[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 01819302.1

[45] 授权公告日 2007 年 6 月 20 日

[11] 授权公告号 CN 1322384C

[22] 申请日 2001.9.27 [21] 申请号 01819302.1

[30] 优先权

[32] 2000. 9.29 [33] US [31] 09/675,113

[86] 国际申请 PCT/US2001/030356 2001.9.27

[87] 国际公布 WO2002/027444 英 2002.4.4

[85] 进入国家阶段日期 2003.5.21

[73] 专利权人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 R·哈勒 A·费斯

[56] 参考文献

EP0902364A1 1999.3.17

WO0033196A1 2000.6.8

CN1231787A 1999.10.13

审查员 盖 浩

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 吴立明 王 勇

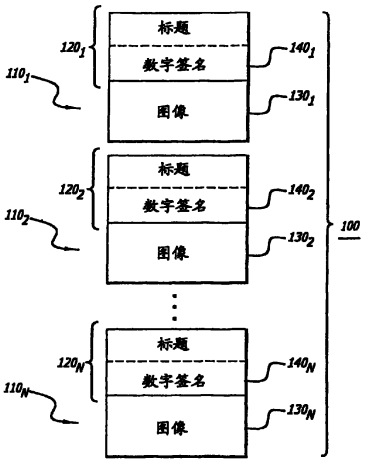
权利要求书 1 页 说明书 9 页 附图 7 页

[54] 发明名称

检验电子设备中储存信息完整性的系统和方法

[57] 摘要

在一种实施方案中，将数字签字图像置入诸如非易失存储器的存储部件。 该数字签字图像包括重新定位后图像和数字签名。 该重新定位后图像是通过将该图像装入该存储部件由对称性重新定位功能改变了的软件模块图像。 该数字签名基于该图像，从而可以用它来分析数据的完整性。



1．一种用于对被重新定位修改的图像进行完整性检验的方法，包括：

将数字签字图像的重新定位后的图像再转换成重新定位前图像，该重新定位前图像是在被对称性重新定位功能改变之前的软件模块图像，该对称性重新定位功能使得重新定位的信息对于使用数字签字的数据完整性检验而言是失败的；

对再转换的重新定位前图像进行散列操作以产生再转换散列值，

从包含在该数字签字图像中的数字签名恢复散列值，该散列值是基于该软件模块的图像；以及

将该散列值同再转换的散列值进行比较。

2．权利要求1的方法，进一步包括：

如果该散列值同再转换的散列值相符，判断该重新定位后图像的完整性保持不变。

3．权利要求1的方法，进一步包括：

当该散列值不和再转换的散列值相符时，判断该重新定位后图像已经被修改成超出由重新定位所引起的修改范围。

4．权利要求1的方法，其中散列操作是一种单向散列操作。

5．一种电子设备，包括：

处理器；和

与该处理器通信的非易失存储器部件，该非易失存储器部件包括：

重新定位后的图像，该图像是在将图像装入该存储器部件时由对称性重新定位功能改变后的软件模块图像，用于改善重新定位图像的检验，和

基于该由一对称性重新定位功能改变之前的软件模块的图像的数字签字。

6．权利要求5的电子设备，其中该非易失存储器部件进一步包括该对称性重新定位功能用于将图像转换成重新定位后图像的信息。

7．权利要求6的电子设备，其中置入该非易失存储器部件之中的信息包括从软件模块图像的起始地址至该软件模块内的信息段的偏移。

检验电子设备中储存信息完整性的系统和方法

技术领域

本发明涉及数据安全领域。更具体而言，本发明涉及用于检验装载于电子设备中的储存信息的完整性的方案。

背景技术

许多电子设备包括一组被称为固件的半永久性储存指令。例如，计算机包括一种叫做基本输入/输出系统（BIOS）的固件。通过该计算机处理器的执行，对 BIOS 编码以完成各种功能。举例来说，在通电的预引导周期期间，BIOS 控制该计算机的初始化以及各种硬件外设的初始化。正常情况下 BIOS 是由单个供应商提供，在计算机制造期间将它装入诸如只读存储器（ROM）部件或闪速存储器部件的非易失存储器的预引导空间。

但是，近来已经希望将更复杂的例程和数据储存在这种非易失存储器的预引导空间。作为一个实例，在最近致力于防止软件病毒和 BIOS 的恶性腐坏之中，可以将 BIOS 代码的图像数字签字以产生数字签名。在执行 BIOS 之前，可以用该数字签名判断该 BIOS 是否被加以修改。这就很大程度上提供了所需要的防病毒保护。

本领域内都知道，数字签名是利用签字人个人密钥的签字数字数据。同加密相似，这种“签字过程”可以利用任何一套软件算法实现，这些软件算法有诸如 Rivert Shamir 和 Adleman（RSA）算法或数字签名算法（DSA），在题为“Digital Signature Standard”的“Federal Information Processing Standards publication 186（1994，5 月 19 日）”中对这些算法都做了说明。通常，这种数字数据是以一种编码形式（叫做“散列值”）固定的，它是在将该散列值签字之前通过对该原始数字数据的单向散列操作得到的。术语“单向”指的是实际上并不存在一种反向操作或功能以从该散列值恢复该数字数据的任何可辨别部分。

最近，计算机产业已经在努力研制一种软件模块集合的 BIOS，它是由不同商家生产的软件模块的集合而非由单一商家生产的一片整体式代码。很可能该种 BIOS 的代码被配置成“原位执行(excute-in-

place)”模块，因为这种代码可以在系统随机访问存储器（RAM）供使用之前加以执行。而且，很可能使用重新定位将该BIOS模块正确装入非易失存储器内，因为对所有的BIOS商家而言无法在此之前就这种特殊的寻址方案达到一致。

就如在该行业中通晓的那样，“重新定位”是一种过程，通过这种过程每一BIOS模块内的地址将根据存储器内对该BIOS模块分配给的特殊地址位置（叫做“基地址”）加以调整。因而，BIOS模块内的软件例程通常用同基地址的相对偏移编码，而这一基地址尚未赋值。在重新定位期间，BIOS模块内各种软件例程的地址将通过将该地址加到每个相对偏移上而加以调整。

不幸的是，假如重新定位是在原位执行BIOS模块上进行，则任何与该BIOS模块的图像相关的数字签名将是无效的，因为使用数字签名的任何数据完整性分析将表明该BIOS模块已经被修改。因此，最终不可能判断该BIOS模块的修改到底是由非授权的还是只是由于重新定位操作引起的。因而，希望研制一种完整性检验机制，这种机制能改进在探测对BIOS非授权修改中数字签字的有效性同时又允许图像进行重新定位。

