

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200610136220.2

[51] Int. Cl.

H04L 9/00 (2006.01)

H04L 9/32 (2006.01)

G09C 1/00 (2006.01)

G06F 12/14 (2006.01)

G11B 20/10 (2006.01)

[43] 公开日 2007 年 4 月 4 日

[11] 公开号 CN 1941691A

[22] 申请日 2002.7.10

[21] 申请号 200610136220.2

分案原申请号 02814451.1

[30] 优先权

[32] 2001.7.17 [33] JP [31] 216138/2001

[71] 申请人 夏普株式会社

地址 日本大阪府大阪市

[72] 发明人 佐藤克彦 泽田裕司

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 王忠忠

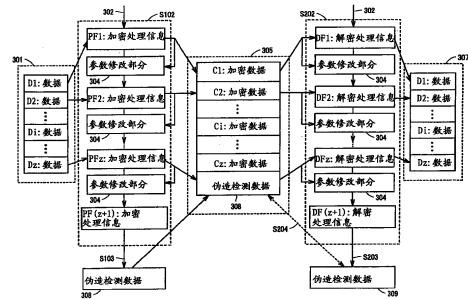
权利要求书 2 页 说明书 17 页 附图 16 页

[54] 发明名称

生成用于检测在处理期间加密数据的虚假改造的数据的设备及方法

[57] 摘要

依次提取一部分要加密的数据(301)。利用加密所述数据的先前所提取的部分的结果，来依次计算所述数据的当前所提取部分的加密结果。利用所依次计算的加密结果，来生成加密数据(305)。在生成加密数据的过程中，将所最终计算的加密结果($PF(z+1)$)添加到已生成的加密数据中。这里，将最终计算的结果用作为用于检测要加密的数据是否是已被伪造的数据的伪造检测数据(308)。



1. 一种再现加密数据的方法，包括以下步骤：

顺序地从划分所述加密数据的多个块的指定块中提取部分所述加密数据 (S1301);

使用对在提取步骤中先前所提取的所述部分的所述数据进行解密的结果，来顺序地计算对在提取步骤中当前所提取的所述部分的所述数据进行所述解密的结果，并且使用顺序地计算的所述解密的所述结果，来生成解密数据 (S1302, S1303); 和

将表示在使用步骤中最终所计算的所述解密的所述结果的所述数据同先前被关联于所述指定块的、用于检测所述指定块是否被伪造的伪造检测数据进行比较，从而根据比较结果来判断是否再现与在使用步骤中所生成的所述指定块相对应的所述解密数据 (S1304)。

2. 如权利要求 1 所述的方法，进一步包括从所述加密数据的所述多个块中分别选择出对应于所述指定块的一块或多块的步骤，其中所述加密数据是通过对要再现的内容进行加密而获得的数据，并且选择步骤选择对应于如下数据大小的所述一块或多块，所述数据大小对应于所述可一次再现的内容量。

3. 如权利要求 1 所述的方法，其中表示所述解密的所述结果的所述数据是与所述解密的所述结果相对应的报文摘要，所述解密的所述结果由表示所述解密的所述结果的所述数据来表示。

4. 如权利要求 1 所述的方法，其中所述解密的所述结果是用在公共密钥加密系统中的全部或部分加密参数 (401)。

5. 如权利要求 1 所述的方法，进一步包括如下步骤：获取所述加密数据 (S1301, S1306) 的步骤，其中如果在比较步骤中判定未对所述指定块进行再现，则在获取步骤中获取对应于所述指定块的所述加密数据。

6. 一种再现加密数据的方法，包括：

提取装置，用于顺序地从划分所述加密数据的多个块的指定块中提取部分加密数据；

顺序计算和生成装置，使用对由所述提取装置先前所提取的所述部分的所述数据进行解密的结果，来顺序计算对由所述提取装置当前

所提取的所述部分的所述数据进行所述解密的结果，并根据顺序地计算的所述解密的所述结果生成解密数据；和

比较装置，用于将表示由所述顺序计算装置最终所计算的所述解密的所述结果的所述数据同先前被关联于所述指定块的、用于检测所述指定块是否被伪造的伪造检测数据进行比较，从而根据比较结果来判断是否再现对应于所述指定块的所述解密数据，所述指定块由所述顺序计算装置加以生成。

生成用于检测在处理期间加密数据的虚假改造的数据的设备及方法

本申请是申请人夏普株式会社于 2002 年 7 月 10 日提交的同名中国专利申请 No. 02814451.1 的分案申请。

技术领域

本发明涉及用于生成能够检测伪造电子数据的加密数据的加密技术，以及用于对加密数据进行解密的解密技术。

背景技术

经过网络发送和接收要求版权保护的程序及数据或高度保密数据，并且将它们记录在只读光盘（CD-ROM）或其它记录介质上并进行商业化分发。这类数据可被未经授权访问该数据的第三方来存取和伪造。为了防止这一事件的发生，对该数据进行加密。

例如，如参照图 5 所述，对要通信的数据进行加密。最初，发送者读取要加密的数据（步骤（S）1001），并且利用哈希函数来计算报文摘要（MD），以及计算用于检测伪造的校验字符串（S1002）。利用不同于计算 MD 的手段可以检测伪造。它可以通过不同手段、例如应用循环冗余码校验（CRC）码来进行检测。然后，依照指定的加密技术来对要加密的数据进行加密（S1003），并且将在 S1002 所获得的 MD 附加于加密数据，并由此将它们发送到对方（S1004）。

尽管未示出，但接收者实施这一处理的逆向形式。更具体而言，具有已接收的加密数据的接收者最初执行解密处理，然后计算 MD。比较这个计算出的 MD 和附加于已接收的加密数据的 MD。如果它们匹配，则判定已接收数据是无伪造的正常数据。

图 16 示意性示出了上述数据流程。在图 16 中，先将要加密的数据 101 分成 z 个子数据 N_i ，其中 $i = 1$ 至 z 。在 S1 和 S2，为每个数据 N_i 使用哈希函数来执行哈希函数处理，并且使用加密处理信息及参数修改部分来执行加密处理。作为结果，生成了加密数据 M_i ，其中 $i = 1$ 至 z 。在这种情况下，将哈希函数处理的最终结果附加于加密数据 $M_1 - M_z$ ，以作为伪造检测的校验字符串 MD，从而完成加密数据 102。为了对加密数据 102 进行解密，最初在 S3，利用解密处理信息及参数修改部分，使加密数据 M_i 经过解密处理，从而获得由数据 P_i 所形成的

解密数据 103，其中 $i = 1$ 至 z 。接着，在 S4，所有数据 P_i 经历哈希函数处理，来计算校验字符串 MD。将计算出的校验字符串 MD 与包含于加密数据 102 中的伪造检测校验字符串 MD 进行比较，且如果两个 MD 相匹配，则判定加密数据 $M_1 - M_z$ 不是伪造数据，而如果两个 MD 不匹配，则判定该数据是伪造数据。

上述常规加密处理需要两步：计算伪造检测校验字符串，以及对数据进行加密。所述解密处理同样需要两步：对数据进行解密，以及计算伪造检测校验字符串以供比较。这些步骤中的每一步都具有十分大量的处理，并且执行加密与解密处理的设备、在它们完成加密以供传输和完成解密以供再现之前，将会需要很长一段时间。这正是实时执行处理的障碍，例如经由网络将来自于服务器的内容分发到对应于客户端的移动终端上，并且立即在该移动终端上再现所述内容。换句话说，具有低处理能力的移动终端，需要很长一段时间来再现所接收到的内容，这样的移动设备提供了很差的实用性。

此外，尽管如此，合法获取的内容仍然会使数据部分丢失，或者被经由网络在发送与接收期间的其它数据、或者在具有存储于其中的内容的介质中的其它数据所代替。在此情况下，为了再次获得合法内容，就必须接收该内容的全部数据，并相应地耗费十分长的一段时间来传递数据。

日本已公开专利 2000-122861 号公开了用以防止软件、数据等等的伪造的技术。在这个技术中，使用如上所述的这类哈希函数来检测伪造。此外，在这个技术中，将要压缩的数据划分成多个块，每一块都当作一个单元，并且一个块不论何时经过加密处理，皆要计算所述块的加密密钥，这种计算明显耗费时间。

发明内容

本发明针对一种使处理量降低的设备和方法，一种促使计算机执行所述方法的程序，一种在其中记录有所述程序的介质。

为了实现上述目的，本发明在一方面，提供了对数据进行加密以生成加密数据的加密方法及设备。当实施此加密时，计算加密结果。所述结果由数据来表示，所述数据将被附加于加密数据。这个表示加密结果的数据，表示用于检测加密数据是否为伪造数据的伪造检测数据。因此，当生成加密数据时，能够获得伪造检测数据。这样就能消

除独立于生成加密数据而计算伪造检测数据的需要。能够以减少的处理量来实现加密。

为了实现上述目的，本发明在另一个方面，提供了一种检测加密数据的伪造的方法及设备。其接收加密数据并对加密数据进行解密，以生成解密数据。当实施此解密时，计算解密结果。所述结果由数据来表示，所述数据表示用于检测加密数据是否为伪造数据的伪造检测数据。因此，当生成解密数据时，能够获得伪造检测数据。这样就能消除独立于生成加密数据而计算伪造检测数据的需要。能够以减少的处理量来实现解密。

在检测加密数据伪造的上述方法及设备中，最好按每个指定大小的数据块对加密数据进行解密，以生成数据块的解密块数据。对于当实施解密时所计算的每个解密块数据，将表示对加密块数据进行解密的结果的数据同附加于数据块的伪造检测数据进行比较，并根据比较结果来检测加密数据是否为伪造数据。对于每个数据块，所述加密数据都能将伪造检测数据附加于其上。可为每个数据块判断加密数据是否为伪造数据。如果判定伪造存在，则就能按块来对加密数据的伪造部分进行定位。除了对应于所述伪造部分的数据块之外，也能对其它数据块正常进行解密。

本发明在又一个方面，提供了一种再现先前已分成多个块的加密数据的方法及设备。其从指定块中顺序提取部分数据。利用对先前所提取的部分数据进行解密的结果，来顺序计算对当前所提取的部分数据进行解密的结果，并且利用所顺序计算的对数据进行解密的结果，来生成解密数据。将表示在生成解密数据过程中所计算的最终解密结果的数据同先前被关联于指定块的伪造检测数据进行比较，并根据比较结果来判断是否应该再现与已生成的指定块相对应的解密数据。

因此，针对每个指定块，可将伪造检测数据关联于加密数据。可为每个指定块判断加密数据是否为伪造数据。可为每个指定块判断相应的解密数据是否可再现。

在再现加密数据的上述方法及设备中，加密数据最好是通过对要再现的内容进行加密而获得的数据，并且根据加密数据的多个块，可以选择并解密对应于数据大小的一块或多块，其中所述数据大小对应于可一次再现的内容量。

