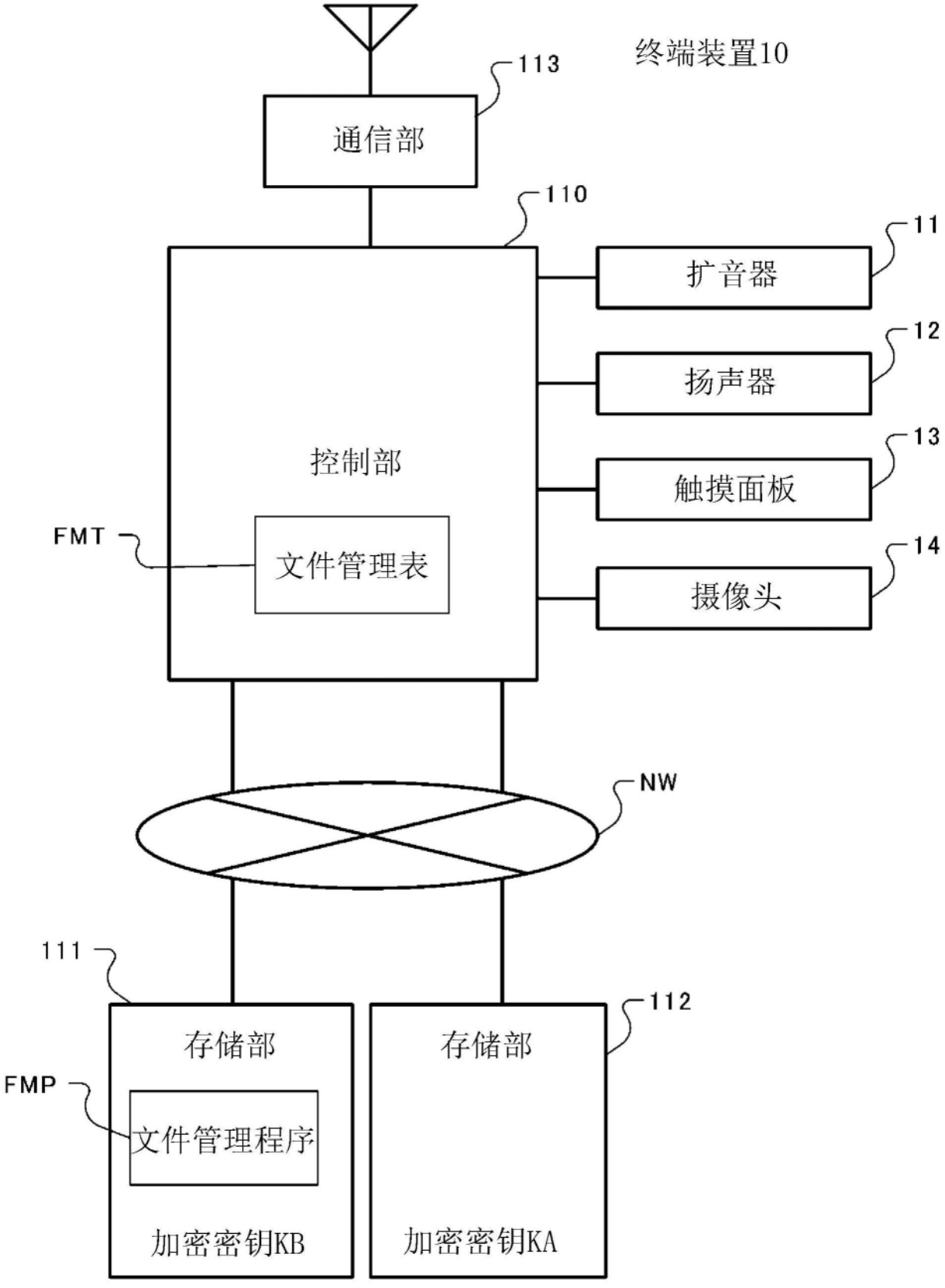

终端装置10
113
通信部
110
11
扩音器
12
扬声器
13
触摸面板
14
摄像头
控制部
FMT
文件管理表
NW
111
存储部
FMP
文件管理程序
加密密钥KB
112
存储部
加密密钥KA