而且，当研制的BIOS是作为由不同商家生产的数字签字BIOS模块的集合时，在某些情况下，也许希望将这些数字签字的模块加以动态链接。特别地，可以将一种BIOS模块配置成调用编码在另一种BIOS模块内的功能。但是，为了使BIOS模块动态链接在一起，将要求至少一种BIOS模块的修改，而这样又势必使同该BIOS模块的图像相关的任何数字签名无效。因此，原始的数字签名对于识别非授权的模块修改将是无效的。因而，希望有一种完整性检验机制能克服这一弊端。

发明内容

本发明的第一方面涉及一种方法，其包括：将数字签字图像的重新定位后的图像再转换成重新定位前图像，该重新定位前图像是在被对称性重新定位功能改变之前的软件模块图像，该对称性重新定位功能使得重新定位的信息对于使用数字签字的数据完整性检验而言是失效的；对再转换的重新定位前图像进行散列操作以产生再转换散列值，从包含在该数字签字图像中的数字签名恢复散列值，该散列值是基于该软件模块的图像；以及将该散列值同再转换的散列值进行比

较。

本发明的第二方面涉及一种用于在一种电子设备中生成约束和重新定位输入表的方法，其包括：找出装在电子设备中的第一数字签字图像的输入表，该输入表的每一条目包括一个标识符和一个第一偏移；访问在第一数字签字图像的输入表中的所选条目内的标识符；判断该标识符是否同装在该电子设备中的第二数字签字图像的输出表内的标识符相符，该输出表的标识符和相应的第二偏移一起储存；和在判断在该输入表中的所选条目内的标识符同所述输出表内的标识符相符时，通过将该第二偏移同第二数字签字图像的起始地址相组合产生一地址，和将该标识符装入该输入表中的所选条目中并且将所述地址装入约束和重新定位输入表的条目。

本发明的第三方面涉及一种电子设备，其包括：处理器；和与该处理器通信的非易失存储器部件，该非易失存储器部件包括：重新定位后的图像，该图像是在将图像装入该存储器部件时由对称性重新定位功能改变后的软件模块图像，用于改善重新定位图像的检验，和基于该由一对称性重新定位功能改变之前的软件模块的图像的数字签字。

本发明的第四方面涉及一种电子设备，其包括：处理器；和与该处理器通信用的存储器，该存储器装载有约束和重新定位输入表、输入表、输出表、软件模块图像，以及基于该输入表、该输出表和该图像的数字签名。

附图说明

从以下对本发明的详细描述，将使本发明的特点和优点变得清晰，其中：

图 1 展示用于将软件模块集合作为固件装入电子设备中的方框图。

图 2 是利用本发明的电子设备的一种实施方案的方框图。

图 3 是图 2 的非易失存储器部件的存储信息的第一种展示性实施方案的方框图，它集体用于用数字签名检验重新定位过的重新定位后图像的完整性。

图 4 是图 2 的非易失存储器部件的存储信息的第二种展示性实施方案的方框图。

图 5 是用于检验储存信息完整性，如图 3 和图 4 中所示的重新定位后图像的完整性的操作流程图。

图 6 是本发明的第二种展示性实施方案的方框图，这种方案的特点是多个数字签字图像通过一个或多个约束和重新定位输入表（BRITs）被动态链接在一起。

图 7 是用于发生约束和重新定位输入表（BRIT）的操作流程图。

图 8 是用于检验图 7 的约束和重新定位输入表（BRIT）的操作流程图。

具体实施方式

现在，对本发明的某些实施方案加以说明，这些方案用于检验在预引导操作期间储存在电子设备中的信息完整性。一般来说，该种储存信息，例如，可以包括数字签字图像，而这种图像包括软件模块的重新定位后图像或者是同另外的数字签字图像动态链接的。

在以下的说明中使用了某些术语来讨论本发明的特点。“软件模块”包括一组执行特殊功能的指令。例如，该软件模块可以是在预引导周期期间被执行以便将电子设备初始化的特征指令。对同该软件模块相关的指令的二进制表示的复制被称之为“图像”。不同类型的图像可以用于代表不同格式化的阶段。例如，“重新定位前图像”是该软件模块在对它进行重新定位操作之前的二进制表示。“重新定位后图像”是重新定位后该模块的二进制表示。

还有，“电子设备”是集体操作以完成一种或多种特定功能的电子软件和硬件之组合。一种电子设备的实例包括计算机（如膝上型、台式、手提式、服务器、大型计算机等），计算机部件（和串行端口），手机，机顶盒（电缆盒，网络计算机，卫星电视接收机等），网络设备等。“链接”从广义上定义为一种或多种建立通信路径的信息承载媒介，包括物理媒介（例如，电线，光纤，电缆，总线跟踪等）或无线媒介（例如，和无线信令技术相结合中的空气）。

简而言之，一种完整性检验机制涉及数字签字图像的配置以包括重新定位信息，重新定位后的图像以及数字签名。“重新定位信息”是一连串对基地址的相对偏移。这些偏移是在储存信息（例如软件模块图像）被编辑并置于像 MC-DOS® “EXE” 格式的可执行格式中以后生成的（MS-DOS 是 Microsoft Corporation of Redmond, Washington

的注册商标）。在重新定位期间，在该基地址，即该软件模块图像被储存和恢复以便执行的存储地址被确定之后，该偏移被转换成合适的地址。因此，重新定位后的图像同重新定位前的图像不同。但是，数字签名是基于重新定位前的图像。

另一种第二完整性检验机制涉及在每种数字签字图像之中包括输入表和输出表。这些表允许在不同数字签字图像之内将功能经由约束和重新定位输入表（Bound & Relocated Import Table:BRIT）动态限制在一起。该 BRIT 驻留在该数字签字图像之外。两种完整性检验机制均可以用硬件或者用置入处理器内（下面说明）的软件程序或只由处理器可执行的软件程序加以完成。

参照图 1，它是“N”个软件模块集合的展示性方框图，这些模块准备作为固件 100 装入电子设备之中。其中每一软件模块 110 N（N≥1）包括标题 120 N 和图像 130 N，用于该固件 100 的一特殊软件段。在将该软件模块以固件形式装入如下面描述的那种非易失存储器之前，每一图像 130 N 由签字人数字签字以产生数字签名 140 N。在每个模块之间可以有不同的签字人，或者多个模块为同一签字人。“签字人”可包括任何承认或保证该数字签名的信赖个人或实体（例如，银行，政府实体，贸易协会，原始设备制造商，商家等）。

参照图 2，它示出了一种电子设备的实施方案图。对于这种实施方案，该电子设备 200 包括芯片组 210，该芯片组分别经由第一总线 240 和第二总线 250 连接到处理器 220 和存储器 230。此外，该芯片组还与第三总线 260 连接，以提供通向 1 个或多个系统资源 270 的通道。其中，第三总线 260 被表示成输入/输出（I/O）总线（例如，外围部件互连“PCI”总线），但是可以采用任何其他类型的总线结构，包括像工业标准结构（ISA），扩展 ISA（EISA），通用串行总线（USB）等总线结构。示出的第三总线 260 是单总线，但是应当理解该第三总线可以包括通过桥电路连接在一起的多条总线。

