



[12]发明专利申请公开说明书

[21]申请号 96195763.8

[43]公开日 1998年8月26日

[11]公开号 CN 1191644A

[22]申请日 96.6.17

[74]专利代理机构 永新专利商标代理有限公司

[30]优先权

代理人 韩 宏

[32]95.6.29 [33]US[31]08 / 497,662

[86]国际申请 PCT / US96 / 10463 96.6.17

[87]国际公布 WO97 / 01902 英 97.1.16

[85]进入国家阶段日期 98.1.23

[71]申请人 硅游戏公司

地址 美国加利福尼亚

[72]发明人 艾伦·E·阿尔肯 迈克尔·巴尼特

小路易斯·D·贾卡洛内

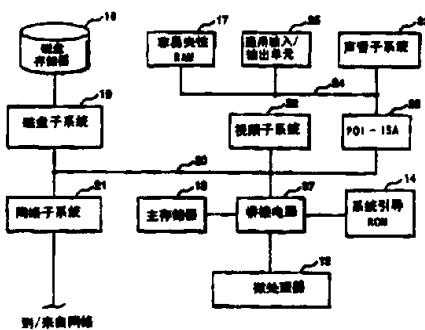
亚当·E·利文索尔

权利要求书 8 页 说明书 14 页 附图页数 3 页

[54]发明名称 具有改进的活动容量、鉴别能力和安全性的电子娱乐场博奕系统

[57]摘要

由几个系统部件组成的电子娱乐场博奕系统，该博奕系统包括微处理器（12）；主存储器单元（13），这是一个典型的随机存取存储器；和系统引导 ROM（14）。该系统还包括非易失性 RAM（17）；大容量存储器单元（18）；磁盘子系统（19）；和 PCI 总线（20）。磁盘子系统（19）最好支持具有任选传输速度和传输量的 SCSI-2。视频子系统（22）也包括在该电子娱乐场博奕系统内且被连接到 PCI 总线（20）上以便提供全彩色静止图像和 MPEG 影片。



权 利 要 求 书

1、一种用于鉴别娱乐场型可视游戏的数据集的方法，所述方法包括以下步骤：

- (a) 为娱乐场游戏提供一数据集；
- (b) 计算该数据集特有的第一简缩位串；
- (c) 对该简缩位串进行加密以便产生一个标记；
- (d) 存储存该数据集和该标记；
- (e) 根据被存储的数据集计算第二简缩位串；
- (f) 对被储存的标记进行解密以便恢复第一简缩位串； 和
- (g) 比较第一和第二简缩位串以便确定第一和第二简缩位串是否匹配。