图7

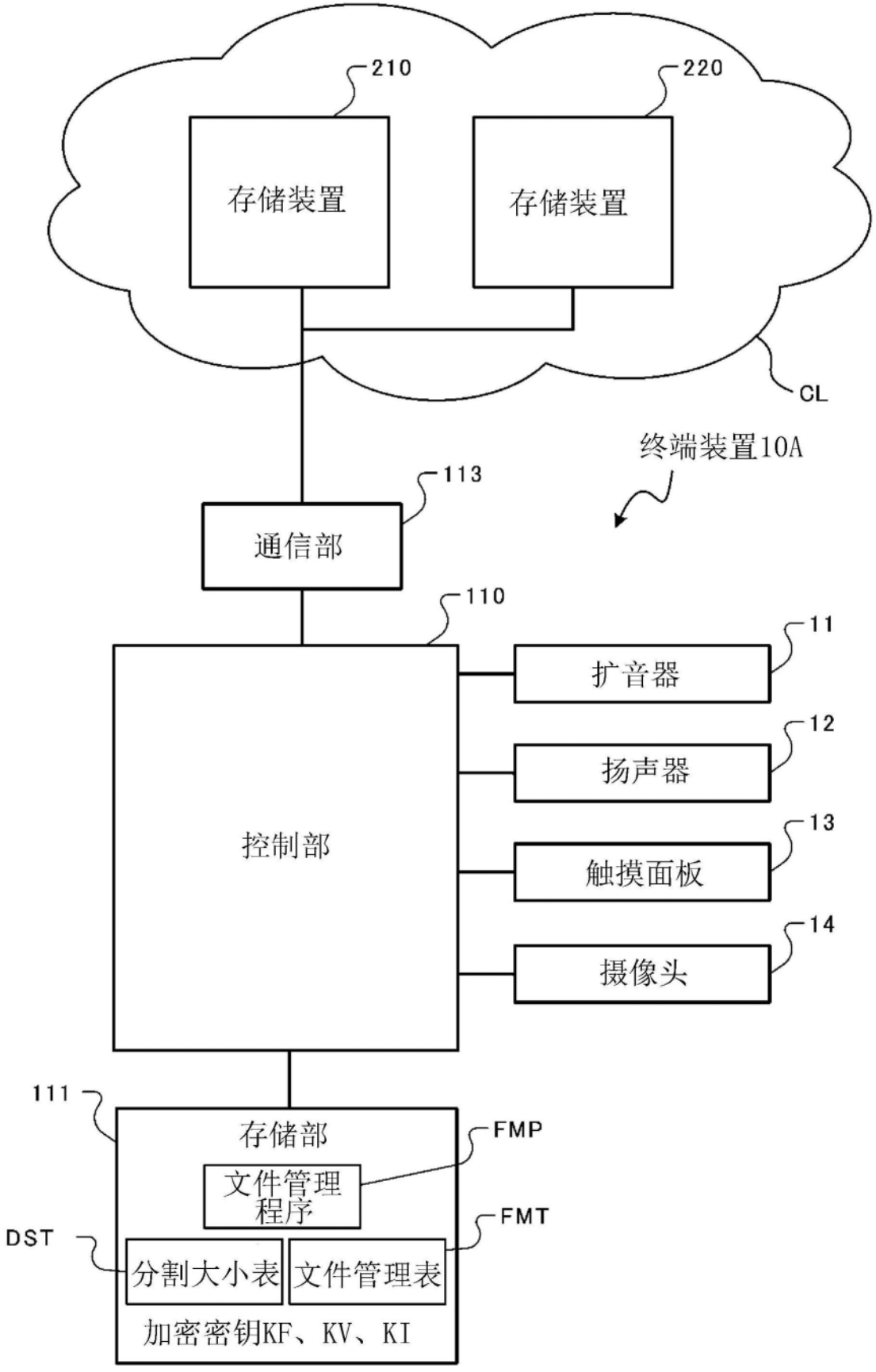

210
220
存储装置
存储装置
CL
终端装置10A
113
通信部
110
控制部
11
扩音器
12
扬声器
13
触摸面板
14
摄像头
111
存储部
FMP
文件管理程序
FMT
DST
分割大小表
文件管理表
加密密钥KF、KV、KI

图8

数据管理表FMT

文件名：FI

数据管理表DMT

数据编号i	加密后的大小	加密密钥
1	509	KF
2	499	KV
3	487	KI
4	509	KF
⋮	⋮	⋮

簇管理表CMT

簇编号j	存储目的地及物理地址	数据编号i
1	PA1	1－8
2	PB2	9－16
3	PA3	17－24
⋮	⋮	⋮

图9

分割大小表DST

生物体信息	条件	分割大小S	
指纹	端点≥分支点	509 byte	S_F
	端点＜分支点	503 byte	
声纹	$f_{top} \geq f_{second}$	499 byte	S_V
	$f_{top} < f_{second}$	491 byte	
虹膜	$N_1 \geq N_0$	487 byte	S_I
	$N_1 < N_0$	479 byte	