内容的一个选定块或多个选定块可以比其它块更早被解密，以供再现。对加密内容进行再现，可以在全部内容都完成解密之前开始。

附图说明

在所述附图中：

图 1 是第一实施例中的加密处理的流程图；

图 2 是第一实施例中的解密处理的流程图；

图 3 示意性示出第一实施例的加密与解密处理中的数据流程；

图 4A 和 4B 是专门作为举例、用来说明第一实施例的加密与解密处理的示意图；

图 5 是专门作为举例、用来说明第一实施例的加密处理的图；

图 6A、6B 和 6C 示出根据作为举例的第二实施例的数据结构；

图 7 是第二实施例中的加密处理的流程图；

图 8 是第二实施例中的解密处理的流程图；

图 9 是第三实施例中的分发系统的配置图；

图 10A 和 10B 作为举例示出第三实施例中电子书内容的数据结构；

图 11 是表示第四实施例的解密处理中的数据流程的示意图；

图 12 是第四实施例中的解密处理的流程图；

图 13 是表示第四实施例的解密处理中的数据流程的示意图；

图 14 示出第五实施例中的信息处理设备的配置；

图 15 是常规加密处理的流程图；和

图 16 是用来说明常规加密与解密处理中的数据流程的示意图。

实施本发明的优选方式

在下文中，将参照附图更加清楚地对本发明的实施例作出描述。

第一实施例

图 1 示出了依照本发明实施例的加密处理的过程。这个过程采用了适用于任何加密系统的加密算法，在所述加密系统中加密结果与解密结果是等同的信息，并且在加密与解密处理中，应用先前的运算结果来随后计算当前的运算结果。照此，可以使用公用密钥加密系统、或者其它类似的、一般所采用的加密系统，并且例如，所述系统可以通过依照称作密码分组链接 (cipher block chaining: CBC) 模式的过程，处理众所周知的数据加密标准 (DES) 来加以实现。注意到：CBC 模式是涉及链接的加密方法，而且接连地采用先前加密结果来计算当

前加密结果。

参照图 1，在加密处理中，最初获得要加密的数据（S101）。尽管未示出，但在每个实施例中，都是在通用个人计算机、移动终端设备、移动电话机或类似的信息处理器设备（下文中简单称为“信息处理设备”）中执行加密与解密处理的。照此，例如可从 CD-ROM 或其它类似的记录介质、内置于信息处理设备的硬盘那里以及经由网络从服务器那里获得要加密的数据。

然后，将已获得的要加密的数据依照加密算法来进行加密（S102）。在这种情况下，利用指定大小的数据单位、从顶部顺序地对要加密的数据进行加密。加密数据由此而生成。对于每个数据单位，执行计算且由此发生加密，所述数据单位提供用以计算后续数据单位的加密处理信息的加密参数值（下文中称为“加密处理信息”）。

当要加密的全体数据都已被加密并且加密数据由此而生成时，使用当前的、最终的加密处理信息来生成伪造检测数据（S103）。将由此而生成的伪造检测数据附加于加密数据。所述加密数据由此而完成（S104）。所述加密处理由此而结束。

图 2 示出了解密处理的过程。这个过程采用了与上述加密算法相对应的解密算法。

所述解密处理基本上是加密处理的逆向形式。参照图 2，最初读取如上所述的已生成的加密数据（S201）。由于解密处理同样是在如上所述的这种信息处理设备中重新执行的，因而也能获得加密数据，如上面就要加密的数据而言所述的那样，例如从 CD-ROM 或类似的记录介质、内置于信息处理设备的硬盘那里以及经由网络从服务器那里获取上述加密数据。

接着，将已获得的加密数据依照解密算法进行解密（S202）。一旦加密数据已经被完全解密，就能检测在加密处理中计算出的与加密处理信息相对应的解密处理信息。按类似于在加密处理中使用的方式，使用已检测到的解密处理信息来生成伪造检测数据（S203）。

判断在 S203 所生成的伪造检测数据与在 S201 读取的伪造检测数据是否相匹配（S204）。如果它们匹配，则加密数据或由加密数据表示的要加密的数据就不是伪造数据，并且获得解密数据（S205）。如果所述伪造检测数据不匹配，则加密数据或由加密数据表示的要加密的数

据是已被伪造过的，并且相应地执行指定的错误处理 (S206)。

现在进行参考来更清楚地描述上述加密与解密处理的过程。

图 3 示意性示出了处理中的数据流程，在所述处理中对要加密的数据进行加密并且继而进行解密，从而获得原始数据（要加密的数据）。

最初参照图 3，将描述加密步骤 (S102)。要加密的数据 301 具有每个预定、指定大小的数据单位，所述数据单位依照加密算法被加密。在此例中，要加密的数据 301 具有每个已顺序加密的数据 D_i ，其中 $i = 1, 2, 3 \dots, z$ 。

在加密步骤 (S102) 中，要加密的数据 301 具有依照指定加密算法所提取并加密的数据 D_i ，用以生成加密数据 C_i ，其中 $i = 1, 2, 3 \dots, z$ 。在这种情况下，参考加密处理信息 PF_j 来转换数据 D_i ，其中 $j = 1, 2, 3 \dots, z, z + 1$ 。注意到：数据 D_1 是参考加密处理信息 PF_1 来转换的，其中在加密处理之前先通过加密密钥 302 初始化所述 PF_1 。通过所使用的加密算法来提前判定是如何通过加密密钥 302 来计算加密处理信息 PF_1 的，以及确定将数据 D_i 转换为加密数据 C_i 的处理。现在将参照图 4A 来描述加密算法的一个例子。

图 4A 示出了当对数据 D_i 进行加密以生成加密数据 C_i 时，在图 3 中所用的加密处理的过程。在图 4A 中，输入数据 A 表示图 3 中的要加密的数据 D_i ，而输出数据 B 表示图 3 中的加密数据 C_i 。这个加密处理包括：对应于加密处理信息 PF_j 的内部转换参数 401、转换部分 402 以及参数修改部分 304。内部转换参数 401 具有参数 X, Y 和 Z，并且在加密处理执行以前，由初始值为 K 的加密密钥 302 来对它们进行初始化。这里，作为初始状态，假定参数 X = 6，参数 Y = 2，而参数 Z = 1。转换部分 402 使用数据 D_i (输入数据 A) 及内部转换参数 401 (参数 X, Y 和 Z) 来执行指定运算，从而计算加密数据 C_i (输出数据 B)。

更具体而言，当接收输入数据 A 时，依照在转换部分 402 中所示的指定表达式来计算输出数据 B。注意到：在所述表达式中，由圆形加号来表示的符号，是指异运算。换言之，通过输入数据 A 和内部转换参数 401 (参数 X, Y 和 Z) 来计算输出数据 B。将运算结果或输出数据 B 输出作为加密数据 C_i ，并且它也被输入到参数修改部分 304。参数修改部分 304 接收加密数据 C_i ，并依照所示指定的转换表达式来使用该加密数据 C_i ，从而更新参数 X, Y 和 Z 的值。

参数修改部分 304 将作更具体地描述。例如，如果在图 4A 中输入数据 A 为 1，则转换部分 402 执行指定运算并且输出数据 B 为 4。输出数据 B (= 4) 被输入到参数修改部分 304，并为参数 X, Y 和 Z 执行运算。运算的结果是，参数 X, Y 和 Z 值被分别更新为 3、6 和 2。更新后的参数 X, Y 和 Z 值被用作在对要加密的数据 301 的数据 D1 的后继数据 D2 进行加密时的内部转换参数 401。此后，为每个数据 Di 重复相似的处理，直到达到要加密的数据 301 的最终数据 Dz。

要加密的数据 301 具有如上所述的已被相继加密的每个数据 Di，以用于生成加密数据 Ci。接着，在获取伪造检测数据 (S103) 的步骤中，获得对应于最终的内部转换参数 401 的加密处理信息 PF (z+1) 作为伪造检测数据 308。将已获得的伪造检测数据 308 附加到加密数据 C1 - Cz 上，以完成加密数据 305。加密处理由此而结束。

现将对图 3 中所示的解密步骤 202 进行描述。当获得加密数据 305 时，使用与加密算法相应的解密算法，来按在加密处理中所应用的数据单位执行解密处理。在解密步骤 202，加密数据 305 具有已提取的加密数据 Ci，并且对照解密处理信息 DFj 将所述加密数据 305 转换成原始数据 Di，其中 j = 1, 2, ... z, z+1。作为结果，生成了数据 D1 - Dz 的解密数据 307。在解密处理之前，先利用等同于在加密处理中所采用的加密密钥 302 来初始化解密处理信息 DF1。在图 4B 中示出了解密处理的一个例子。

注意到：在解密处理中使用的加密密钥 302，可由发送加密数据 305 的用户预先告知。或者，可将所述密钥包含在加密数据 305 的一部分当中，并且在发送加密数据 305 的同时将所述密钥发送出去。这里，在解密处理中所采用的加密密钥 302 可以经任意过程加以获得。

图 4B 示出了对图 3 中加密数据 Ci 进行解密以生成数据 Di 作为解密数据 307 的解密处理的过程。在图 4B 中，输入数据 B 表示图 3 中的加密数据 Ci，而输出数据 A 表示图 3 中解密数据 307 的数据 Di。如在图 4A 和 4B 中所示，这个解密处理类似于加密处理，包括：与解密处理信息 DFj 相对应的内部转换参数 401、转换部分 402 以及参数修改部分 304，其执行对应于加密处理的逆向形式的运算。内部转换参数 401 具有参数 X, Y 和 Z，并且这些参数都具有在解密处理之前利用初始值为 K 的加密密钥 302 先被初始化的值。这里，同样是在加密处理中，

将参数 X, Y 和 Z 分别初始化为数值 6、2 和 1。转换部分 402 使用加密数据 Ci (输入数据 B) 和内部转换参数 401 (参数 X, Y 和 Z) 来执行指定的运算, 从而对加密数据 Ci 进行解密以提供数据 Di (输出数据 A)。换言之, 输出数据 A 是依据输入数据 B 和内部转换参数 401 (参数 X, Y 和 Z) 来加以计算的。输入数据 B 被输入到转换部分 402 以及参数修改部分 304。参数修改部分 304 按照已接收的输入数据 B 和所示的指定转换表达式, 来更新内部转换参数 401 (参数 X, Y 和 Z) 的值。

这里, 如果要加密的数据 D1 具有数值 1, 那么加密数据 C1 就具有数值 4。因此, 在图 4B 中值为 4 的数据 B 是输入, 而转换部分 402 对其执行运算, 并输出值为 1 的数据 A, 所述数据 A 与原始数据 D1 同值。当加密数据 305 由此而无伪造时, 加密处理信息 PFj 与解密处理信息 DFj 相等。由此, 如果要加密的数据 301 具有每个数据单位或者具有伪造的部分数据 Di 的数据 D1 - Dz, 那么对应于数据 Di 的加密处理信息和解密处理信息就不匹配, 并且加密与解密处理信息 PFj 与 DFj 可以分别用作伪造检测数据 308 与 309。

此外, 数据 B (具有数值 4) 被输入到参数修改部分 304, 并且对内部转换参数 401 (参数 X, Y 和 Z) 进行运算, 并分别将它们更新为数值 3、6 和 2。将具有已更新值的参数在解密数据 C2 时用作内部转换参数 401。此后, 类似地重复解密处理, 直到达到数据 Cz 为止。

针对加密数据 C1 到 Cz, 执行上述解密处理以生成解密数据 307 的数据 D1 - Dz。然后, 在 S203, 获得 (或生成) 最终的解密处理信息 DF (z+1), 以作为伪造检测数据 309, 并且在 S204, 对于附加到加密数据 304 上的伪造检测数据 308 与所获得的伪造检测数据 309 是否相匹配而作出判定。如果所述数据相匹配, 则就判定加密数据 305 或者要加密的数据 301 被正常接收, 而没有被伪造。否则, 就判定所述数据已被伪造。

内部转换参数的另一个例子

对于如上所述的伪造检测数据 308 而言, 正好使用了内部转换参数 401 中参数 X, Y 和 Z 的三个值, 并且如图 1 中所示的生成伪造检测数据的步骤 103 并未实施任何步骤。然而, 如果使用不同类型的加密处理, 那么就要结合内部转换参数 401 来处理大量数据。在此情况下, 与加密数据 305 有关的附加数据量就不容忽略。在此情况下, 在生成

伪造检测数据 (S103) 的步骤中，可以从最终的内部转换参数 401 来获得报文摘要 (MD)，并且将所述报文摘要作为伪造检测数据而附加于加密数据 305 (S104)。