如图所示，系统资源 270 连接到多总线中的至少一个。该系统资源 270 包括通信设备 280 和非易失存储器部件 290。通信设备 280 被配置成经通信链接建立同另一电子设备的通信。通信设备 280 的实例包括网络接口卡，调制解调器卡或外部调制解调器。非易失存储器部件 290 包括以 1 个或多个软件模块的数字签字图像为特征的固件。在

一种实施方案中，这些软件模块的1个或多个可以形成该电子设备200的基本输入/输出系统（BIOS）代码。这种非易失存储器部件290包括可编程的非易失存储器，如闪速存储器，电池支持的随机存取存储器（RAM），只读式存储器（ROM），可擦除可编程的ROM（EPROM），电可擦除PROM（EEPROM），或任何适合于储存该模块的其他类型存储器。

参照图3，它显示图2的非易失存储器部件290的装载和储存信息的第一实施方案的方框图。该非易失存储器部件290用1个或多个数字签字图像300装载，300本身集体作为固件运行。对于这种实施方案，数字签字图像300包括重新定位信息310，重新定位前图像320以及数字签名330。形成任何图像的元件的定位是设计选择。

重新定位信息310包括对重新定位前图像320内的某些例程的相对偏移315。通常，该偏移315是在与该数字签字图像相关的该软件模块被编辑时发生的。偏移315用于在重新定位期间一旦图像300的叫做基地址“B_ADDR”的起始位置，被确定后正确对该软件模块之内的信息段寻址。该重新定位是用对称重新定位功能进行的，这种功能允许对使用数字签名330的数据完整性检验取消该重新定位过的信息。

在重新定位期间，依据装载期间图像300的重新处理前的图像320，该重新处理前的图像320被转换成（重新定位成）重新定位后的图像340。即是说，重新定位前的图像320被重新定位以便从配给图像300的基地址恢复。实质上，该重新定位操作将B_ADDR加到包含在该重新定位信息310之内的偏移315上。这样就修改了诸如储存在非易失存储器部件中的重新定位后的图像340的二进制图像，而与由商家编码的重新定位前的图像320不同。

数字签名330包括至少该重新定位前图像320的一种散列值，它是由签字人的个人密钥（PRK）以数字方式签字的。虽然该重新定位后的图像340在重新定位之后现在驻留在该非易失存储器部件之中，但应当知道该数字签名330是依据重新定位前图像320，而重新定位前图像320是在装入非易失存储器部件之前最初产生的二进制形式。

参照图4，它显示非易失存储器部件290的储存信息的第二展示性实施方案的方框图。该非易失存储器部件290包含形成固件400（例如BIOS）的多幅数字签字图像410_1-410_M（“M”为正整数）。例如，作为一种展示性实例，每一数字签字图像410_1-410_M是用一重新定位前的

图像 420_1-420_M、重新定位信息 430_1-430_M和数字签名 440_1-440_M所形成的。每一数字签名 400_1-400_M是依据至少一种与它对应的重新定位前图像 420_1-420_M的散列值，并且用 1 个或多个签字人的个人密钥（PRK）数字签字的。在用数字签字图像 410_1-410_M装载时，该非易失存储器部件 290 进行重新定位操作，这种操作将所储存的图像分别从重新定位前的图像 420_1-420_M修改成重新定位后的图像 450_1-450_M。

现在参照图 5，它显示用于检验所储存信息完整性的操作流程图，例如图 3 和图 4 的重新定位后的图像的操作流程图。对于完整性检验，数字签字图像的重新定位后的图像被转换成重新定位前的图像（方框 500）。这是利用包含在该数字签字图像中的重新定位信息实现的。具体而言，对每一偏移进行一次或多次算术操作，即，作为一个实例，将同该非易失存储器部件相关的基地址从在重新定位信息中提到的每一偏移减去。此后，在方框 510，对再转换的重新定位前的图像进行散列操作以产生一散列值（称为再转换散列值）。

对该数字签字图像的数字签名加以访问并将该数字签名的散列值加以恢复（方框 520）。这一点可以将该数字签字图像通过为解码目的而装备有该签字人的公共密钥的数字签名算法而加以运行实现。此后，将该恢复后的散列值同其再转换的散列值进行比较（方框 530）。如果判断两者相符，则该重新定位后的图像得到验证（方框 540），不然的话，表明该图像没有得到验证，该图象已经被修改成超出了重新定位所引起的那种修改范围（方框 550）。

图 6 是本发明的第二展示性实施方案的方框图，其中多幅（M）数字签字图像 600_1-600_M通过 1 个或多个约束和重新定位输入表（BRITs）动态链接在一起。每一个 BRIT 仅对应一个数字签字图像。考虑到每一数字签字图像 600_1-600_M可以包括 BRIT 或者仅有一个分组的数字签字图像 600_1-600_M可以被提供 BRIT。

在该实施方案中，示出了两幅数字签字图像 600_1和 600_M的动态链接。其中，数字签字图像 600_1包括 BRIT 600_1，输入表 620_1，输出表 630_1，基于选择信息（如软件模块）的图像 640_1以及数字签名 650_1。该数字签名 650_1是通过对输入表 620_1，输出表 630_1以及图像 640_1进行单向散列操作以产生最终散列值发生的。最终的散列值是由签名人利用它个人的密钥数字签字的。

一般而言，输入表 620_1 储存信息的列表，它位于另一数字签字图像之中（如图像 640_M），对于图像 640_1 的正当执行需要对它进行访问。输入表 620_1 包括多个条目 625，输入表 620 的至少 1 个条目（如条目 626）包括标识符 627 和第一偏移 628。该标识符 627 既可以在电子设备内部发生也可以经集中化机构遥控产生，它表明不包含在该数字签字图像 600_1 内的哪个信息段或哪些信息段（如函数，例程，代码，数据等）是在执行期间被图像 640_1 所要求的。该标识符 627 可以被表示为一种字符数字名字或者被承认的唯一识别号（如一种 16 字节的值）所代表。第一偏移 628 是一种偏移指针，它指向与条目 626 相对应的 BRIT 610 的一个条目。

输出表 630 是包含在数字签字图像中的信息列表，它用于其他数字签字图像的恢复。例如，输出表 630_M 的条目包括用于包含在图像 640_M 中的每段信息的标识符 635 以及第二偏移 636。该第二偏移 636 等效于从该数字签字图像 600_M 的地址位置至数字签字图像 600_1 的图像 640_1 所要求的信息段的地址位置的偏移。