图10

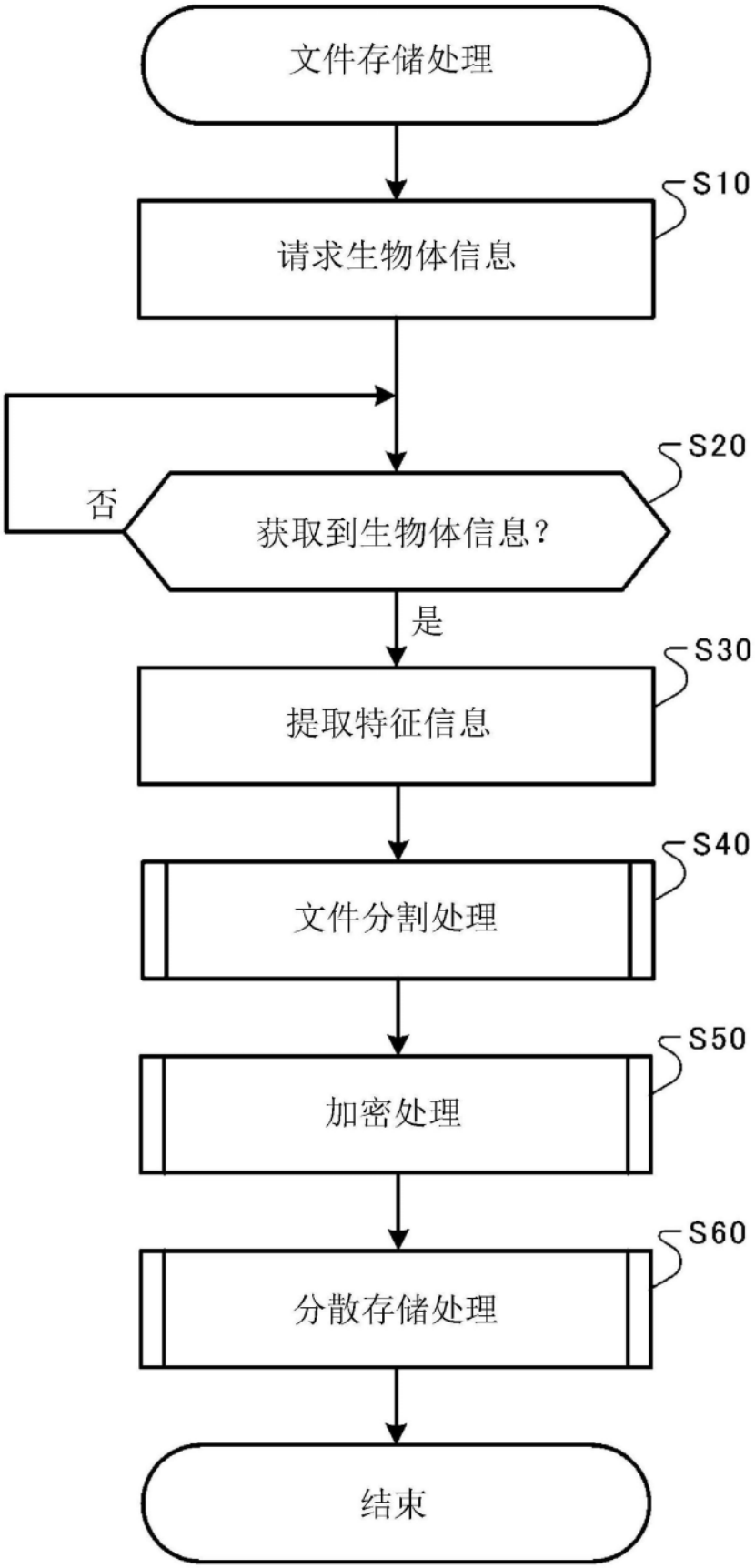

文件存储处理
S10
请求生物体信息
S20
否
获取到生物体信息？
是
S30
提取特征信息
S40
文件分割处理
S50
加密处理
S60
分散存储处理
结束