图 5 示出了与如之前所述的加密步骤不同的加密步骤。这里，未示出相对应的解密处理，这是由于其配置就是加密处理的逆向形式。图 5 的加密系统具有：对应于加密处理信息 PFj 的内部转换参数 501、转换部分 1202 以及参数修改部分 1203。在图 5 的系统中，按所预定的那样，将作为数据 A 而接收的要加密的数据 301 顺序转换成加密数据 305，并输出为数据 B。在此例中，内部转换参数 501 具有 256 个转换表 T(0), T(1), ..., T(255)。转换部分 1202 使用转换表 T(0) 至 T(255)、按字节将要加密的数据 301 转换成加密数据 305。参数修改部分 1203 使用输出的加密数据 305 的信息来更新转换表 T(0)至 T(255) 的内容 (或值)。在加密处理之前，先利用初始值为 K 的加密密钥 302 对所述内部转换参数 501 的内容进行初始化。

例如，如图 5 中所示，如果转换表 T(0) 具有数值 6、转换表 T(1) 具有数值 2、……、且输入数据 A 为 0，那么输出数据 B 就为 6，而如果输入数据 A 为 1，则输出数据 B 就为 2。

参数修改部分 1203 从已接收输出数据 B 以及特定的函数 “f” 和 “g” 获得将要交换的两个值 “idx1” 和 “idx2”，并且交换表 T(idx1) 与 T(idx2) 的值。例如，如图 5 中所示，“idx1” = 0 而 “idx2” = 4，并且交换表 T(0) 与 T(4) 的值。作为结果，表 T(0) 具有从 6 更新为 4 的值，且类似地表 T(4) 具有从 4 更新为 6 的值。

尽管这里未示出，但是解密处理具有作为内部转换参数的表，所述表执行与加密处理转换的逆向形式相对应的转换，并且当执行与加密处理转换的逆向形式相对应的转换处理的同时，所述解密处理顺序地更新表的内容。

对于图 5，内部转换参数 501 对应于 256 个数据大小，所述数据大小非常大从而无法用作伪造检测数据 308。因此，转换内部转换参数 501 以提供降低的数据量。例如，这可以通过利用能依据大量数据来生成特定字节数量的数据的诸如 MD5 (报文摘要 5)、安全哈希算法 1 (SHA-1)、以及类似算法之类的哈希函数来完成，不过不局限于此。或者，可以不使用哈希函数，并且内部转换参数 501 可能仅仅具有提供作为

已转换数据的一部分。如果将内部转换参数 501 用作伪造检测数据 308，则这种转换处理就能降低伪造检测数据 308 的量。

此外，解密处理也能使用在生成伪造检测数据的步骤 103 中所使用的手段，来获得相同的结果。因此，通过将附加于加密数据的伪造检测数据与在解密处理过程中所获得的伪造检测数据进行比较，就能够作出关于要加密的数据 301 或加密数据 305 是否已被伪造的判定。

因此，通过执行如下处理就降低伪造检测数据 308 的大小，所述处理为内部转换参数 501 使用了哈希函数。一般而言，由于与要加密的数据 301 作了比较，内部转换参数 501 具有非常小的数据量，并且使用哈希函数来实现转换处理，如上所述那样，不会引起降低整体处理效率。

第二实施例

在第一实施例中，利用在要加密的数据 301 被完全加密 (S102) 和解密 (S202) 时所获得的加密处理信息 PF (z+1) 和解密处理信息 DF (z+1)，来生成伪造检测数据 308 和 309。在本发明的实施例中，将要加密的数据 301 划分成多个块，并且利用在每个块完全被加密时所获得的加密处理信息以及每个块被完全解密时所获得的解密处理信息，来生成伪造检测数据。

图 6A 示出了已被划分成 n 个块 B_k 的要加密的数据 301，其中 k = 1, 2, 3, ..., n。虽然期望块 B_k 是所用加密处理单位的整数倍，但是所述块可以具有依处理设备的存储器容量、处理能力等等而确定大小的数据，其中所述处理设备发送及接收要加密的数据 301。例如，DES 允许采用 64 位单位进行加密，而由此块 B_k 具有 64 位整数倍的大小。如果按位来提供加密，则块 B_k 就可具有任意大小。

图 6B 示出了在对图 6A 中所示的要加密的数据 301 进行加密之后所获得的加密数据 305 的数据结构。如图 6B 中所示，加密数据 305 由加密块 CB_k 和伪造检测数据 BD_k 构成，其中 k = 1, 2, 3, ..., n，并且加密块 CB_k 与伪造检测数据 BD_k 之间存在一一对应。每当对块 B_k 完全进行了加密，就会生成伪造检测数据 BD_k，并将数据 BD_k 附加到随后与之相应的加密块 CB_k 上。更具体而言，轮流为每一块 B_k 记录下加密 CB_k 及为块 CB_k 的数据所计算的伪造检测数据 BD_k。在本发明的实施例中，要加密的数据 305 可具有除上述结构之外的结构。例如，如图 6C 中所

示，可将加密块 CB₁-CB_n 数据和伪造检测数据 BD₁-BD_n 分别记录在不同位置上。

依照本发明的实施例，加密与解密处理分别如图 7 与 8 中所示那么执行。类似于第一实施例中那些步骤的任何步骤都将不作描述。

在加密处理中，如图 7 中所示，最初从要加密的数据 305 来获得预定大小的单个块 B_k 的数据 (S601)，并将该数据加密 (S602)。当块 B_k 的数据完全被加密时，获得加密处理信息 PF_k，并且利用这个信息来生成伪造检测数据 BD_k (S603)，并将加密块 CB_k 及伪造检测数据 BD_k 存储起来以提供如图 6B 或 6C 中所示的数据结构 (S604)。针对要加密的数据 301 的所有块 B_k 重复这一系列步骤 (S605)。由此而获得 (生成) 加密数据 305。

在解密处理中，如图 8 中所示，最初读取这样所获得的加密数据的伪造检测数据 BD_k 和与之相应的加密块 CB_k (S701)，并且实施解密处理 (S702)。然后，使用解密处理信息 DF_k 来生成伪造检测数据 (S703)，并且作出关于已生成的伪造检测数据与在 S701 所读取的伪造检测数据 BD_k 是否匹配的判定 (S704)。如果它们匹配，则就获得解密数据 (S705)。否则，判断加密数据 305、或者由加密数据 305 所表示的要加密的数据 301 已被伪造，并且对于解密处理将会产生错误 (S706)。类似地，针对所有加密块 CB_k (S707) 重复这一系列的步骤，从而获得解密数据 307。

因此，将要加密的数据 301 划分成多个块 B_k，并将伪造检测数据 BD_k 附加到每块 B_k 上，使对应每块 B_k 的要检测伪造能够找出已伪造的部分要加密的数据 301 的位置。除了与已伪造的部分要加密的数据 301 相对应的那些块之外，也能正常地对其它块 B_k 进行解密。例如，如果通信错误发生，且导致要加密的数据 301 (加密数据 305) 被局部破坏，则就能使所述数据被最小限度地损坏。

第三实施例

同上述每个实施例的特定应用一样，第三实施例针对的是分发电子书数据（在下文中称为“电子书内容”）的系统。

图 9 示出了电子书内容分发系统。这个系统包括：内容产生设备 801、服务器设备 802、数据显示设备 803，以及允许设备 801 与 802 相互之间进行通信、同时允许设备 802 与 803 相互之间进行通信的网络 804。内容产生设备 801 由通用个人计算机构成，用以产生电子书内

容。内容产生设备 801 包括：内容输入部分 805、实施如先前所述的这种加密处理的数据加密处理部分、以及发送与接收部分 807。内容创建器经由内容输入部分 805 来输入电子书内容 800。已输入的电子书内容 800 由加密处理部分 806 来进行加密，并且经由网络 804、通过发送与接收部分 807 将已加密的电子书内容 800 发送至服务器设备 802。

虽然这里的电子书内容 800 从外部被输入到内容产生设备，但是用户可以操作内容输入部分 805 来产生所述内容。

电子书内容 800 具有例如被分隔成要加密的数据 301 和加密数据 305 的数据结构，如图 10A 和 10B 中所示的那样。一般而言，通常将电子书内容配置成包含多个文件，这些文件包括：描述主文本的文本文件、诸如图表、图片或照片之类的图像文件、诸如音效之类的音频文件等等。在本实施例中，如图 10A 中所示，对应于要加密的数据 301 的电子书内容 800 从顶部开始包括有：表明电子书内容 800 中所包含文件数目的数据 FM 和每个文件的文件信息 FD_h，其中 $h = 1, 2, 3, \dots, n$ 。如图 10B 中所示，对应于加密数据 305 的电子书内容 800 包括：对应于各个文件信息 FD_h、且通过对文件信息 FD_h 的内容进行加密而获得的文件数据 FDCh，其中 $h = 1, 2, 3, \dots, n$ 。例如，如果电子书内容 800 包含文本文件、图像文件和音频文件这三个文件，则文件信息 FD1、FD2 和 FD3 就将分别包括文本数据、图像数据和音频数据。文件信息 FD_h 包括相应文件的信息，就比如：文件名、与文件中所存储数据相关的偏移量值、文件中所存储的数据大小、以及所使用的加密方法和密钥。

由加密处理部分 806 依照先前在每个实施例中所述的方法来对文件信息 FD_h 进行加密。对于文件信息 FD1，将感兴趣的文件划分成多个块，并对其按块进行加密，以转换成文件信息 FDC1。对于文件信息 FD2，使感兴趣的文件全部都经过加密，以转换成文件信息 FDC2。按块还是整个地对文件的数据进行加密，要依数据的类型而定。更具体而言，如果数据为文本数据、音频数据或电影图像（视频）数据，则按块来加密数据就允许对数据进行随机访问和再现以进行解密。这能提供比对数据进行完全解密的情况更短的访问时间。此外，如果数据是不被部分访问的静态图像或类似数据，则可对数据整个地进行完全加密。

在图 9 中，服务器设备 802 由通用个人计算机构成，并且包括：发送与接收部分 808 和内容数据库 809。通过内容产生设备 801，由发

送与接收部分 808 来发送和接收已加密的电子书内容 800。所接收到的电子书内容 800 被存储到内容数据库 809 中。数据显示设备 803 经由网络 804 来发出发送请求。所述请求被发送与接收部分 808 接收，并且作为响应，从内容数据库 809 中读取由已接收请求表示的、与电子书相应的加密内容，并且经由网络 804、通过发送与接收部分 808 将所述内容发送至数据显示设备 803。

数据显示设备 803 由信息处理设备构成。数据显示设备 803 包括经由网络 804 发送和接收数据的发送与接收部分 810、处理用户指令的用户指令处理部分 811、存储电子书内容的存储设备 812、对加密电子书内容进行解密的数据解密处理部分 813，已如前所述的、以及包括在屏幕上显示电子书内容的显示单元 814。

用户经由用户指令处理部分 811、根据显示在屏幕上的电子书内容的菜单来选择期望的电子书内容。作为响应，发送与接收部分 810 向服务器设备 802 发送请求，以发送选定的内容。随后，服务器设备 802 发送加密的电子书内容，所述内容又由发送与接收部分 810 加以接收并存储到存储设备 812 中。由数据解密处理部分 813 对存储到存储设备 812 中的加密电子书内容进行解密，并且数据显示设备 814 将作为结果的、原始电子书内容 800 显示在屏幕上。在这种情况下，如果作出适配，对仅能一次显示的数据量进行解密，则就能以比当解密全部数据时所花时间更短的一段时间来解密和显示数据。更具体而言，按照对应于显示缓冲器大小的块数，来对按块进行加密的电子书内容进行解密，所述显示缓冲器与数据显示单元 814 相关联。对于电子书内容，最初都典型地显示顶部页。由此，按照对应于显示缓冲器大小的块数、从顶部开始对电子书内容 800 进行解密。