如图所示，该 BRIT 610_1 同该数字签字图像 600_1 相关联。BRIT 610_1 的每一条目包括标识符 627 以及该信息段的位置的地址指针 611。地址指针 611 是图像 640_M 的起始地址同第二偏移 636 的算术组合。因此，在图像 600_1 的执行期间，对由标识符 627 参考的信息段的请求经由 BRIT 至图像 640_M 中的一个位置进行路径选择，如图 660 中的虚线所表示。这样就使得在那一位置的信息段可以被访问而不会对图像 640_M 产生修改。因此，数字签名 650_1 和 650_M 仍可以用于监测输入表 620_1 和 620_M，输出表 630_1 和 630_M 和/或图像 640_1 和 640_M 的修改。

参照图 7，它是用于发生图 6 所示的第一数字签字图像 600 的约束和重新定位输入表（BRIT）的操作流程图。最初，将所有在非易失存储器部件之中的数字签字图像找出（方框 700）。随后，将第一数字签字图像的输入表找出（方框 710）。对该输入表的一个初始条目，确定其标识符并进行搜索以找到另一数字签字图像的输出表中的一种相匹配的标识符，也就是说，即除该第一数字签字图像还找到的任何其他数字签字图像（方框 700 和 730）的一种相匹配的标识符。

假如没有找到该匹配的标识符，将错误报告（方框 740 和 750）。如果，例如，在第二数字签字图像内找到了该匹配的标识符，则将对

应于该标识符并驻留在第二数字签字图像中的该输出表中的偏移同该第二数字签字图像的起始地址以算术方式加以组合（方框 740 和 760）。将组合后的地址连同与输入表相关的标识符放入该 BRIT 的一个条目（方框 770）。这一过程一直继续直至在输入表中的所有条目在 BRIT 都具有相对应的条目为止（方框 780）。

参照图 8，它是用于检验图 7 的约束和重新定位输入表（BRIT）的操作流程图。在本实施方案中，发生所有数字签字图像的列表（方框 800）。对每种数字签字图像，通过确认它相应的输入表，输出表以及图像还没有被修改来实现对这些数字签字图像完整性的检验（方框 810）。例如，对第一数字签字图像，这可以通过对该第一数字签字图像的输入表，输出表以及图像进行散列操作来实现。这样就产生最终的散列值。将该最终散列值同来自该数字签名与该第一数字签字图像相关联的恢复后的散列值相比较。假如该最终散列值同恢复的散列值相符，则该第一数字签字图像的输入表、输出表以及图像没有被修改。将这一操作对所有余下的数字图像加以继续。

如果该数字签字图像的完整性不能得到检验，则报告错误（方框 820）。否则，对该第一数字签字图像，判断在它的输入表内的标识符是否同另一数字签字图像的输出表中的一标识符相符（方框 830）。假如没有找到相符，则报告错误（方框 820）。假如找到了相符，判断对应于该输入表的标识符的 BRIT 条目是否指向由另一数字签字图像的输出表的相匹配的标识符所规定的一个地址（方框 840）。因为该 BRIT 仅能指向由包含在一数字签字图像中的输出表所规定的一个地址，它仅能指向所信赖的信息。假如对应于输入表的该标识符的 BRIT 条目指向由另一数字签字图像的输出表的相符合的标识符所规定的一个地址，则该 BRIT 得到检验（方框 850）。否则，该 BRIT 没得到检验（方框 860）。

尽管对某些示例性实施方案做了说明并示出了相应的附图，当然这些实施方案只是示范性的，而不是对本发明宽广范围的限制，并且不应当将本发明限制到所示和所说明的这些特殊的结构和布局，因为对本领域内的那些技术人员来说可以做出各种其他的修改。

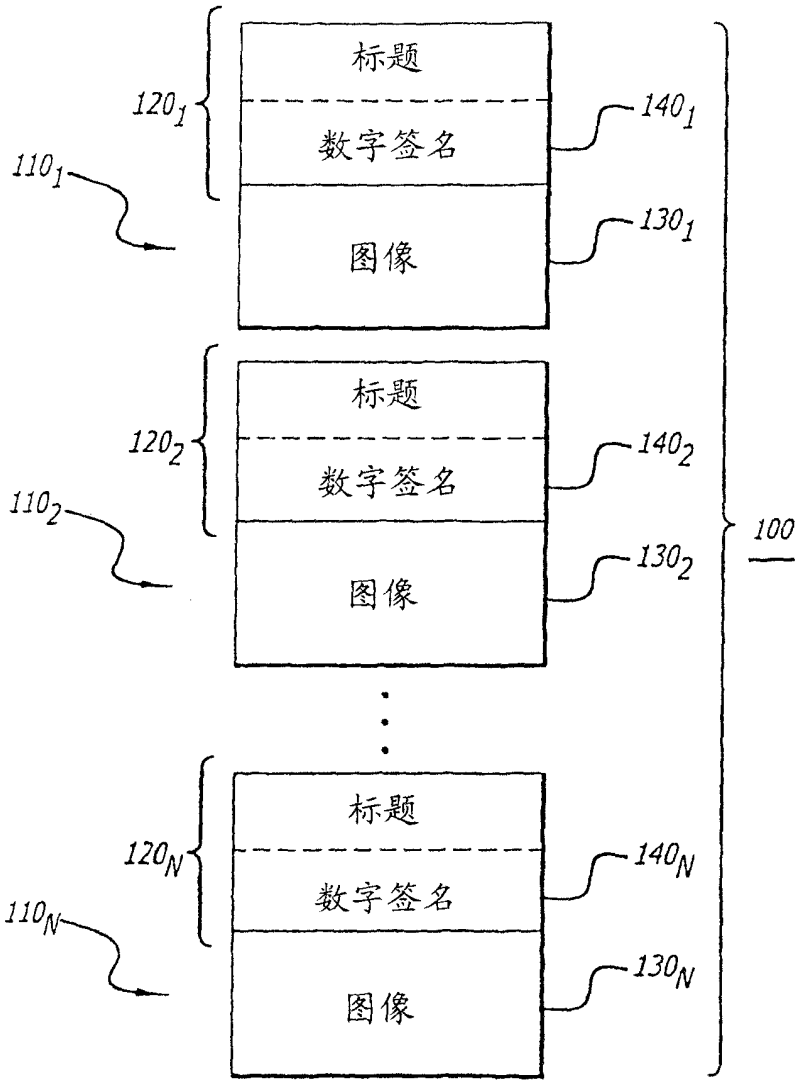

标题
数字签名
图像
120_1
140_1
130_1
110_1
120_2
140_2
130_2
110_2
120_N
140_N
130_N
110_N
100