图11

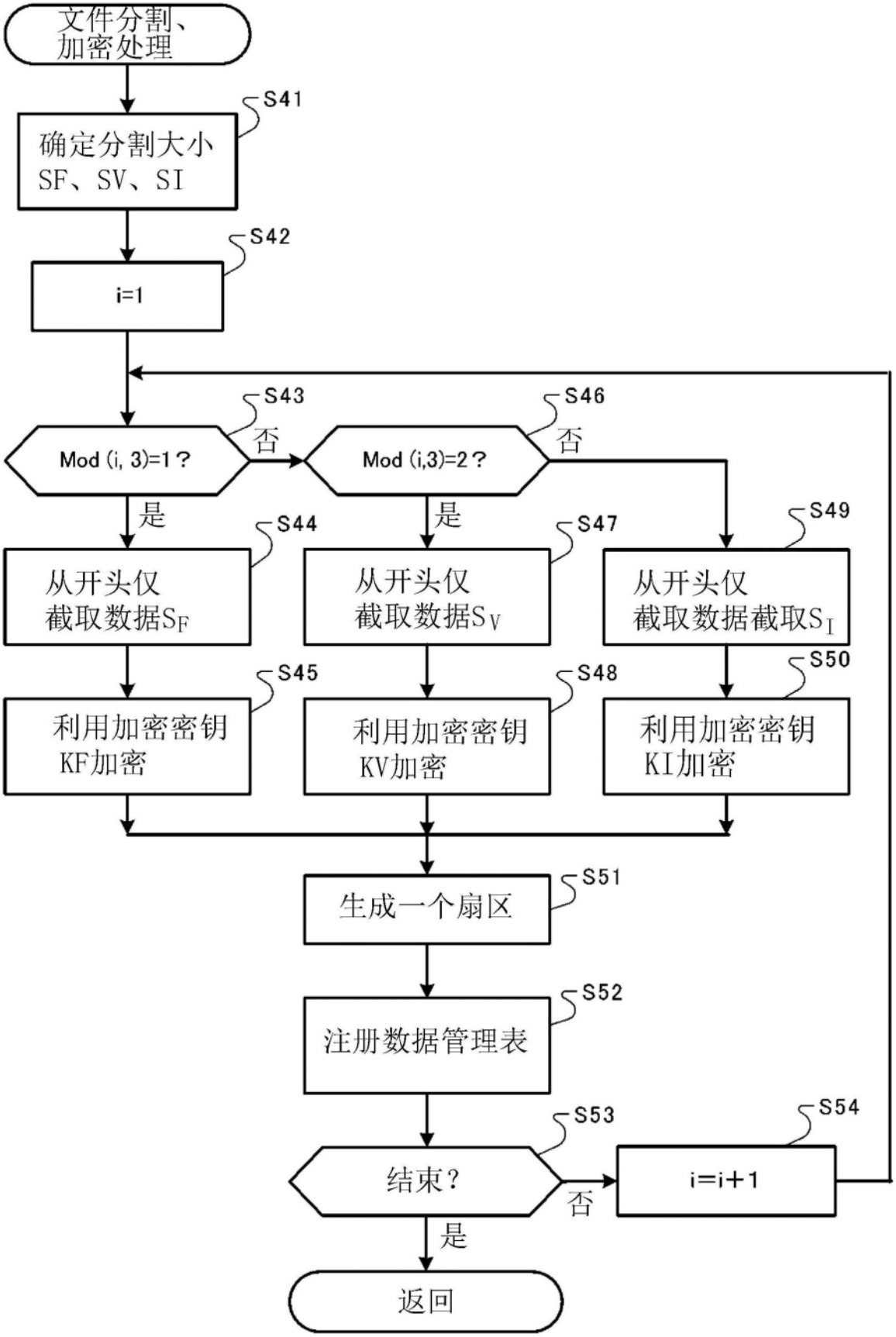

文件分割、
加密处理
S41
确定分割大小
SF、SV、SI
S42
i=1
S43
Mod (i, 3)=1？
否
S46
Mod (i,3)=2？
否
是
是
S44
从开头仅
截取数据SF
S47
从开头仅
截取数据SV
S49
从开头仅
截取数据截取SI
S45
利用加密密钥
KF加密
S48
利用加密密钥
KV加密
S50
利用加密密钥
KI加密
S51
生成一个扇区
S52
注册数据管理表
S53
结束？
否
S54
i=i+1
是
返回