此外，当经由用户指令处理部分 811 接收用户指令例如来进行翻页、输出声音等之时，从存储设备 812 那里获取指令所需的数据，并由数据解密处理部分 813 来对其进行解密，并且当实施解密时判断伪造是否存在。如果判定伪造存在，则数据显示单元 814 就显示数据，或者音频输出部分（未图示）就输出声音。如果判定所述数据为伪造数据，那么就可以相应地告知用户以中断当前处理。

尽管在本实施例中对电子书内容进行加密并从而进行分发，但是也可以对除电子书内容之外的信息进行加密和分发。例如，可以对音

乐数据、运动图片数据以及程序进行加密和分发。

第四实施例

第二实施例的另一个特定应用，将参照图 11 和 12 来作描述。在本实施例中，考虑的是一种数字内容分发系统。为说明起见，这个系统类似于图 9 中所示的系统。在本实施例中，数字内容不限于电子书内容，而可以为音乐数据、视频数据等等。

典型地，可以经网络来获取数字内容，并且为说明起见，第三方未对经网络所发送和接收的数据进行伪造。换言之，为说明起见，仅仅将能合法获得的数据经网络进行传递。然而，经网络而通信的数据会由于通信错误等原因而被丢失。在这种情况下，合法获得的数字内容就无法得以再现。为了再现数字内容，就必须再次访问并获取数字内容的所有数据。在本实施例中将要描述能解决如下情况的过程，所述情况是：当在网络上通信数据时，数据就被丢失。

图 11 示意性示出了图 9 的服务器设备 802 中和数据显示设备 803 中的数据。更具体而言，该图示出了与在服务器设备 802 当中存储于内容数据库 809 中的加密数据 305 相应的数字内容，在网络 804 上被发送到数据显示设备 803，并且被存储到存储设备 812 中。对于数字内容的加密数据 305 具有每个加密块 CBk 和与之相应的伪造检测数据 BDk 被分开的结构，如在第二实施例中所描述的。为说明起见，在数据显示设备 805 中存储于存储设备 812 中的且与数字内容相应的加密数据 305 的加密块 CB2，例如因通信错误而具有伪造的数据。

当数据显示设备 803 操作以允许再现（或解密）时，由相应的伪造检测数据 BD2 来在加密块 CB2 中检测伪造。作为响应，数据显示设备 803 告知服务器设备 802：加密块 CB2 被伪造。服务器设备 802 随应地仅将加密块 CB2 及伪造检测数据 BD2 重发至数据显示设备 803。已接收到这些重发数据的数据显示设备 803 能够提供再现。应当注意到：仅仅把全部内容（或全部加密数据 305）的一部分从服务器设备 802 重发至数据显示设备 803。如果检测到伪造，并且合法数据将被再次通信及获取，则其就能在一段减少的时间中加以通信。

图 11 中与数据显示设备 803 有关的过程，将参照图 12 的流程图来加以描述。现在将对数字内容进行解密和再现。更具体而言，数据

显示设备 803 最初获取加密数据 305 的第一加密块 CB1 以及伪造检测数据 BD1 (S1301)。对已获得的加密块 CB1 进行解密 (S1302)。用类似于第二实施例中所述的方式来实施这一解密。利用解密处理信息来生成伪造检测数据 (S1303)。将附加于加密块 CB1 的伪造检测数据 BD1 与在 S1303 所生成的伪造检测数据进行比较，来判断它们是否匹配 (S1304)。如果匹配，则就获取解密数据 (S1305)，并且判断是否存在后续加密块 (S1307)。如果存在，则处理就返回至 S1301。否则，处理就结束。

如果判定所述数据不匹配，那么就判断加密块 CB1、或者由加密数据 CB1 所表示的块 B1 被伪造，并再次经网络 804 从服务器设备 802 那里获取加密块 CB1 (S1306)。因此，就能解决因网络 804 上的通信错误而造成的伪造。

尽管在图 11 中数字内容是存储在数据显示设备 803 中的存储设备上 812 的，但是也可通过网络 804 来接收数字内容并加以再现。例如，从内容的顶部顺序地再现音乐、图像等。照此，如果数据顶部存在，则就能开始再现。换言之，数据被通过网络 804 接收，而同时所述数据能够被再现。图 13 示意性示出了在这种情况下服务器设备 802 中的数据和数据显示设备 803 中的数据。

图 13 示出了在网络 804 上、将在服务器设备 802 中存储于内容数据库 809 中的加密数据 305 的数字内容发送至数据显示设备 803。在图 13 中，服务器设备 802 仅仅将加密块 CB1 和 CB2 传递至数据显示设备 803 上，并且后续加密块由要获得的数据 900 来表示。在数据显示设备 803 中，数据解密处理部分 813 开始解密处理。这样一来，就相继从加密块 CB1 那里读取数据，并且让已读取的加密块 CB1 数据经过解密以及伪造检测。如果检测表明数据未被伪造，则就直接对其进行再现。如果已读取的加密块 CB2 被伪造，则数据显示设备 803 就将信息 901 输出到服务器设备 802 上，以表明加密块 CB2 被伪造，并且数据显示设备 803 就再次从服务器设备 802 那里接收和获取加密数据块 CB2 以及相应的伪造检测数据 BD2。此后，类似地获取并再现后续块。

这种过程提供了降低的传输时间，并且经过网络 804 可连续不断地获取加密数据 305、对所述加密数据进行解密和再现。

第五实施例

在上述每一个实施例中所述的加密与解密处理，均能部分或全部地以执行这种过程的程序或硬件逻辑形式来提供（所述程序是指适用于由计算机执行处理的有序指令串）。

如果其是以程序形式提供的，则就能将该程序安装在信息处理设备中以实施期望的处理。在这种情况下，可以把所述程序预先记录在计算机可读记录介质中并加以提供。作为选择，可以经网络将其从服务器设备上下载或提供到信息处理设备中，或者可预先将其安装在信息处理设备中并加以提供。

图 14 示出了信息处理设备的配置，所述信息处理设备能执行如上述每一个实施例中所述的加密与解密处理的程序。图 14 的配置对应于图 9 的内容产生设备 801、服务器设备 802 及数据显示设备 803 中每一个的配置。参照图 14，所述信息处理设备包括：液晶或阴极射线管（CRT）等监视器 110、键盘 150、鼠标 160、中央处理单元（CPU）122、存储器 124，所述存储器配置成包括：只读存储器（ROM）或随机访问存储器（RAM）、硬盘 126、可拆卸地接纳 FD 132 以存取 FD 132 的软盘（FD）驱动设备 130、可拆卸地接纳 CD-ROM 142 以存取 CD-ROM 142 的光盘只读存储器（CD-ROM）驱动设备 140、以及将所述信息处理设备连接于网络 804 的通信接口 180，其中所述网络 804 适用于诸如因特网之类的各种网络。这些组件均通过总线而链接。可以给所述信息处理设备提供磁带设备，所述磁带设备可拆卸地接纳盒式磁带以存取磁带。

在本实施例中，上述记录介质可以是将要在图 14 的信息处理设备中实施的处理所需的存储器，比如存储器 124 本身，或者它也可以是磁带、FD 132 及 CD-ROM 142（未图示），或是当将其安置在磁带设备（未图示）中时可读的记录介质、FD 驱动设备 130、CD-ROM 驱动设备 140 或类似的程序读取设备。总之，存储在记录介质中的程序都可由 CPU 122 来访问并执行，或者一旦从记录介质中被读取或下载到图 14 中的指定存储区，例如存储器的存储区 124，就由 CPU 122 来读取并执行。这个下载程序是预先存储在感兴趣的信息处理设备中的。

注意到：上述记录介质是被配置成可从信息处理设备主体上分离的介质，并且它可以是容纳固定程序的介质。例如，它可以是：磁带、盒式磁带、或类似类型的带；FD 132、硬盘 126 或类似的磁盘；或是 CD-ROM 142/磁性光盘（MO）/迷你盘（MD）/数字多功能光盘（DVD）

或类似的光盘；IC 卡（包括存储卡）/光卡或类似的卡；或是掩膜式 ROM、可擦除可编程 ROM（EPROM）、电 EPROM（EEPROM）、闪速 ROM 或类似的半导体存储器。

此外，由于在本实施例中信息处理设备连接于上述网络 804，因而记录介质可以是接收经网络 804 下载的程序从而使得程序流动的记录介质。如果所述记录介质接收经网络 804 下载的程序，则就可以预先将下载程序存储在信息处理设备的主体中，或者预先将其从另一记录介质安装到所述信息处理设备的主体中。

注意到：记录介质可以存储除程序以外的内容。例如，它可以存储数据。

由此，如在每一个实施例中所述，由于实施具有伪造检测功能的加密处理，因而就可以生成转换参数值并将其用作为伪造检测数据，来消除计算伪造检测数据的处理，并且减少在加密处理中包含的量。同样也能减少解密处理的量。作为结果，加密与解密处理可以免除显著的工作量，并由此而快速地实施所述加密与解密处理。

此外，可以按块来对要加密数据进行处理，并且判断每一块是否存在伪造还是不存在伪造。照此，如果数据被伪造，则就能容易地对落入伪造范围的要加密的数据（或块）进行定位。另外，在那种情况下，可以对除伪造块以外的数据正常进行解密。另外，对于具有按时序再现的数据的音乐、视频、电子书及其它类似内容而言，首先仅能对所需部分（或块）进行解密，并且可以在所有数据皆完全被解密之前开始进行再现。