图 1

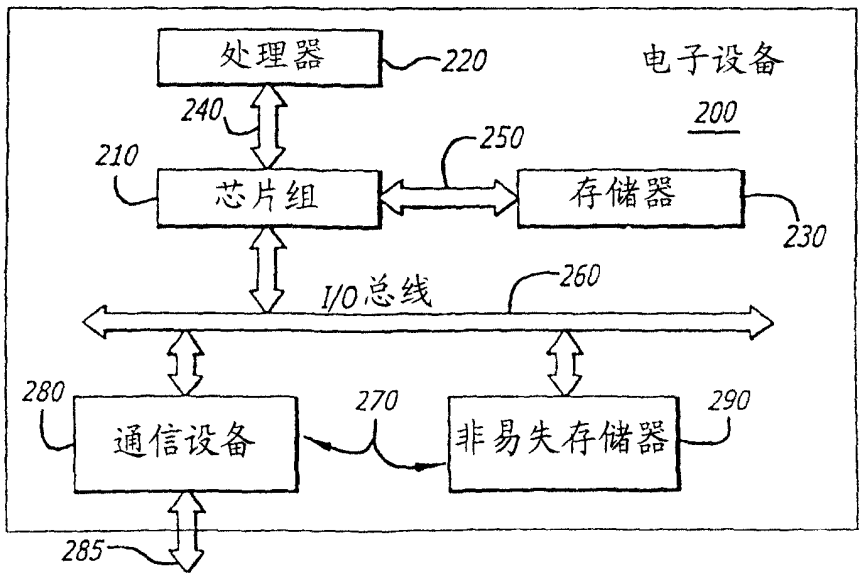

处理器
220
电子设备
200
240
250
210
芯片组
存储器
230
I/O总线
260
280
270
290
通信设备
非易失存储器
285

图 2

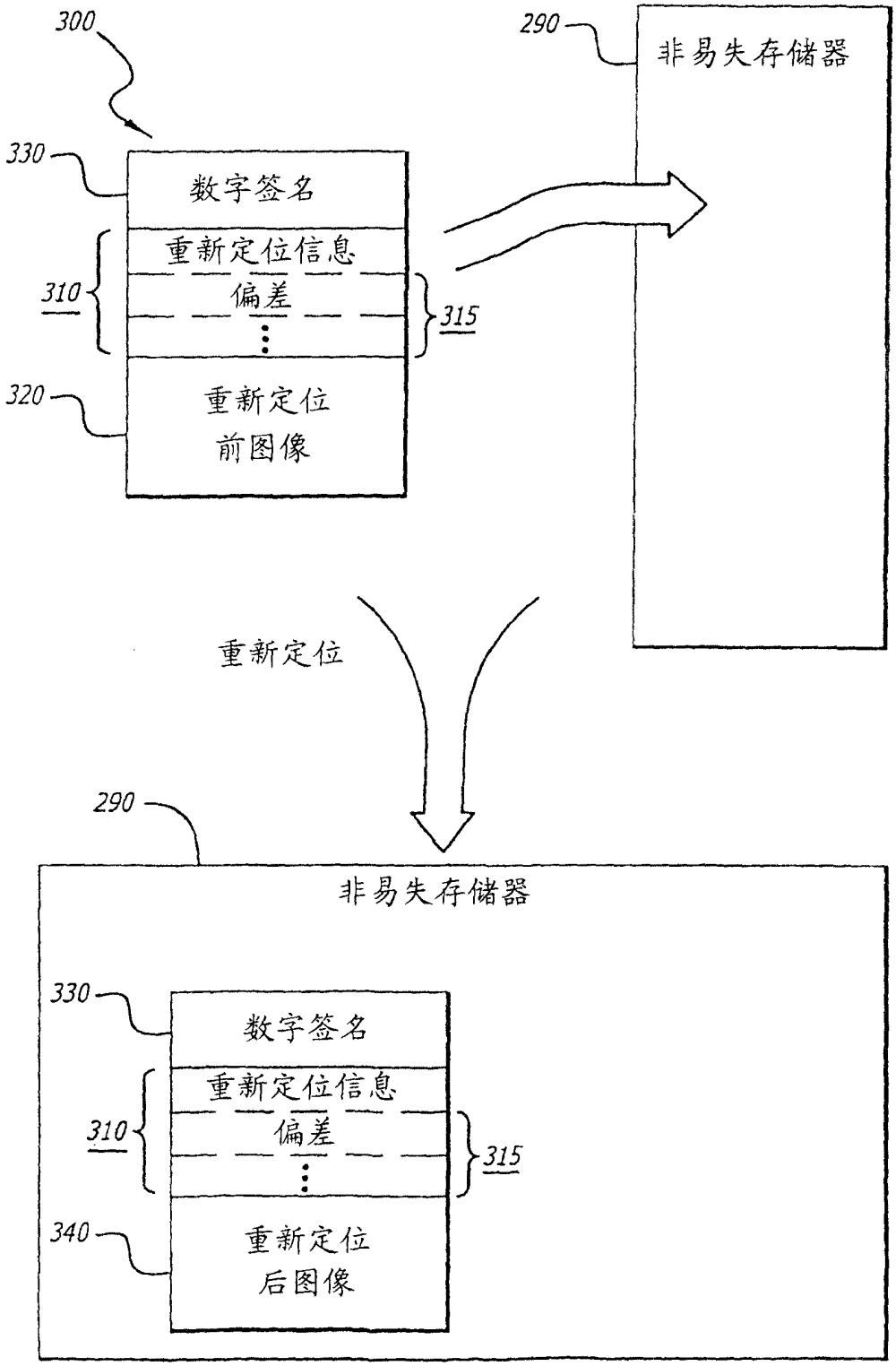

300
290
非易失存储器
330
数字签名
重新定位信息
310
偏差
315
320
重新定位
前图像
重新定位
290
非易失存储器
330
数字签名
重新定位信息
310
偏差
315
340
重新定位
后图像