2、根据权利要求1 所述的方法，其中所述计算步骤 (b) 是用一个散列函数执行以产生该数据集的一散列值，其中所述第一简缩位串包括该数据集的散列值。

3、根据权利要求2 所述的方法，其中该散列值包括该数据集的信息提要。

4、根据权利要求1 所述的方法，其中所述加密步骤 (c) 是用专有加密密钥执行的。

5、根据权利要求1 所述的方法，其中所述解密步骤 (f) 是用公用解密密钥执行的。

6、根据权利要求1 所述的方法，其中所述加密步骤 (c) 是用专有加密密钥执行的，所述解密步骤 (f) 是用公用解密密钥执行的。

7、根据权利要求1 所述的方法，其中所述计算步骤 (e) 是用一个散列函数执行以产生该被储存数据集的一散列值，其中所述第二简缩位串包括该被储存数据集的散列值。

8、根据权利要求7 所述的方法，其中该散列值包括该被储存数据集的信息提要。

9、根据权利要求1所述的方法，其中所述储存步骤(d)包括将该数据集和标记储存到一大容量存储设备中的步骤。

10、根据权利要求9所述的方法，其中该大容量存储设备包括一个磁盘驱动单元。

11、根据权利要求9所述的方法，其中该大容量存储设备包括一个C D - R O M 单元。

12、根据权利要求9所述的方法，其中该大容量存储器包括一个网络存储系统。

13、根据权利要求1所述的方法，其中所述步骤(a)到(d)在第一场所执行，其中所述步骤(e)到(g)在第二场所执行。

14、根据权利要求13所述的方法，其中第一场所包括制做设备，其中第二场所为博奕设备。

15、一种用于制作可鉴别的娱乐场游戏数据集的方法，所述方法包括步骤：

- (a) 为娱乐场游戏提供一数据集；
- (b) 计算该娱乐场游戏数据集特有的第一简缩位串；
- (c) 对该简缩位串进行加密以便产生一个标记；和
- (d) 储存该娱乐场游戏数据集和该标记。

16、根据权利要求15所述的方法，其中所述计算步骤(b)是用一个散列函数执行以产生该被储存娱乐场游戏数据集的一散列值，其中所述第一简缩位串包括该被储存娱乐场游戏数据集的散列值。

17、根据权利要求16所述的方法，其中该散列值包括该娱乐场游戏数据集的信息提要。

18、根据权利要求15所述的方法，其中所述加密步骤(c)是用专有加密密钥执行的。

19、根据权利要求15所述的方法，其中所述储存步骤(d)包括将娱乐

场游戏数据集和标记储存到一大容量存储设备中的步骤。

2 0 、根据权利要求1 9 所述的方法，其中该大容量存储设备包括一个磁盘驱动单元。

2 1 、根据权利要求1 9 所述的方法，其中该大容量存储设备包括一个C D - R O M 单元。

2 2 、根据权利要求1 9 所述的方法，其中该大容量存储设备包括一个网络存储系统。

2 3 、一种对具有一被加密标记的娱乐场型可视游戏的娱乐场游戏数据集进行鉴别的方法，其中该被加密标记是自娱乐场游戏数集算出的第一简缩位串被加密的，所述方法包括步骤：

- (a) 根据娱乐场游戏数据集计算第二简缩位串；
- (b) 对该标记进行解密以便恢复第一简缩位串； 和
- (c) 将第一和第二简缩位串进行比较以便确定第一和第二简缩位串是否匹配。

2 4 、根据权利要求2 3 所述的方法，其中所述计算步骤 (a) 是用一个散列函数执行以产生该娱乐场游戏数据集的一散列值，其中所述第二简缩位串包括该娱乐场游戏数据集的散列值。

2 5 、根据权利要求2 4 所述的方法，其中该散列值包括该娱乐场游戏数据集的信息提要。

2 6 、根据权利要求2 3 所述的方法，其中所述解密步骤 (b) 是用公用解密密钥执行的。

2 7 、一种用于提供对娱乐场型游戏的数据集进行鉴别的电子博奕系统，所述系统包括：

第一装置，用于储存一娱乐场游戏数据集和所述游戏数据集的一标记，所述标记包括根据该娱乐场游戏数据集算出的唯一的第一简缩位串的一加密版本；

第二装置，用于储存一鉴别程序，该鉴别程序可以根据所述第一存储单元中

储存的娱乐场游戏数据集计算第二简缩位串以及可以对所述第一存储装置中储存的加密标记进行解密以便恢复第一简缩位串；

处理装置，用于启动鉴别程序以根据所述第一存储装置中储存的娱乐场游戏数据集计算一个简缩位串以及用于启动鉴别程序以对所述第一存储装置中储存的加密标记进行解密以便产生一个被解密的简缩位串；和

比较装置，用于将被算出的第二简缩位串与被解密的简缩位串进行比较以便确定这两者是否匹配。

2 8 、根据权利要求2 7 所述的系统，其中所述第一存储装置包括一个大容量存储设备。

2 9 、根据权利要求2 8 所述的系统，其中所述大容量存储设备包括一个磁盘驱动单元。

3 0 、根据权利要求2 8 所述的系统，其中所述大容量存储设备包括一个C D - R O M 单元。

3 1 、根据权利要求2 8 所述的系统，其中所述大容量存储设备包括一个网络存储器单元。

3 2 、根据权利要求2 7 所述的系统，其中所述第二存储装置包括一个只读存储器装置。

3 3 、根据权利要求3 2 所述的系统，其中所述只读存储器装置包括一个不可修改的存储器装置。

3 4 、根据权利要求3 2 所述的系统，其中所述只读存储器装置包括用于储存所述鉴别程序的可以根据娱乐场游戏数据集计算简缩位串的一部分的第一部分和用于储存鉴别程序的可以对加密标记进行解密的的一部分的第二部分。