尽管已经详细地描述并说明了本发明，但是应当清楚地理解：上述内容仅仅是说明性和举例性的，而不是限定性的，本发明的精神和范围仅由所附权利要求来加以限定。

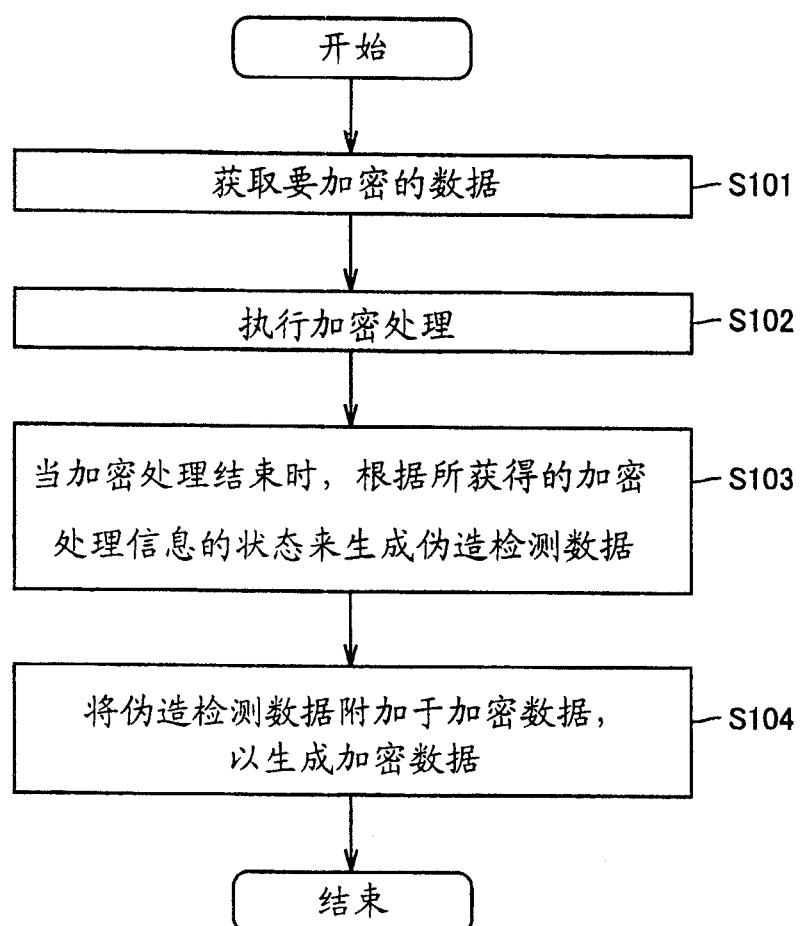


图 1

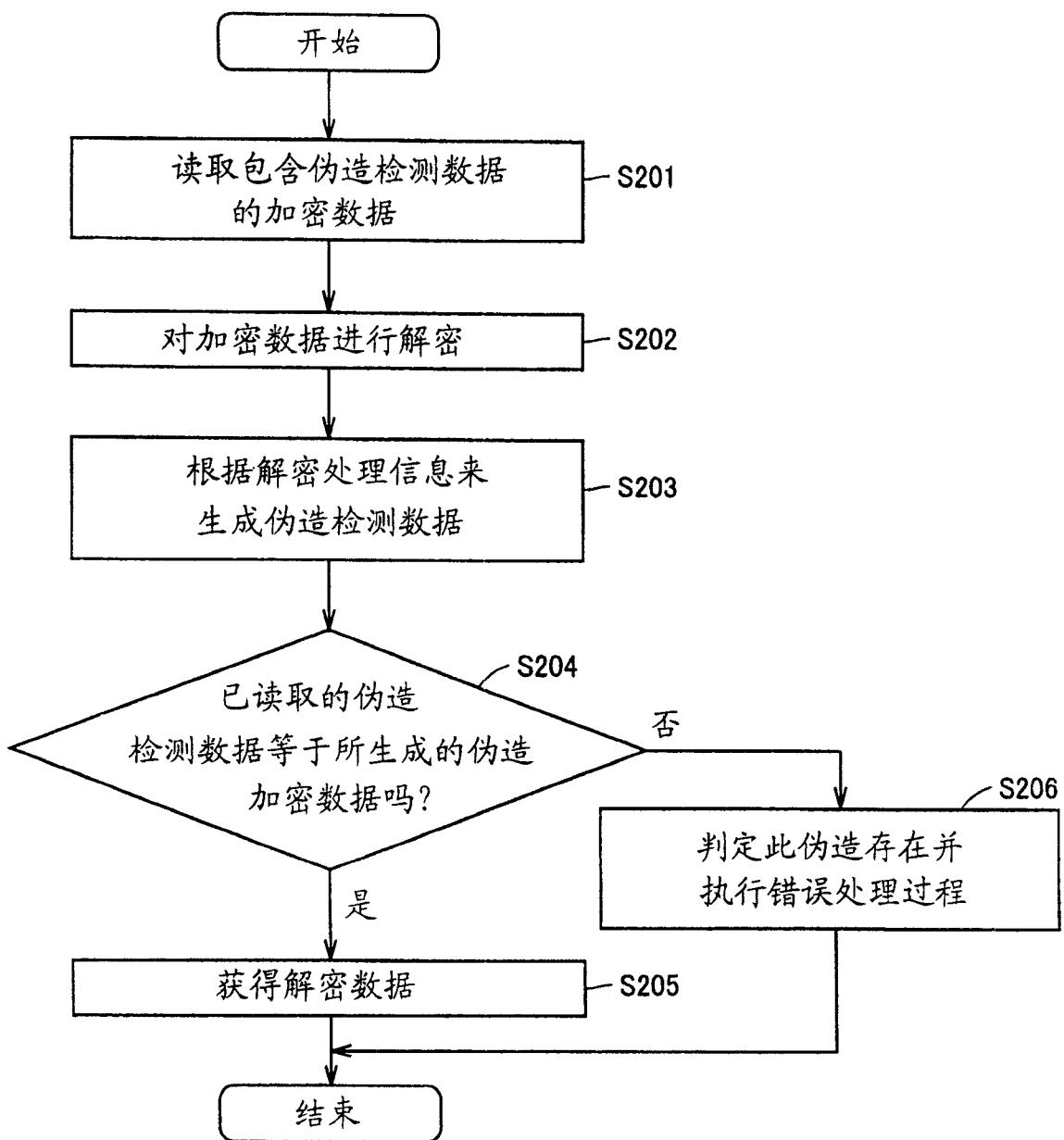
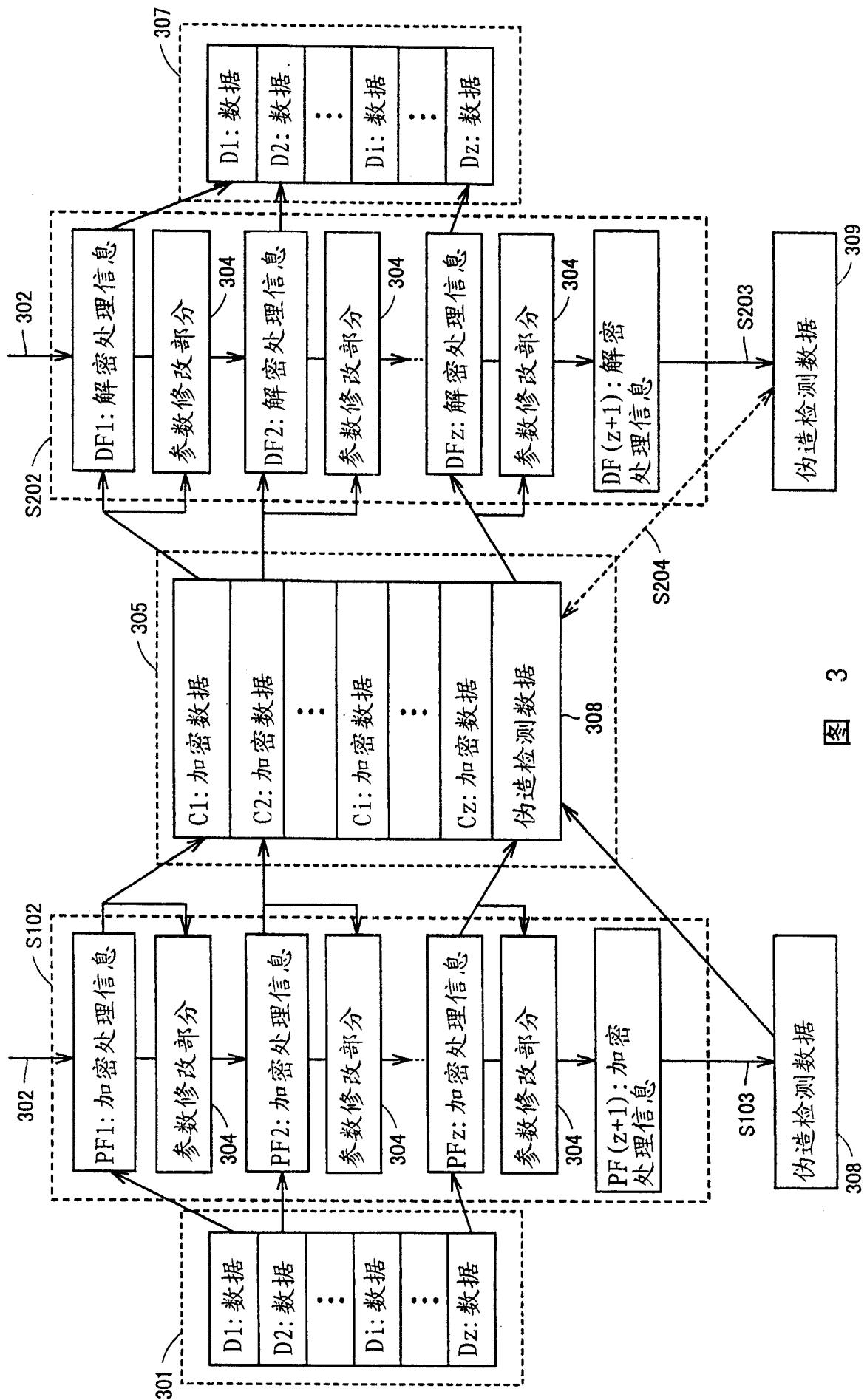