图12

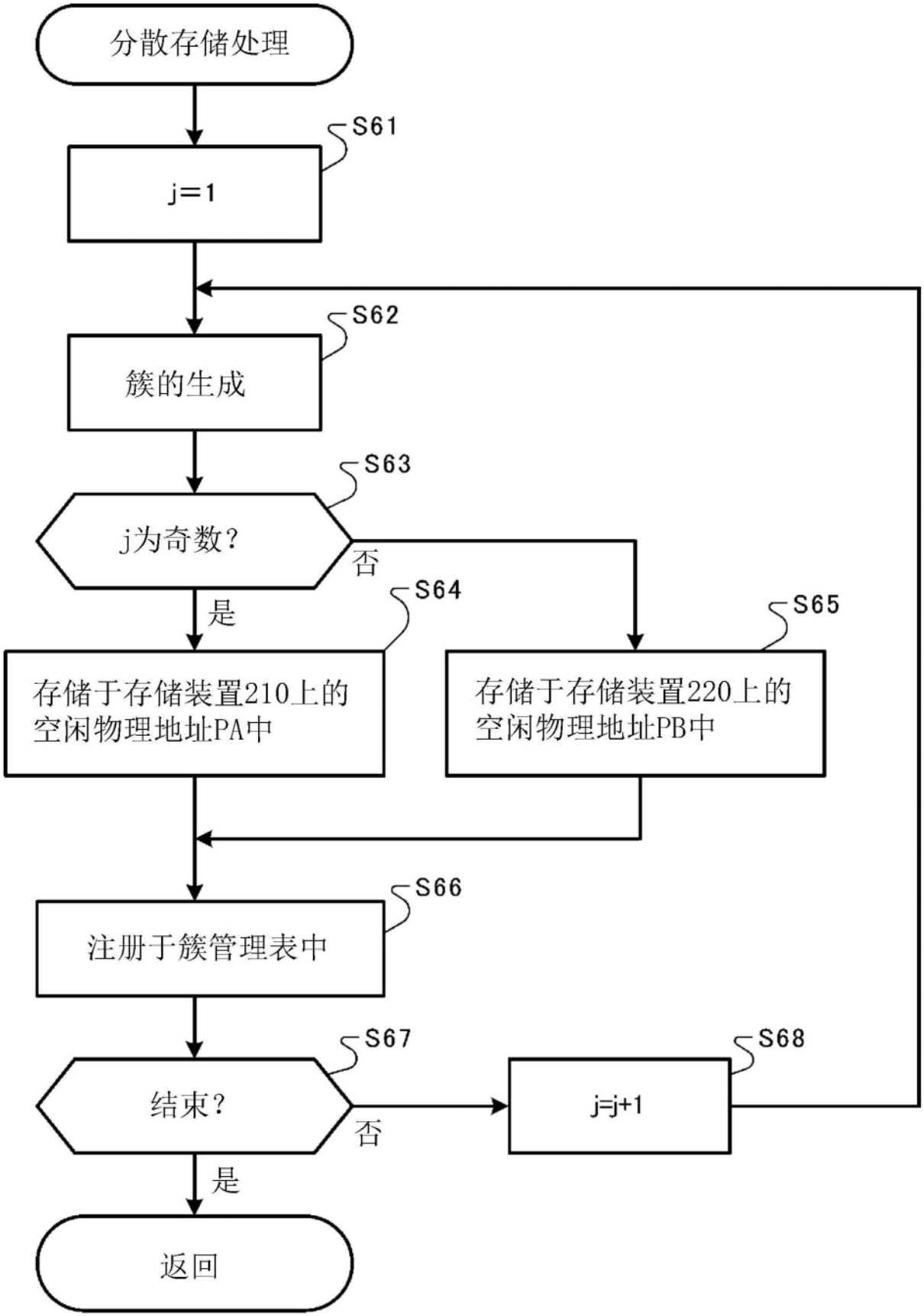

分散存储处理
S61
j=1
S62
簇的生成
S63
j为奇数?
否
是
S64
存储于存储装置210上的
空闲物理地址PA中
S65
存储于存储装置220上的
空闲物理地址PB中
S66
注册于簇管理表中
S67
结束?
否
是
S68
j=j+1
返回