3 5 、根据权利要求3 4 所述的系统，其中所述第二R O M 部分用于存储一解密密钥。

3 6 、一种用于鉴别娱乐场游戏数据集和加密标记的不可修改的只读存储器装置，该加密标记是自根据娱乐场游戏数据集算出的原始信息提要被加密的，该

只读存储器装置中已经储存了与用于计算娱乐场游戏数据集的原始信息提要的信息提要程序相对应的信息提要计算程序、以及储存了与制作原始信息提要的加密标记时所用的加密程序和加密密钥相对应的解密程序和解密密钥。

3 7 、根据权利要求3 6 所述的装置，其中信息提要计算程序包括一个散列函数。

3 8 、根据权利要求3 6 所述的装置，其中该储存的解密密钥包括一个公用密钥。

3 9 、根据权利要求3 6 所述的装置，还包括一个储存在所述不可修改的只读存储器装置中的用于保证信息提要计算程序、解密程序和解密密钥的使用的初始装入程序。

4 0 、一种用于制作可鉴别的娱乐场游戏软件信息的方法，所述方法包括步骤：

- (a) 提供有关娱乐场游戏的软件信息；
- (b) 计算娱乐场游戏软件信息特有的第一简缩位串；
- (c) 对该简缩位串进行加密以便产生一个标记； 和
- (d) 储存该娱乐场游戏软件信息和该标记。

4 1 、根据权利要求4 0 所述的方法，其中所述计算步骤 (b) 是用一个散列函数执行以产生该被储存娱乐场游戏软件信息的一散列值，其中所述第一简缩位串包括该被储存娱乐场游戏软件信息的散列值。

4 2 、根据权利要求4 1 所述的方法，其中该散列值包括该娱乐场游戏软件信息的信息提要。

4 3 、根据权利要求4 0 所述的方法，其中所述加密步骤 (c) 是用专有加密密钥执行的。

4 4 、根据权利要求4 0 所述的方法，其中所述储存步骤 (d) 包括将该娱乐场游戏软件信息和标记储存到一存储器装置中的步骤。

4 5 、一种对具有加密标记的娱乐场游戏软件信息进行鉴别的方法，其中该

加密标记是从根据该娱乐场游戏软件信息算出的第一简缩位串被加密的，所述方法包括步骤：

- (a) 根据该娱乐场游戏软件信息计算第二简缩位串；
- (b) 对该标记进行解密以便恢复第一简缩位串；和
- (c) 将第一和第二简缩位串进行比较以便确定第一和第二简缩位串是否匹配。

4 6、根据权利要求4 5 所述的方法，其中所述计算步骤 (a) 是用一个散列函数执行以产生该娱乐场游戏软件信息的一散列值，其中所述第二简缩位串包括该娱乐场游戏软件信息的散列值。

4 7、根据权利要求4 6 所述的方法，其中该散列值包括该娱乐场游戏软件信息的信息提要。

4 8、根据权利要求4 5 所述的方法，其中所述解密步骤 (b) 是用公用密钥执行的。

4 9、一种用于提供对有关娱乐场型游戏的软件信息进行鉴别的电子博奕系统，所述系统包括：

第一装置，用于储存娱乐场游戏软件信息和所述娱乐场游戏软件信息的标记，所述标记包括根据该娱乐场游戏软件信息算出的唯一的第一简缩位串的加密版本；

第二装置，用于储存一鉴别程序，该鉴别程序可以根据所述第一存储装置中储存的娱乐场游戏软件信息计算第二简缩位串以及可以对所述第一存储装置中储存的加密标记进行解密以便恢复第一简缩位串；