图 2



3

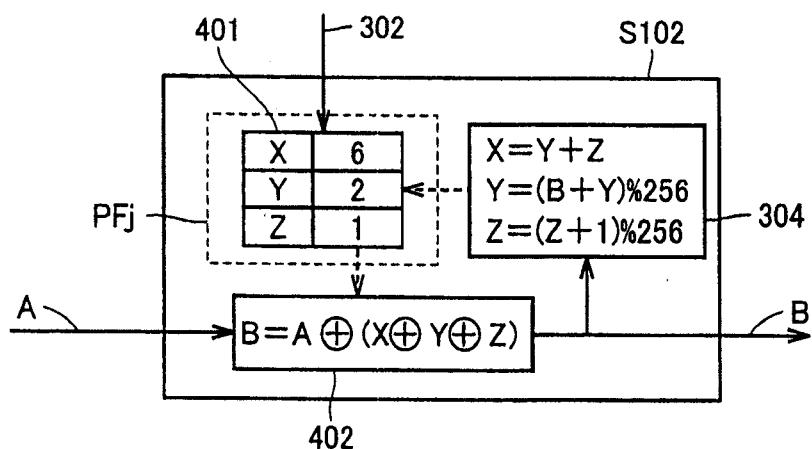


图 4A

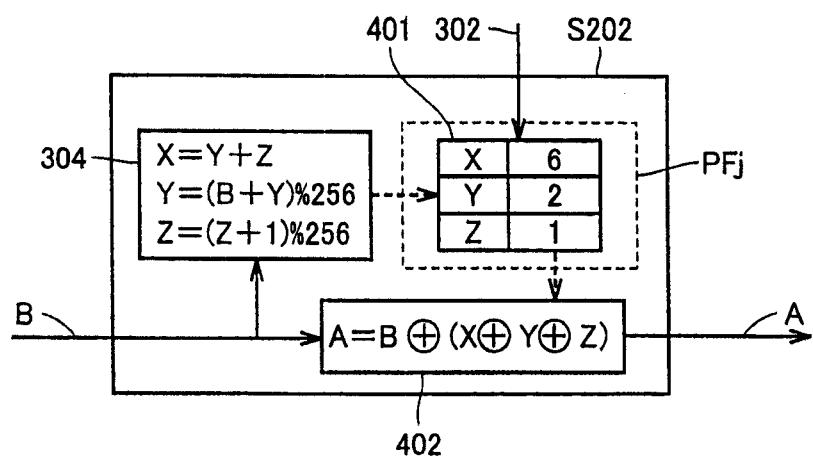


图 4B

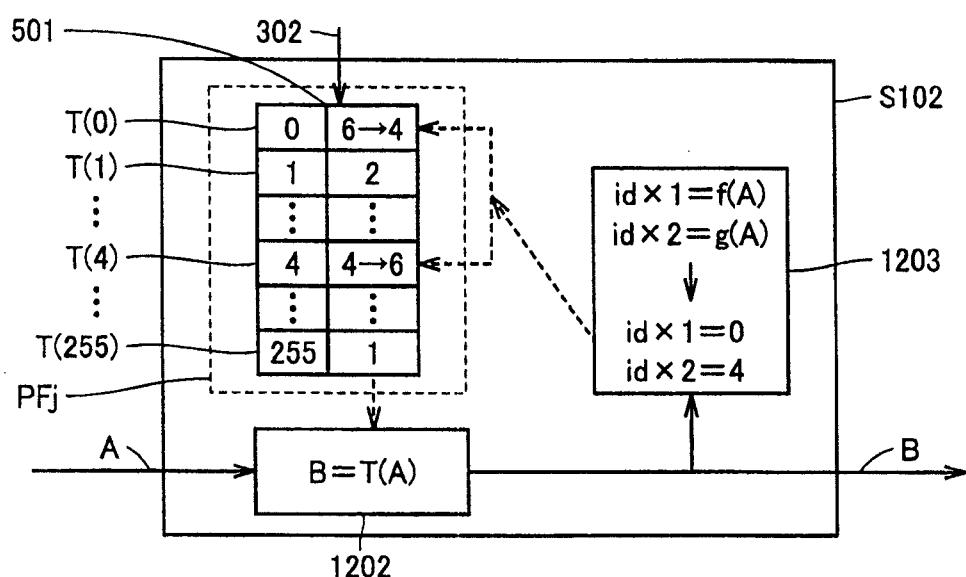
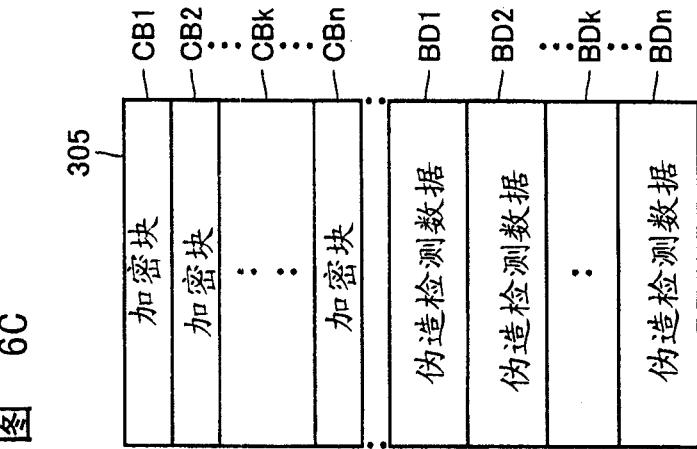
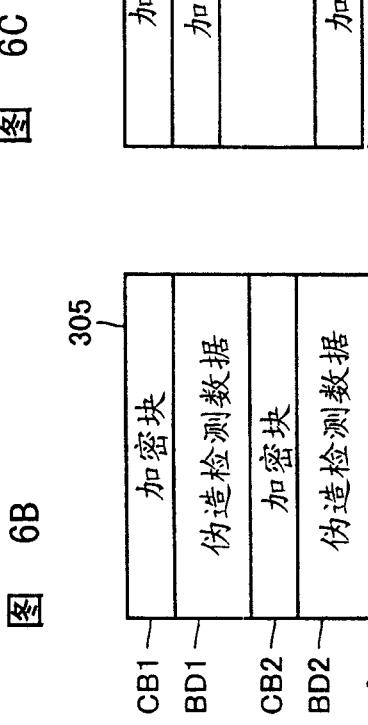
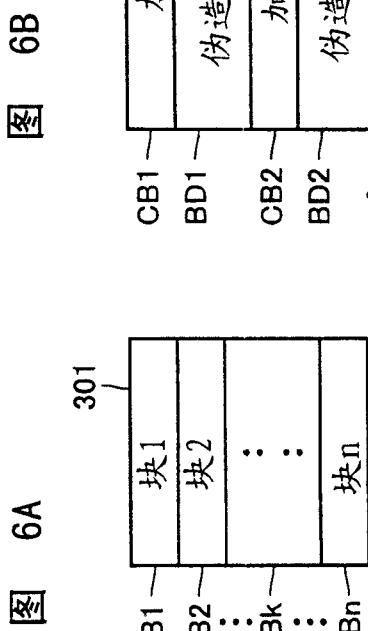