图 3

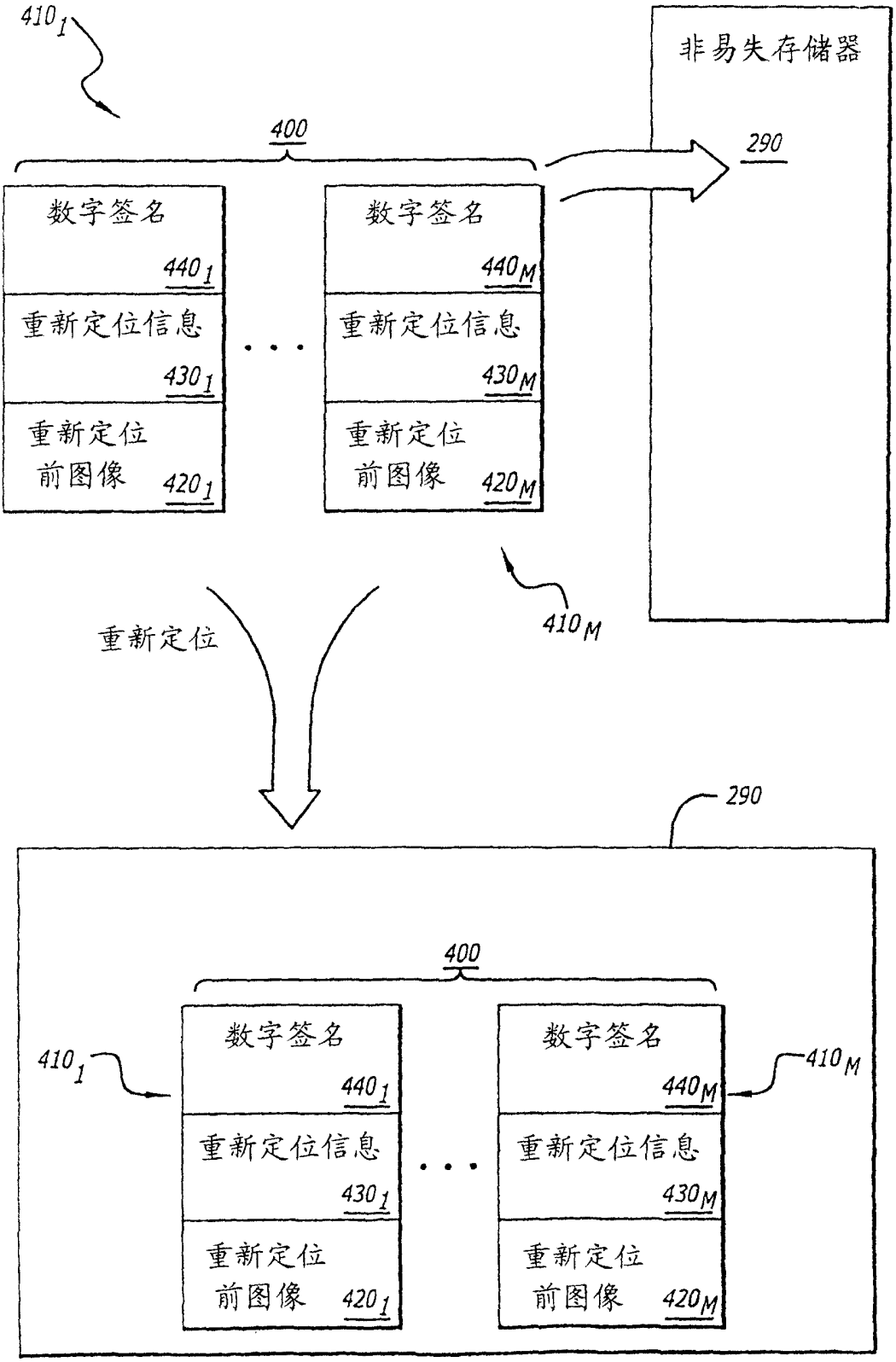

410 1
非易失存储器
400
290
数字签名
440 1
重新定位信息
430 1
重新定位
前图像
420 1
数字签名
440 M
重新定位信息
430 M
重新定位
前图像
420 M
410 M
重新定位
290
400
410 1
数字签名
440 1
重新定位信息
430 1
重新定位
前图像
420 1
数字签名
440 M
410 M
重新定位信息
430 M
重新定位
前图像
420 M

图 4

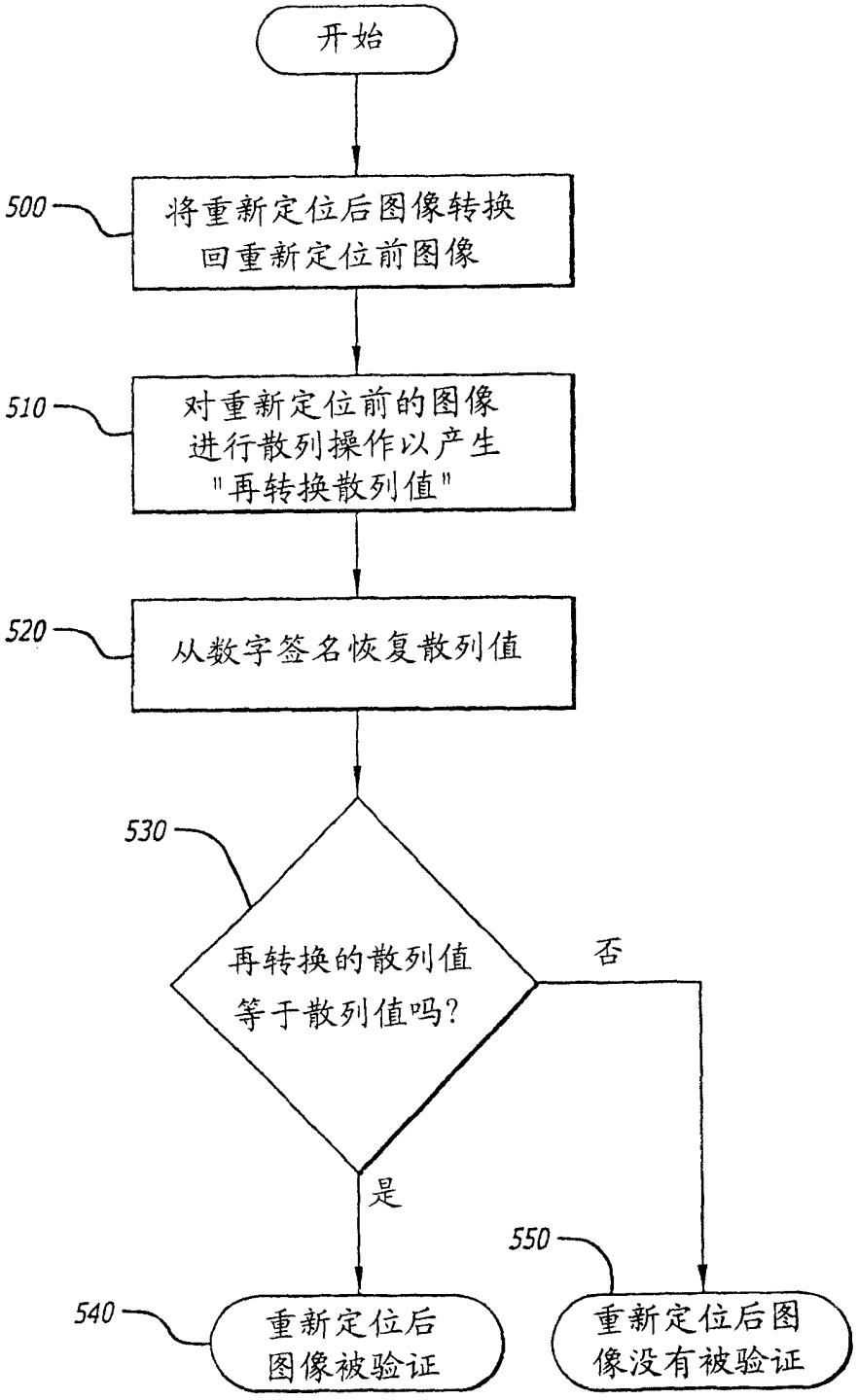

开始
500
将重新定位后图像转换回重新定位前图像
510
对重新定位前的图像进行散列操作以产生"再转换散列值"
520
从数字签名恢复散列值
530
再转换的散列值等于散列值吗?
否
是
550
540
重新定位后图像被验证
重新定位后图像没有被验证