处理装置，用于启动鉴别程序以根据所述第一存储装置中储存的娱乐场游戏软件信息计算一个简缩位串以及用于启动鉴别程序以对所述第一存储装置中储存的加密标记进行解密以便产生一个被解密的简缩位串；和

比较装置，用于将被算出的第二简缩位串与被解密的简缩位串进行比较以便确定这两者是否匹配。

5 0、根据权利要求4 9 所述的系统，其中所述第一存储装置包括一个存储

器装置。

5 1 、根据权利要求5 0 所述的系统，其中所述存储器装置包括一个只读存储器。

5 2 、根据权利要求5 0 所述的系统，其中所述存储器装置包括一个R A M

5 3 、根据权利要求4 9 所述的系统，其中所述第二存储装置包括一个只读存储器装置。

5 4 、根据权利要求5 3 所述的系统，其中所述只读存储器装置包括一个不可修改的存储器装置。

5 5 、根据权利要求5 3 所述的系统，其中所述只读存储器装置包括用于存储所述鉴别程序的可以根据该娱乐场 游戏软件信息计算简缩位串的一部分的第一部分和用于储存鉴别程序的可以对加密标记进行解密的一部分的第二部分。

5 6 、根据权利要求5 3 所述的系统，其中所述第二R O M 部分用于储存解密密钥。

5 7 、根据权利要求4 9 所述的系统，其中所述娱乐场游戏软件信息包括程序信息。

5 8 、根据权利要求4 9 所述的系统，其中所述娱乐场游戏软件信息包括一固定数据集。

5 9 、一种用于鉴别娱乐场游戏软件信息和加密标记的不可修改的只读存储器装置，该加密标记是从根据娱乐场游戏软件信息算出的原始信息提要被加密的，该只读存储器装置中已经储存了与用于计算娱乐场游戏软件信息的原始信息提要的信息提要程序相对应的信息提要计算程序、以及储存了与制作原始信息提要的加密标记时所用的加密程序和加密密钥相对应的解密程序和解密密钥。

6 0 、根据权利要求5 9 所述的装置，其中信息提要计算程序包括一个散列函数。

6 1 、根据权利要求5 9 所述的装置，其中该储存的解密密钥包括一个公用密钥。

6 2 、根据权利要求5 9 所述的装置，还包括一个储存在所述不可修改的只读存储器装置中的用于保证信息提要计算程序，解密程序和解密密钥的使用的初始装入程序。

说 明 书

具有改进的活动容量、鉴别能力和安全性的电子娱乐场博奕系统

本发明涉及以微处理器为基础的用于冒险娱乐场的博奕系统。

以微处理器为基础的用于冒险娱乐场，以扩充传统的投币机游戏（例如，三取一游戏或分类游戏）和诸如扑克和黑杰克之类的纸牌游戏的博奕系统是众所周知的。在一个这种类型的典型博奕系统中，以微处理机为基础的系统包括用于提供游戏活动能力的硬件和软件部分。硬件部分包括一个用于显示游戏活动的视频显示器，用于让玩家选择其它纸牌或游戏活动的机械开关，硬币接收器和检测器以及在以微处理器为基础的系统中常见的诸如随机存取存储器（R A M）、只读存储器（R O M）、处理器和一条或多条总线之类的电子部件。软件部分包括初始化软件，信贷与支付子程序，游戏图像与规则数据集，和一个随机数发生器算法。为了适合于娱乐场，电子博奕系统必须为软件部分提供保密和鉴别性能。为此，博奕委员会至今已要求电子博奕系统的所有软件部分被储存在不可修改的存储器中，该存储器典型地是不可修改的R O M。另外，一般要在由博奕委员会指定的安全场所保存一份R O M的内容或该内容的信息提要（或这两者）进行存档以便从博奕机上取下的单个R O M的内容能够与保管的版本核对。