图 5



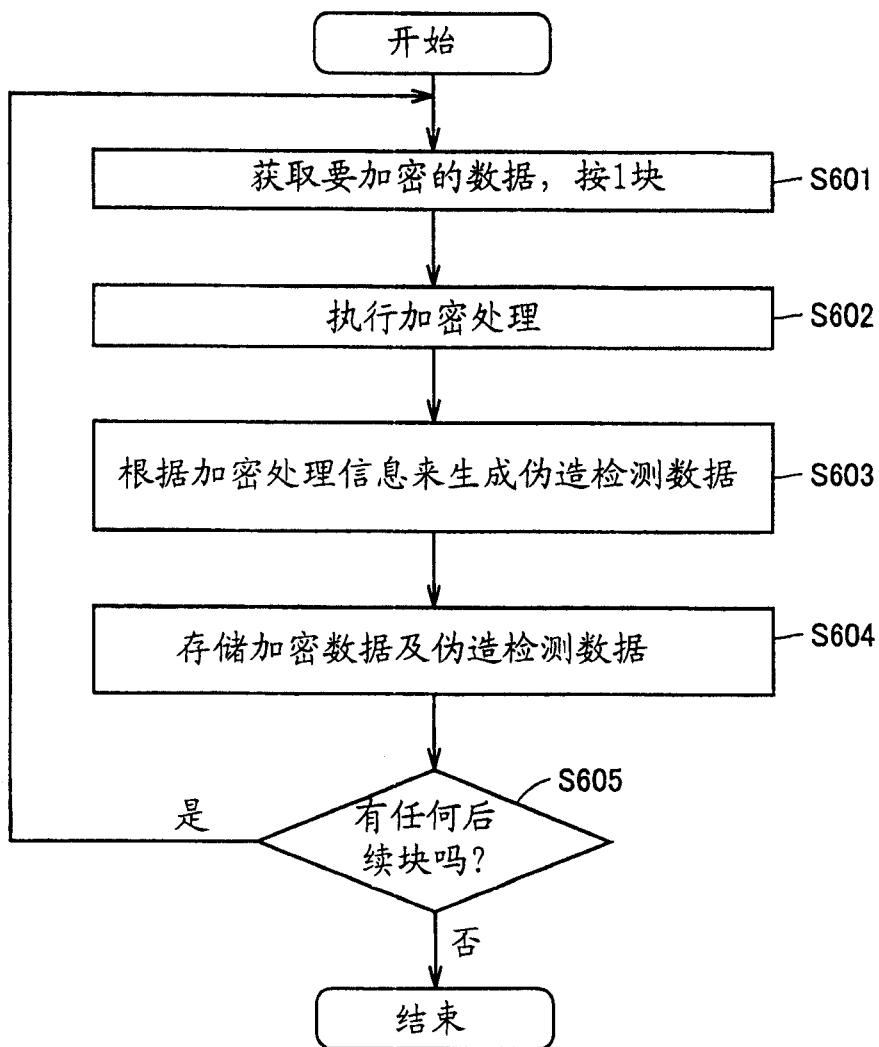


图 7

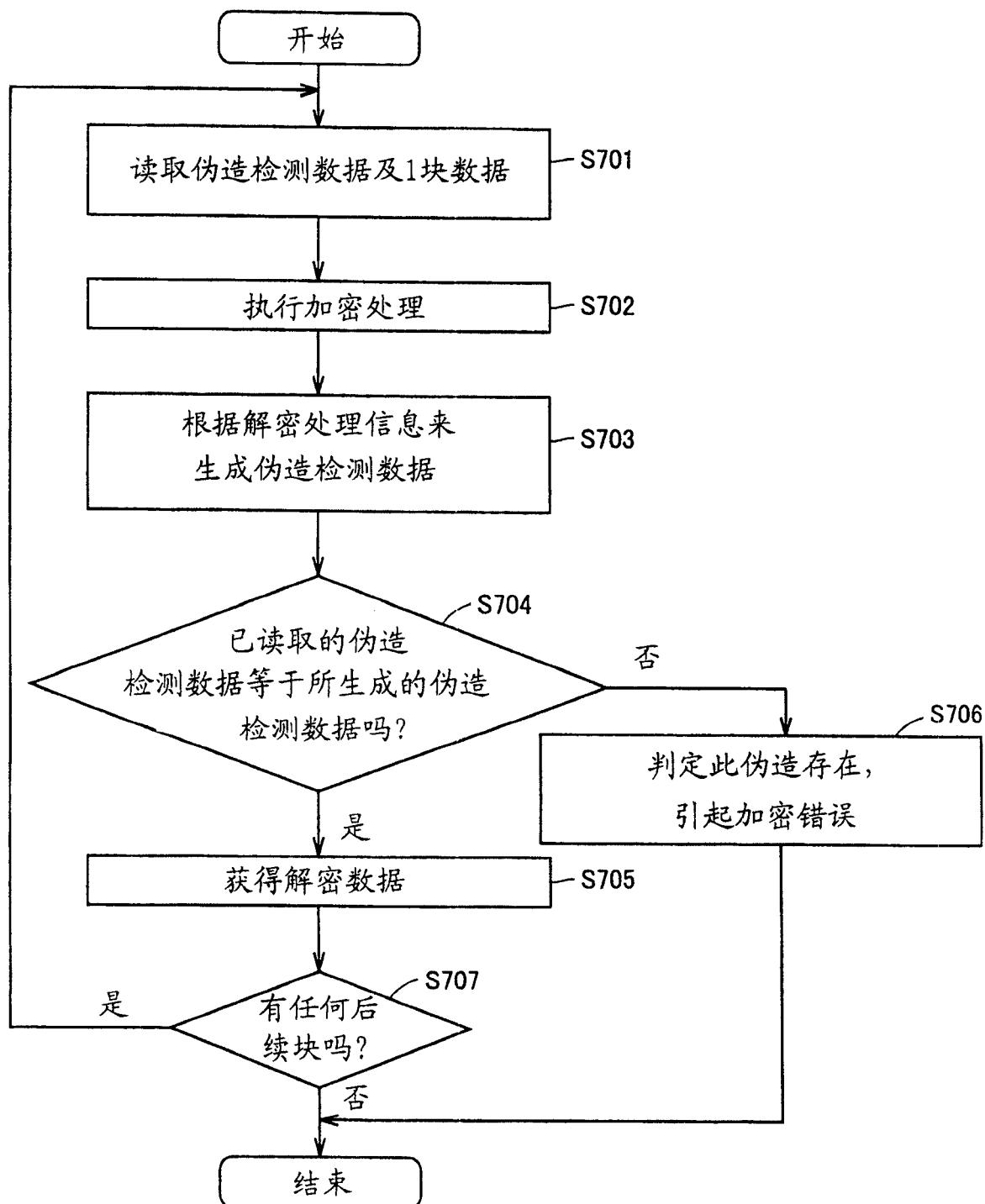


图 8

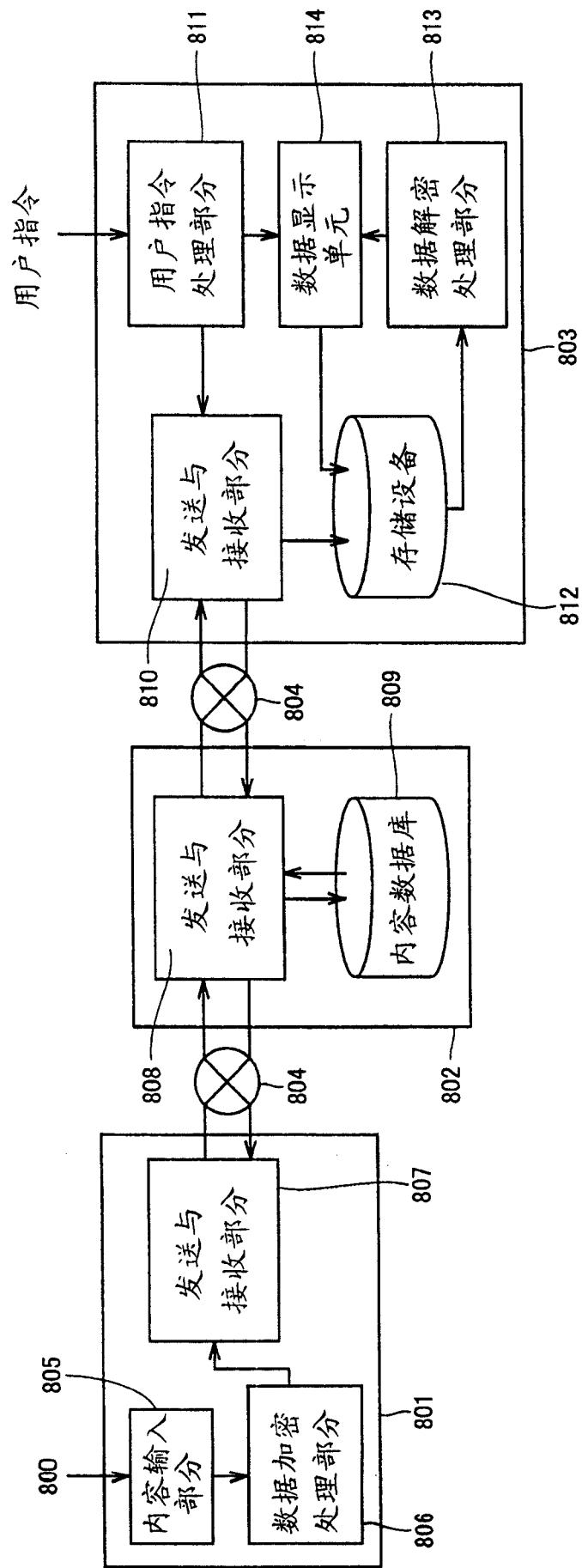


图 9

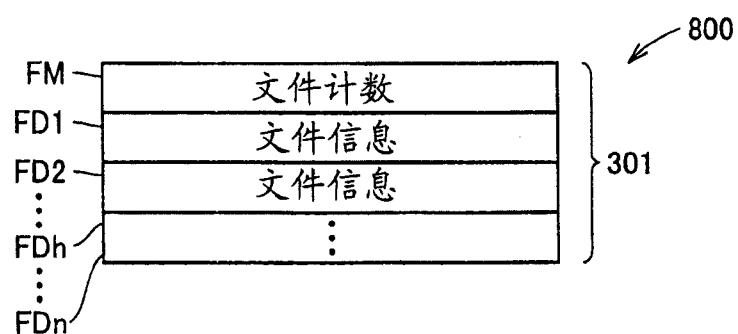


图 10A

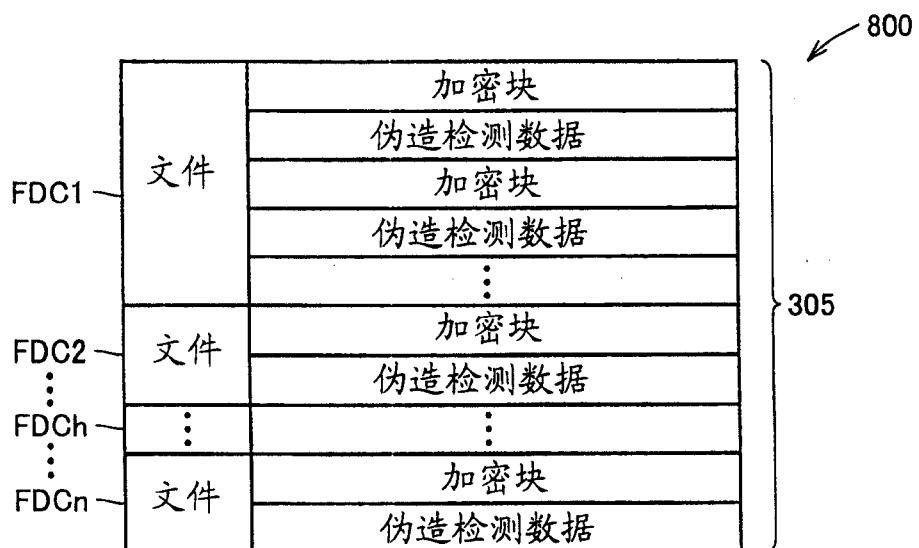


图 10B

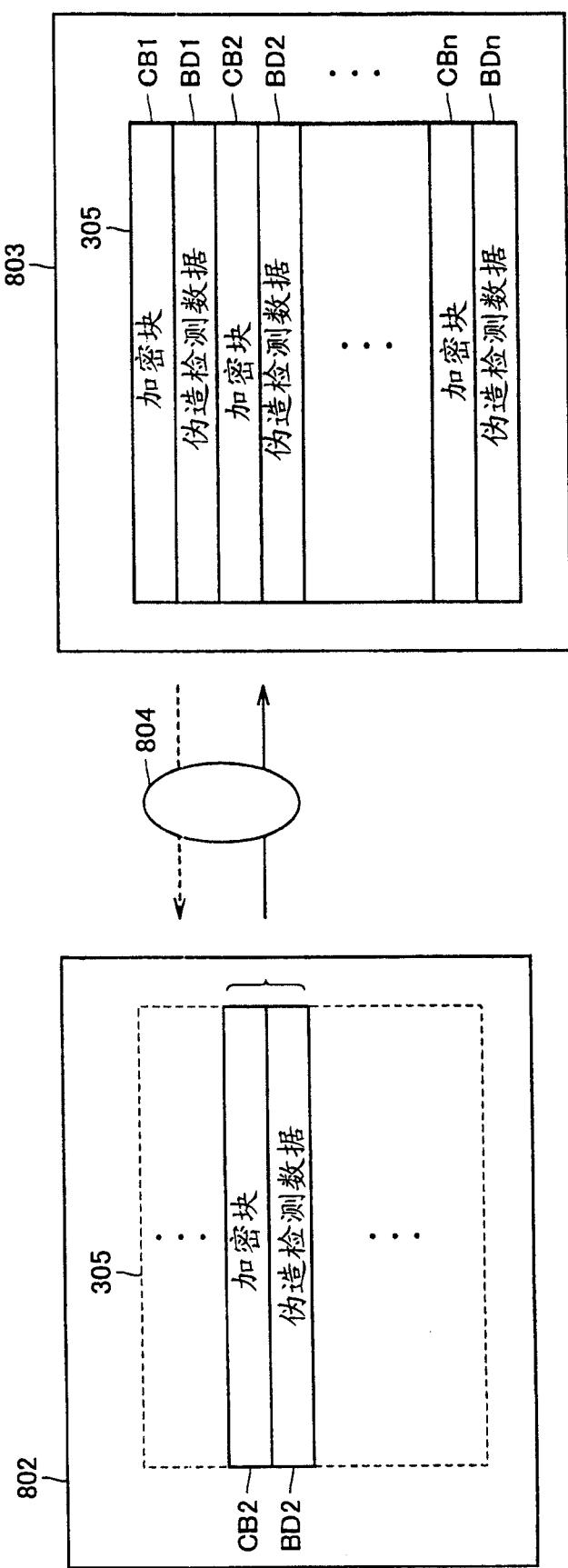