图 5

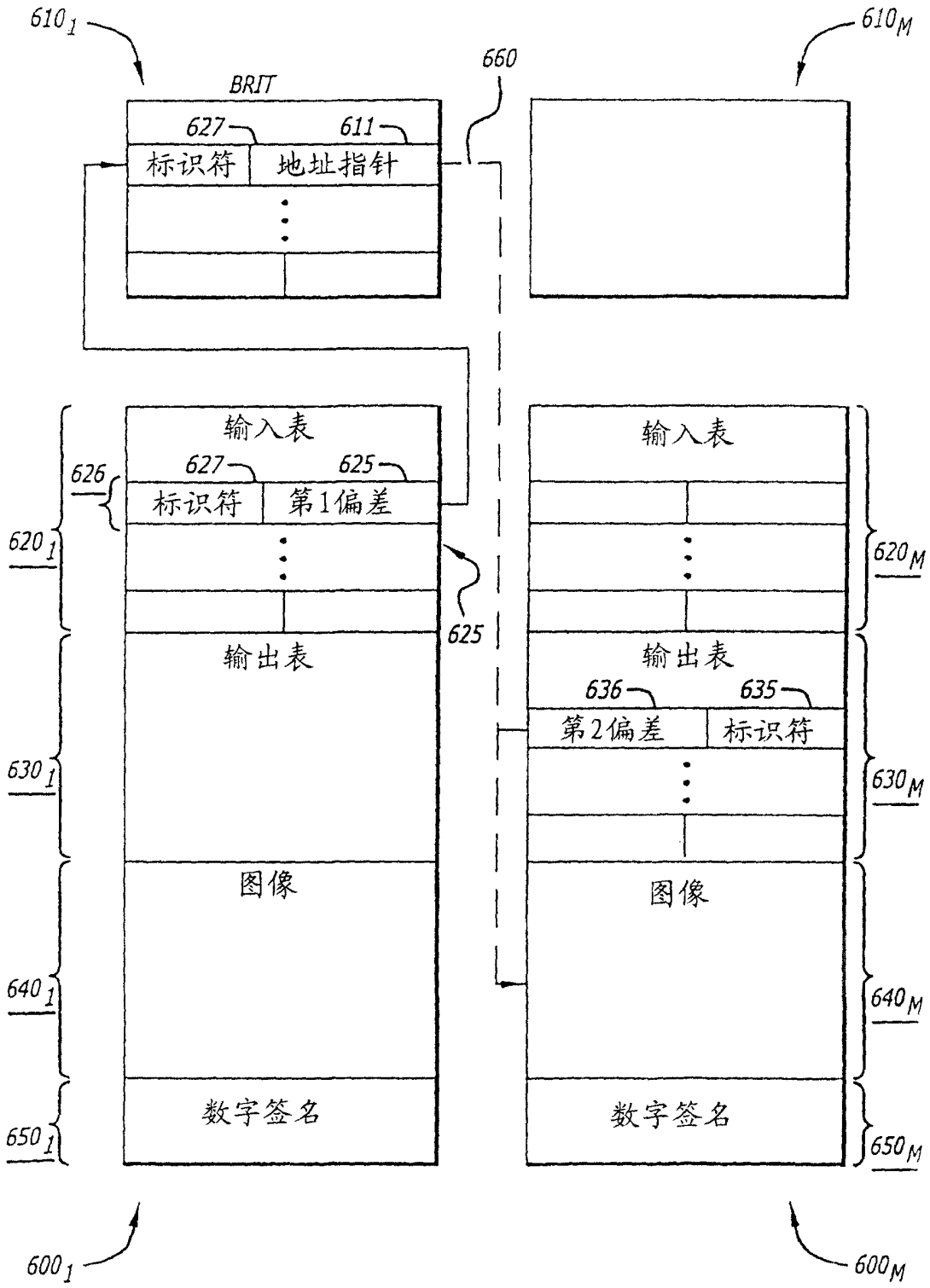

610_1
610_M
660
BRIT
627
611
标识符
地址指针
输入表
626
627
625
标识符
第1偏差
620_1
620_M
625
输出表
输出表
636
635
第2偏差
标识符
630_1
630_M
图像
图像
640_1
640_M
数字签名
数字签名
650_1
650_M
600_1
600_M