图13

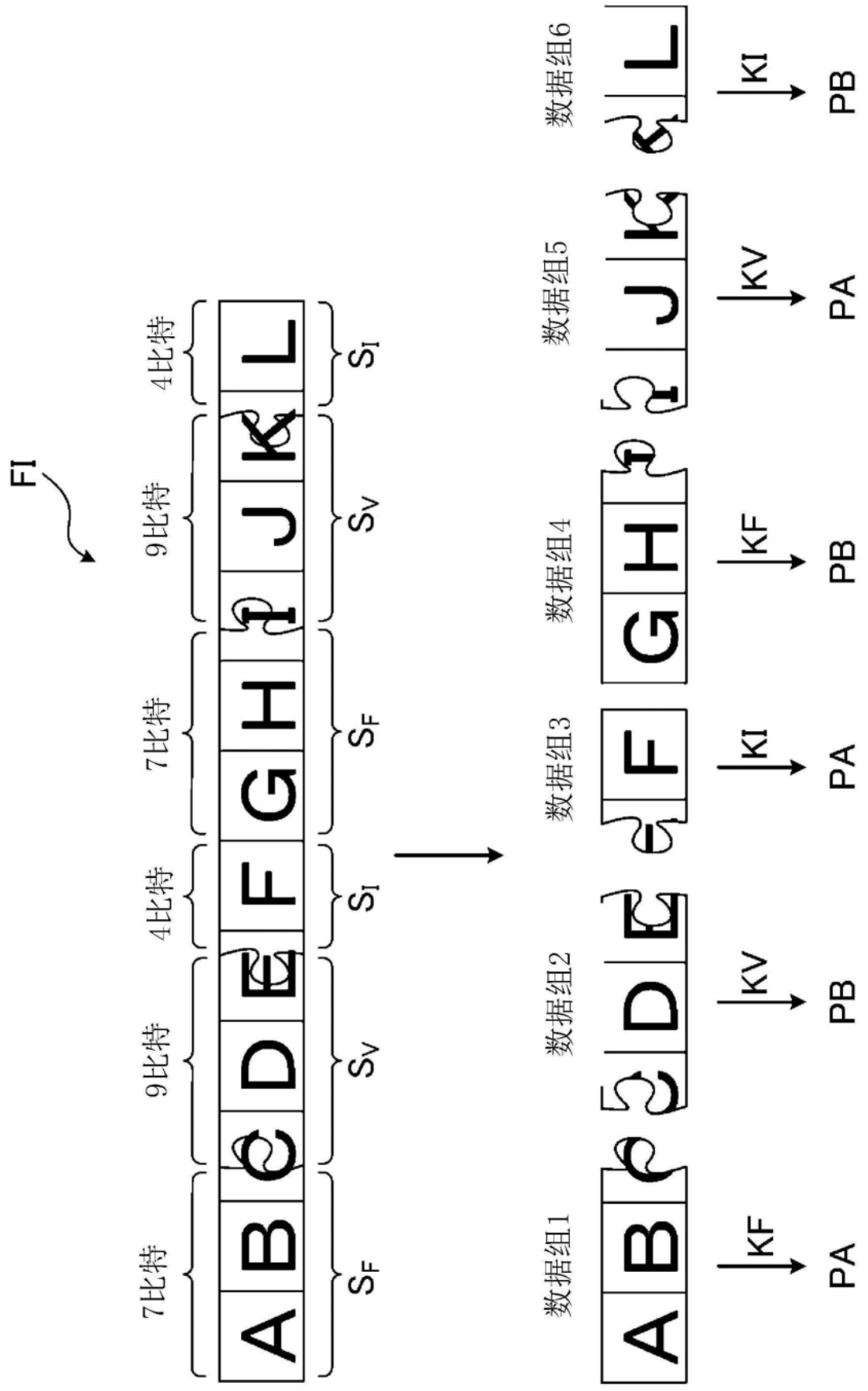

FI
7比特
9比特
4比特
7比特
9比特
4比特
A B C D E F G H I J K L
S_F
S_V
S_I
S_F
S_V
S_I
数据组1
数据组2
数据组3
数据组4
数据组5
数据组6
KF
KV
KI
KF
KV
KI
PA
PB
PA
PB
PA
PB