图 11

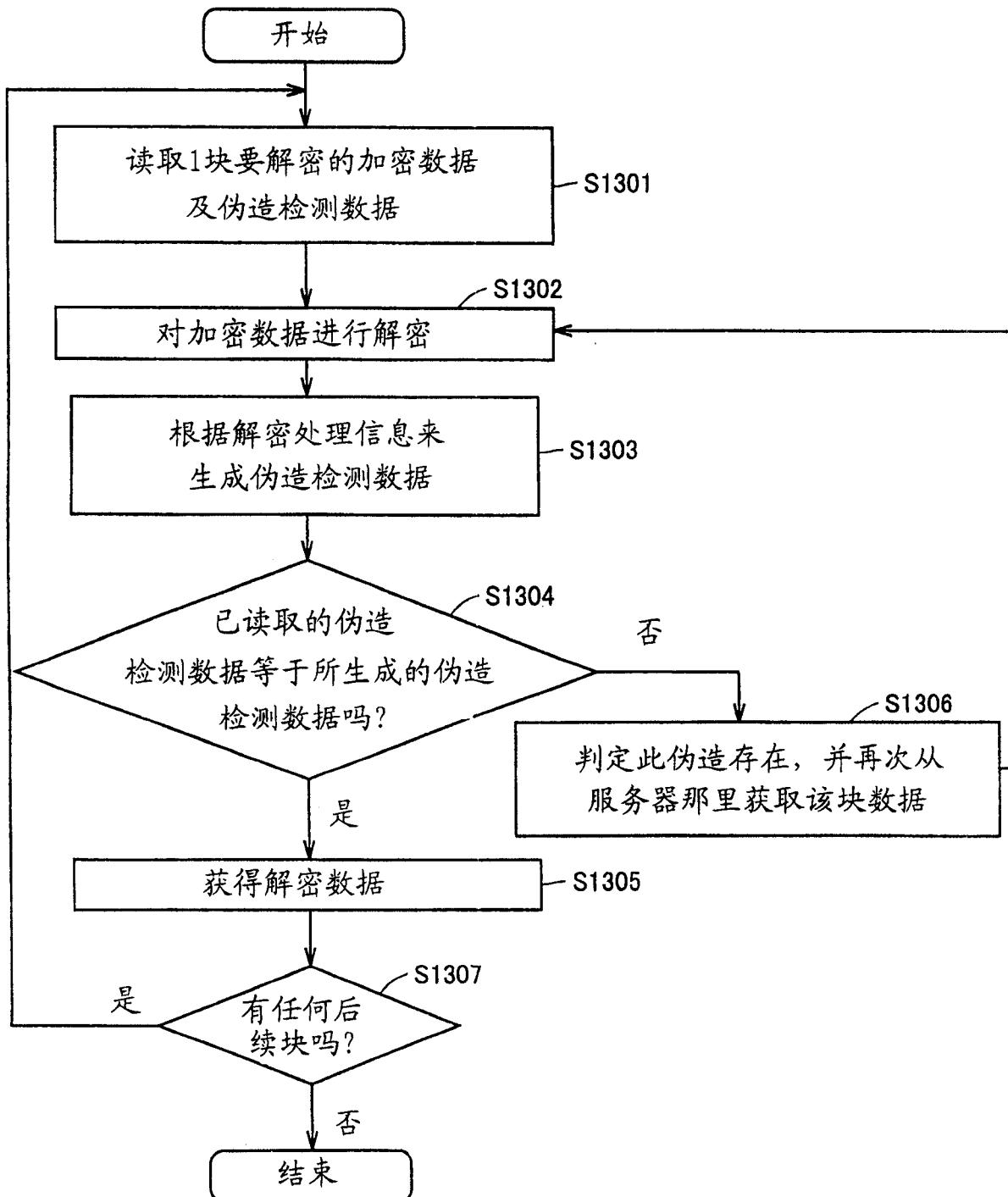


图 12

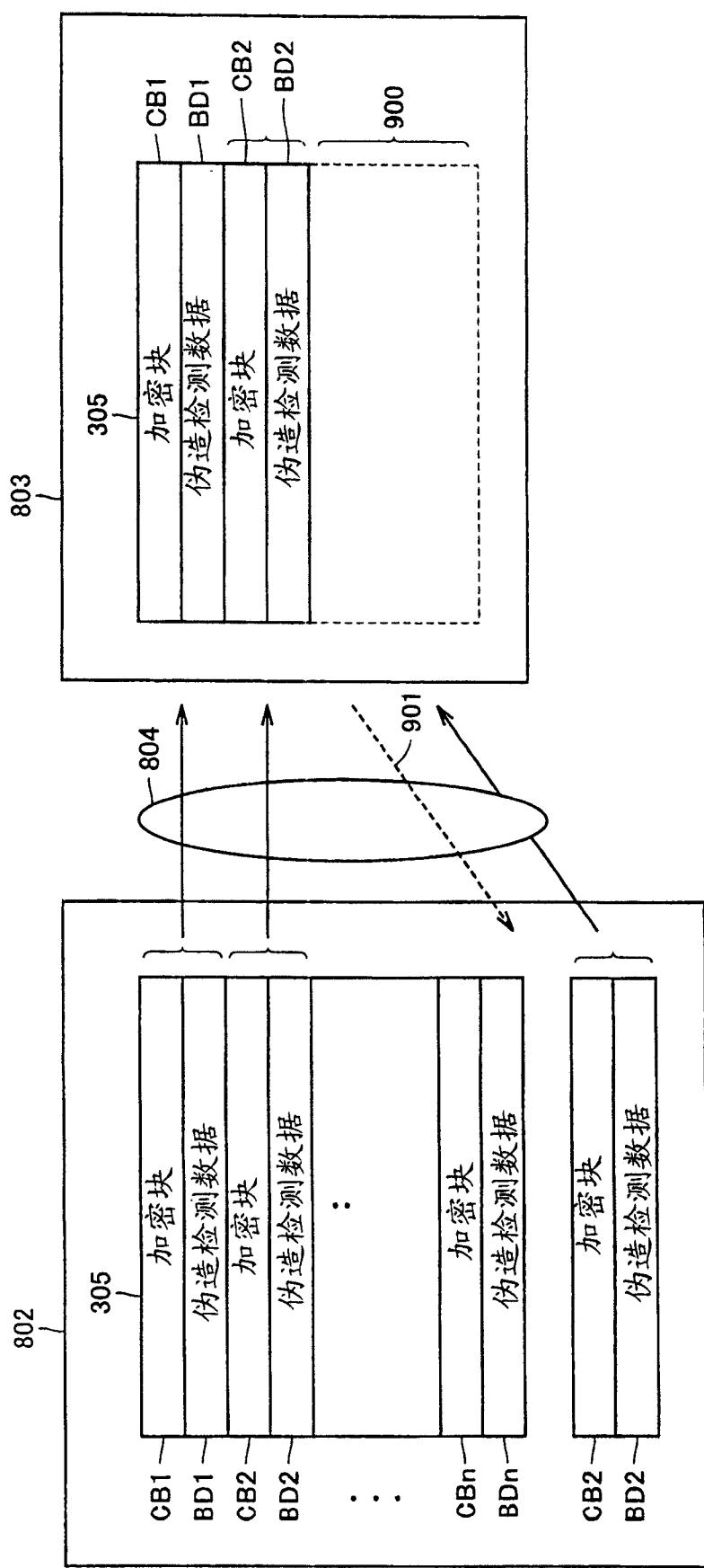


图 13

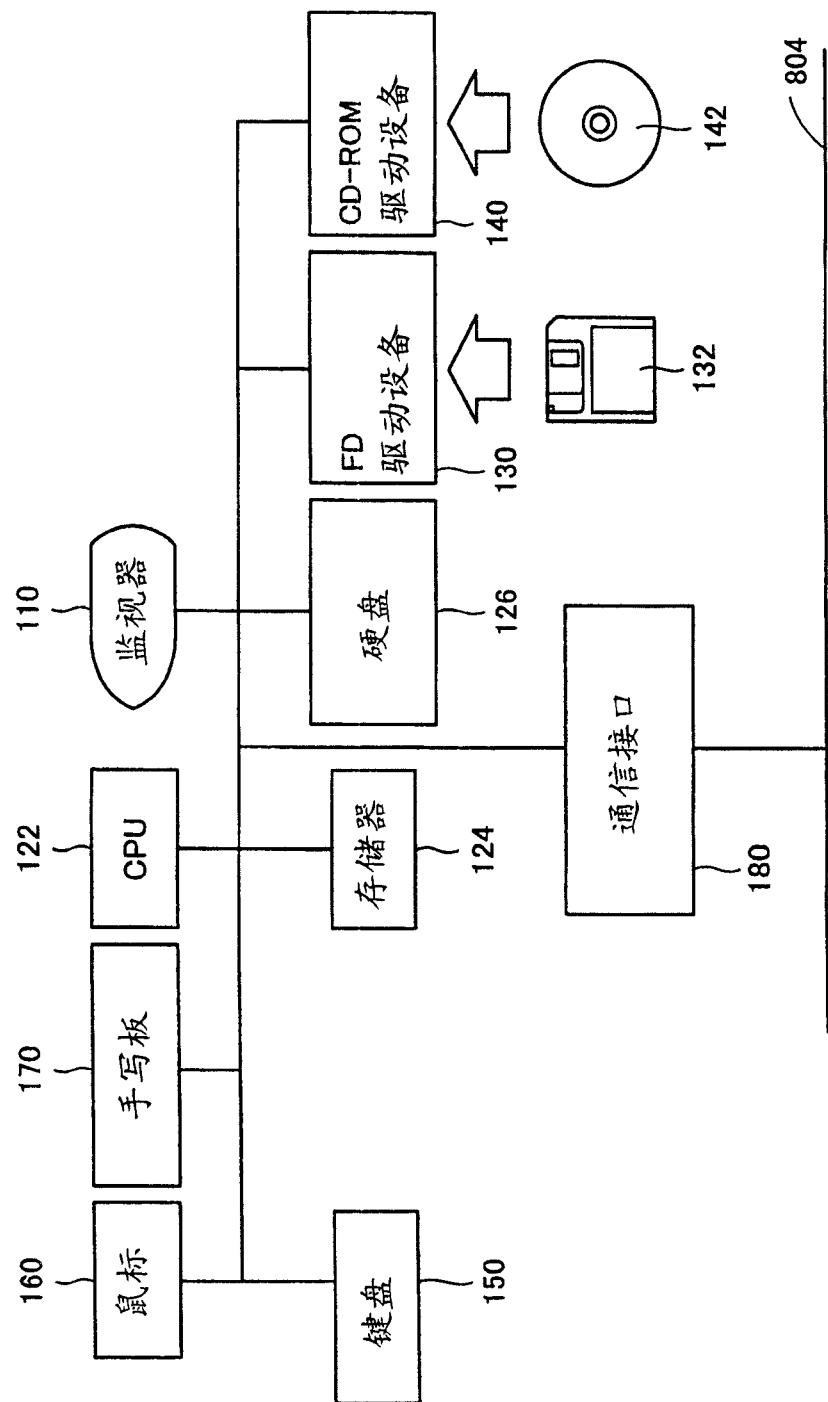


图 14

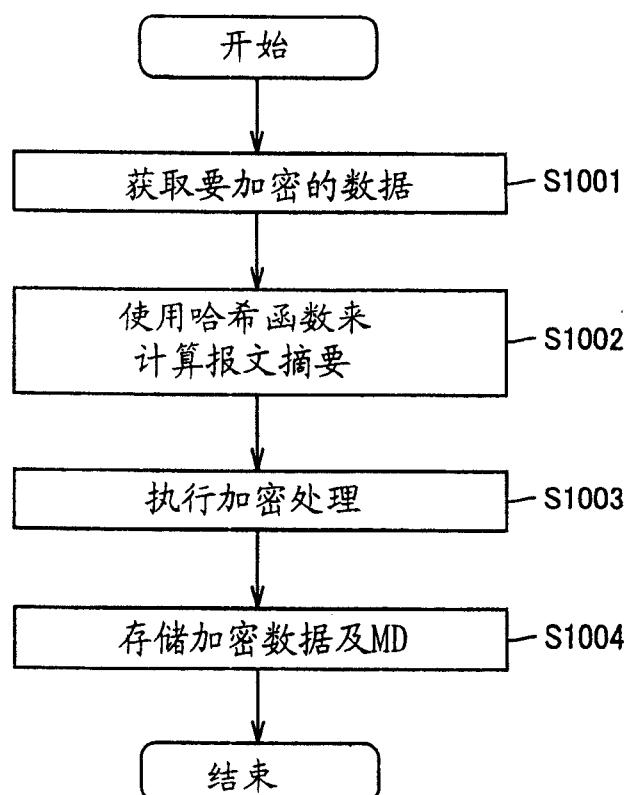


图 15 现有技术

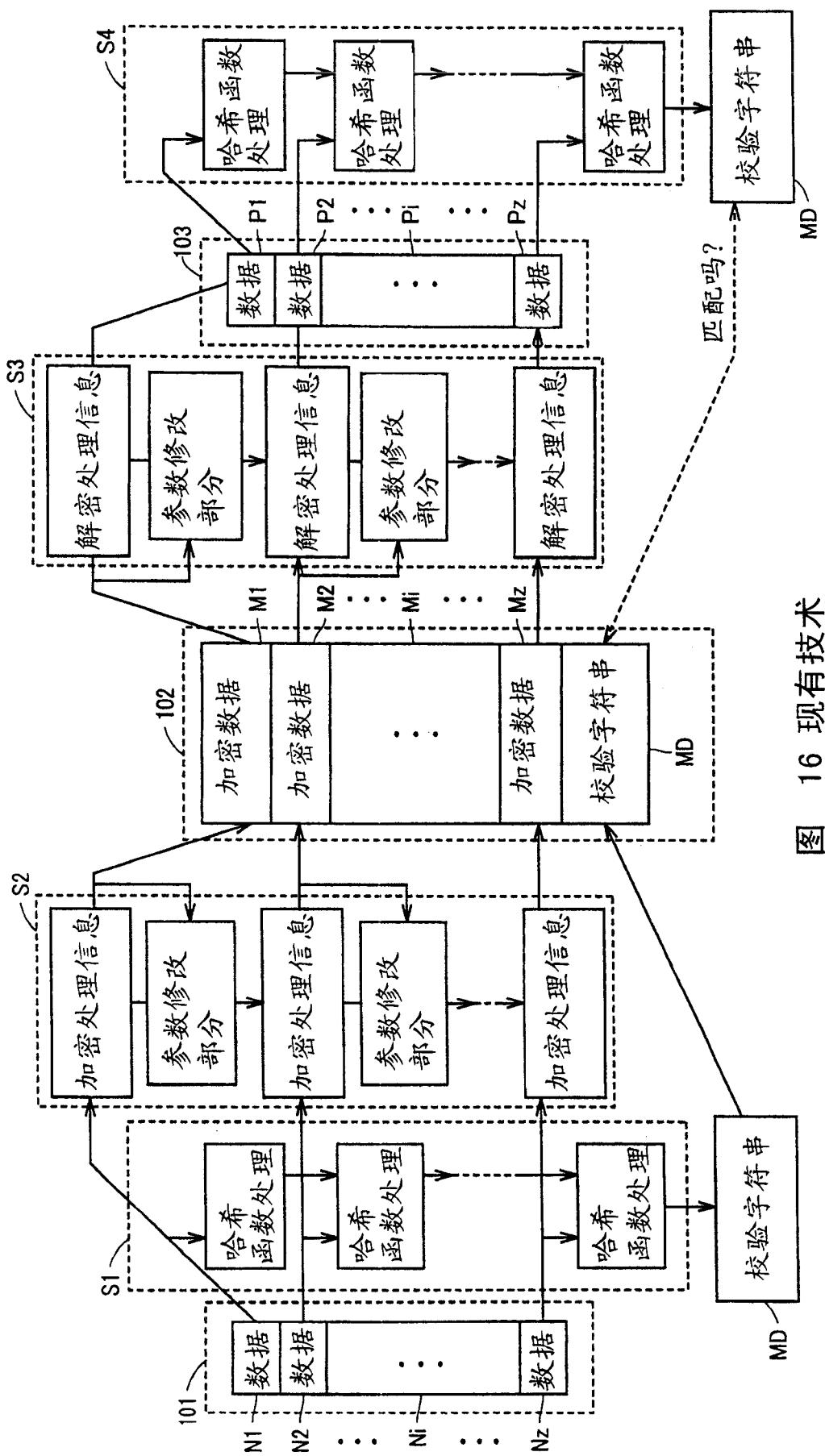


图 16 现有技术