图 6

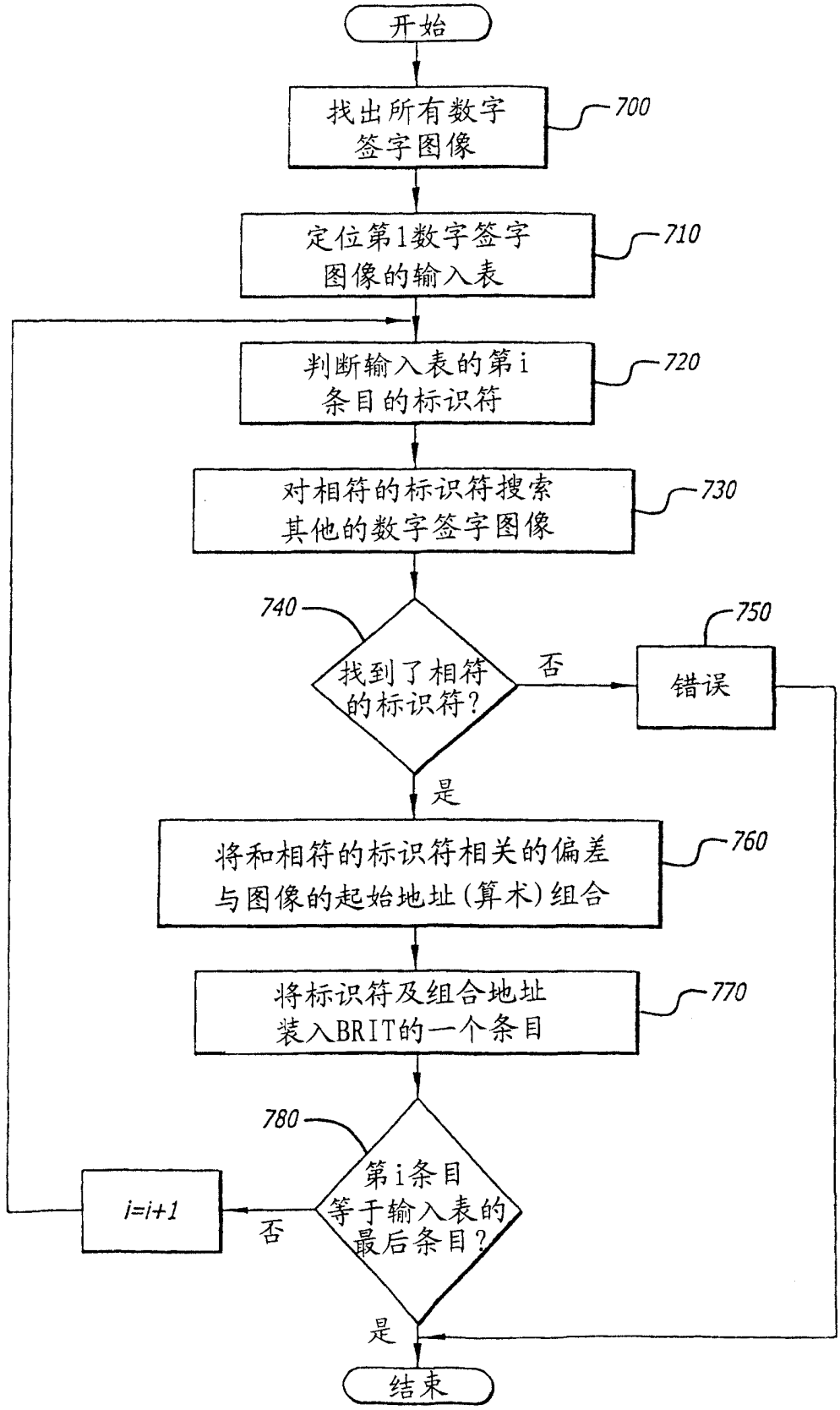

开始
找出所有数字签字图像
700
定位第1数字签字图像的输入表
710
判断输入表的第i条目的标识符
720
对相符的标识符搜索其他的数字签字图像
730
740
找到了相符的标识符?
否
750
错误
是
将和相符的标识符相关的偏差与图像的起始地址(算术)组合
760
将标识符及组合地址装入BRIT的一个条目
770
780
第i条目等于输入表的最后条目?
否
i=i+1
是
结束

图 7

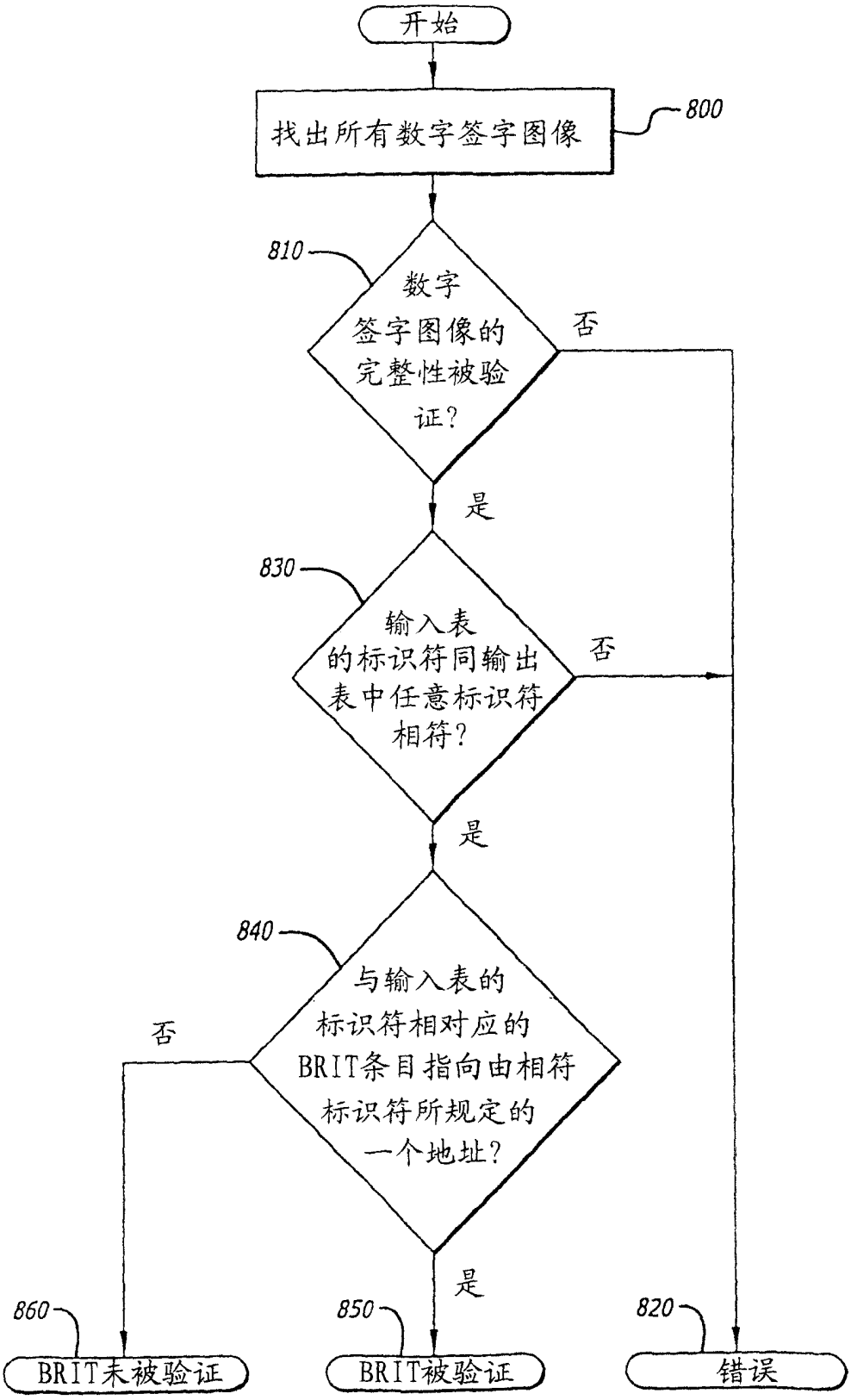

开始
找出所有数字签字图像
800
810
数字签字图像的完整性被验证?
否
是
830
输入表的标识符同输出表中任意标识符相符?
否
是
840
与输入表的标识符相对应的BRIT条目指向由相符标识符所规定的一个地址?
否
是
860
BRIT未被验证
850
BRIT被验证
820
错误

图 8