图14

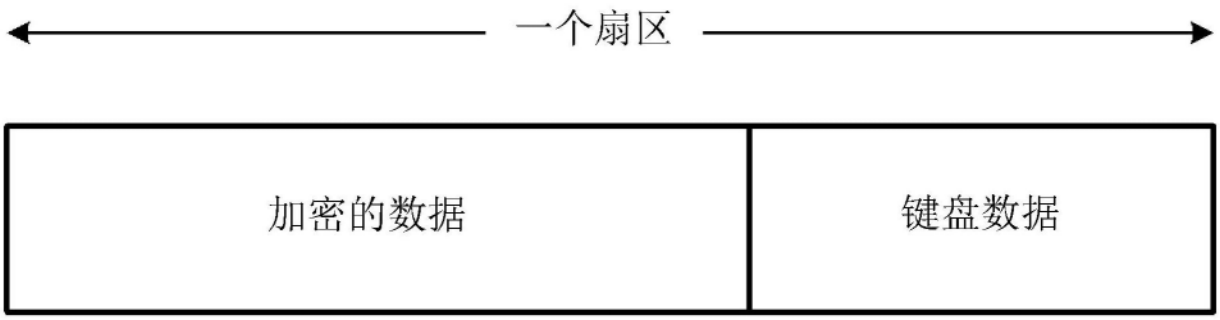


图15

加密密钥表EKT

生物体信息	条件	加密密钥
指纹	端点≥分支点+3	KF1
	端点<分支点+3	KF2
声纹	$f_{top} \geq f_{third}$	KV1
	$f_{top} < f_{third}$	KV2
虹膜	$N_1 \geq N_0-2$	KI1
	$N_1 < N_0-2$	KI2

图16

存储目的地表SAT

生物体信息	条件	存储目的地
指纹	端点≥分支点+1	奇数簇：210 偶数簇：220
	分支点-1<端点<分支点+1	奇数簇：220 偶数簇：111
	端点<分支点-1	奇数簇：111 偶数簇：210

图17A

存储目的地表SAT

生物体信息	条件	存储目的地
指纹	端点≥分支点+1	210
	分支点-1<端点<分支点+1	220
	端点<分支点-1	111

图17B

生物体信息选择表BST

条件（指纹信息）	加密所使用的生物体信息
端点≥分支点＋5	Mod(3)=1: 指纹 Mod(3)=2: 声纹 Mod(3)=0: 虹膜
端点＜分支点＋ 5	Mod(3)=1: 指纹 Mod(3)=2: 虹膜 Mod(3)=0: 声纹

图18A

生物体信息选择表BST

条件（指纹信息）	加密所使用的生物体信息
端点≥分支点	Mod(2)=1: 虹膜 Mod(2)=0: 声纹
端点＜分支点	虹膜

图18B

键盘数据位置选择表

条件（虹膜信息）	键盘数据的位置
$N_1 \geqslant N_0$	开头
$N_1 < N_0$	从开头起的第100比特起

图19

图20A

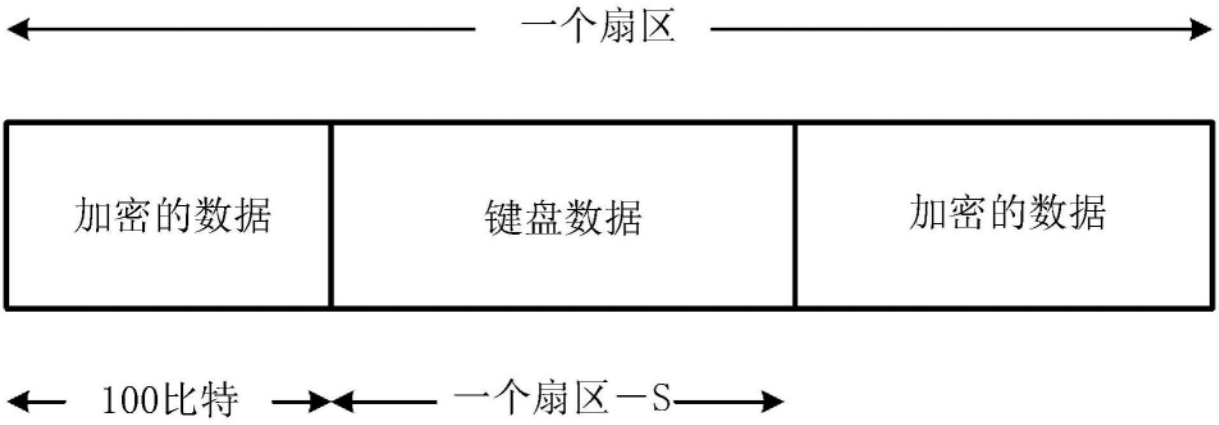


图20B