在一个典型的管理方法中，在R O M被安装到博奕机上之前通过使用一种被称为散列函数的已知算法初始地产生了R O M内容的信息提要。散列函数是一种计算程序，它从一可变尺寸的数字输入产生一个固定尺寸的位串。该固定尺寸的位串被作为散列值。如果散列函数难以转换 - 作为单值散列函数 - 那么还可以把散列函数作为信息提要函数，其结果作为信息提要。对任何给定的可变尺寸输入数据集即，储存在R O M中的游戏数据集来说，信息提要都是唯一的。当以后需要对任何给定的游戏机上的R O M进行鉴别时，从游戏操纵台上取出R O M，然后用原来的散列函数直接从R O M计算出R O M内容的信息提要。被计算出的信

息提要与在指定的保管场所（一般在娱乐场所内）归档的信息提要进行比较。每当游戏机产生一个超出给定限值的清算结果时，一般就要执行这个程序。如果两个信息提要匹配，那么就认为该R O M的内容是被鉴别过的（被核实过的），于是就向玩家付偿。

尽管已经觉得这样的电子娱乐场博奕系统有助于促进娱乐场游戏活动，要求将娱乐场游戏程序储存在不可修改的R O M存储器中的这样限制产生了许多不利的条件限制。首先，由于通常用于储存程序的R O M存储媒体的容量有限，因此严重限制了这种系统的可利用的游戏活动范围。对于使用动作图像和伴音多媒体部件的复杂游戏来说，需要更多的存储器容量，大约为几百兆字节。然而，实践证明这么大量的具体设备是不切实际的，因而极大地妨碍了为更多的玩家制作复杂游戏。其次，鉴别检查仅仅是在限定的基础上或在其它重大比赛以后才执行的，并且鉴别过程要求在证实R O M内容的可靠性之前停止游戏活动。

本发明包括一个电子娱乐场博奕系统，它极大地扩充了娱乐场游戏活动能力以及增强了保密性能和鉴别性能。特别是，本发明包括一个电子娱乐场博奕系统与方法，它极大地扩充了用于储存大量高清晰度，高音质娱乐场型游戏的大容量存储能力以及提供了已储存的游戏程序信息的增强型鉴别，并带有高保密因数

根据本发明的第一特征，对娱乐场游戏数据集的鉴别是用娱乐场游戏操纵台上的不可能修改的R O M中储存的鉴别程序在游戏操纵台上进行的。娱乐场游戏数据集和一个专门标记储存在大容量存储装置中，该大容量存储装置可以包括一个只读单元或者一个读/写单元，它或者可以安装在娱乐场游戏操纵台上或者可以安放在远处并通过合适的网络与娱乐场游戏操纵台连接起来。储存在不可修改的R O M中的鉴别程序在适当的时候，如在游戏活动开始之前，在游戏活动间隙期间或当提出要求时对娱乐场游戏数据集进行鉴别检查。在适当的时刻，通过计算不可修改的R O M中的内容的信息提要并将这计算出的信息提要与在R O M被安装到娱乐场游戏操纵台上之前被安全储存的从R O M内容中算得的信息提要的拷贝进行比较可以核实不可修改的R O M中的内容。

从处理过程角度看，本发明的这个方面包括一种用于鉴别娱乐场型游戏数据集的方法，它由两阶段组成：游戏数据集制做阶段和游戏数据集检查阶段。在游戏数据集制做阶段中，该方法开始做下列工作：为娱乐场游戏提供数据集，计算娱乐场游戏数据集所特有的第一简缩位串，对第一简缩位串进行加密以便给娱乐场游戏数据集设置一个加密标记，以及将娱乐场游戏数据和该标记存入到大容量存储装置中。最好用散列函数计算第一简缩位串以便产生娱乐场游戏数据集的信息提要。然后从该信息提要对该标记进行加密。当娱乐场游戏数据集和专门标记被储存以后，这个信息就被装入到娱乐场游戏操纵台上。娱乐场游戏数据集检查阶段执行下列工作：用同样的散列函数从被储存的娱乐场游戏数据集中计算出第二简缩位串，对被储存的加密标记进行解密以便恢复第一简缩位串，以及将第一和第二简缩位串进行比较以便确定这两种位串是否匹配。如果匹配，那么就认为娱乐场游戏数据集是可靠的；如果不匹配，那么就拒绝鉴别并且禁止游戏活动。

加密/解密过程最好用专有密钥/公共密钥技术执行，在该技术中，游戏制造商用他们自身保管的专有加密密钥对第一简缩位串进行加密。对标记的解密可以用公共密钥来做，公共密钥与娱乐场游戏数据集一起储存在游戏操纵台上的不可修改的只读存储器中。娱乐场程序数据集最好储存在诸如磁盘驱动单元或C D - R O M 盘驱动单元或网络文件单元之类的大容量存储装置中，所选择的单元具有相对较大的容量。大容量存储装置的实际容量将取决于娱乐场游戏的存储要求并且能满足任何特定应用的要求。

每当将娱乐场游戏数据集从大容量存储装置传送到系统主存储器中时，就要运行鉴别程序。鉴别程序还可以为安装在游戏操纵台上的操作器开关或者通过网络的遥控远程操作器开关。因此，每当发生数据传送以及在其它适当的时候总是可以自动检查数据集的可靠性。

为了检测游戏操纵台上的不可修改的只读存储器中的内容是否被窜改，可以将为其中储存的鉴别程序而算出的信息提要安全地储存在游戏操纵台以外的场所，如储存在娱乐场管理人员的保密设备中或储存在博奕委员会的设备中（或储存在

这两处）。对不可修改的只读存储器元件的可靠性的检查方式与目前在现有设备上所用的方式相同，即直接从不可修改的只读存储器设备中计算信息提要以及将这样算出的信息提要与保管的文本进行比较。

从装置的角度看，本发明的第一方面包括一个具有在允许进行游戏活动之前对娱乐场型游戏的游戏数据集进行鉴别的装置的电子娱乐场博奕系统，该系统包括用于储存娱乐场游戏数据集和游戏数据集的标记的第一装置，该标记包括从娱乐场游戏数据集算出的唯一的第一简缩位串的加密版本；用于储存鉴别程序的第二装置，该鉴别程序能从第一存储单元中储存的游戏数据集出计算出第二简缩位串以及能对第一存储装置中储存的加密标记进行解密以便恢复第一简缩位串；用于使鉴别程序从第一存储装置中储存的娱乐场游戏数据集计算一个简缩位串并用于使鉴别程序对加密标记进行解密的处理装置；及用于将被算出的第二简缩位串与被解密的简缩位串进行比较以便确定这两者是否匹配的装置。第一存储装置最好包括一个大容量存储设备，如磁盘驱动单元，C D - R O M 单元或网络存储单元。第二存储装置最好包括一个储存鉴别程序的不可修改的只读存储器。

根据本发明的第二方面，储存在娱乐场游戏操作台上的不可修改的R O M 中的鉴别程序被用于对储存在电子娱乐场博奕系统的存储设备，例如系统引导R O M，含有操作系统程序、系统驱动程序和执行/装入程序的存储设备，和并入到电子娱乐场博奕系统结构中的其它存储器设备中的所有其它程序和固定数据的可靠性进行测试。每个这样的存储设备中的内容，无论是程序信息还是固定数据，都包括根据使用散列函数从原始程序信息或固定数据集中算出的信息提要被加密的标记。当系统初始化时，储存在不可修改的R O M 中的鉴别程序被用于对各个存储设备中的内容进行鉴别，所采用的方式与鉴别娱乐场游戏数据集时所采用的方式基本相同。更具体地，使用与原始所用的相同散列函数计算用于给定的程序或固定数据集信息以产生用于该程序或该固定数据集的信息提要。为恢复信息提要，可以用合适的解密程序和解密密钥对加密的标记进行解密。然后将这两个版本的信息提要进行比较，如果发现这两个版本一致，那么就认为有关程序或固定

数据集是可靠的因而允许它由该系统使用。一旦所有的有关程序和固定数据集被这样鉴别以后，就进行娱乐场游戏数据集的鉴别过程，然后允许进行游戏活动（假定鉴别结果是匹配的）。

从处理过程角度看，本发明的第二方面包括一种用于鉴别一程序或一娱乐场型游戏程序的游戏数据集的方法，它由两阶段组成：一程序或固定数据集制做阶段和程序或固定数据集检查阶段。在程序或固定数据集制做阶段中，该方法开始做下列工作：为娱乐场游戏提供一程序或固定数据集，计算该程序和固定数据集所特有的第一简缩位串，对第一简缩位串进行加密以便设置该程序或固定数据集的一加密标记，以及将该程序或固定数据集和该标记存入到存储设备中。最好用散列函数来计算第一简缩位串以便产生该程序或固定数据集的信息提要。然后将从该信息提要对该标记进行加密。当程序或固定数据集和特有标记被储存到存储设备中以后，该存储设备就被安装到娱乐场游戏操纵台上。娱乐场游戏程序或固定数据集阶段执行下列工作：根据存储器设备中储存的娱乐场游戏程序或固定数据集用同样的散列函数计算第二简缩位串，对储存在存储器设备中的加密标记进行解密以便恢复第一简缩位串，以及将第一和第二简缩位串进行比较以便确定这两位串是否匹配。如果匹配，那么就认为娱乐场游戏程序或固定数据集是可靠的；如果不匹配，那么就拒绝鉴别并且禁止使用那个娱乐场游戏程序或固定数据集。

每当需要调入或使用一给定的娱乐场游戏程序或固定数据集时就要运行鉴别子程序。还可以定期运行鉴别子程序或当需要时 - 或者是由安装在娱乐场游戏操作台上的操作器开关提出的请求或者是通过网络从远处提出的请求时立刻执行鉴别子程序。因此，每当需要使用那个程序或固定数据集时以及在其它适当的时候，如在博奕委员会检查期间，总是可以自动检查娱乐场游戏程序或固定数据集的可靠性。

从装置的角度看，本发明的第二方面包括一个用于在允许使用那个casion游戏程序或固定数据集的系统之前，对娱乐场游戏程序或固定数据集进行鉴别的电子娱乐场博奕系统，该系统包括用于储存娱乐场游戏程序或固定数据集及其标记

的第一装置；该标记包括根据娱乐场游戏程序或固定数据集算出的唯一的第一简缩位串的加密版本；用于储存鉴别程序的第二装置，该鉴别程序能根据第一存储装置中储存的娱乐场游戏程序或固定数据集计算出第二简缩位串以并能对第一存储装置中储存的加密标记进行解密以便恢复第一简缩位串；用于使鉴别程序可根据第一存储装置中储存的娱乐场游戏程序或固定数据集计算出第二简缩位串并用于使鉴别程序对加密标记进行解密的处理装置；及用于将被算出的第二简缩位串与被解密的简缩位串进行比较以便确定这两者是否匹配的装置。第一存储装置最好包括一个存储器设备，如只读存储器或随机存取存储器。第二存储装置最好包括一个储存鉴别程序的不可修改的只读存储器。

本发明的电子娱乐场博奕系统在不损害安全性又提高对游戏的鉴别活动能力的同时大大扩充了供更复杂和更吸引人的娱乐场型游戏使用的容量。另外，由于代表各种游戏的娱乐场游戏数据集可以被储存在可修改的媒体中而不是象在现有娱乐场博奕系统中那样被储存在只读存储器中，因此本发明的博奕系统在改变游戏活动方面有很大的灵活性。

通过将鉴别处理从娱乐场游戏数据集存储器中分离出来，本发明能安全分配与执行程序码和数据，这与所采用的具体分配或存储技术无关。更准确地说，本发明允许娱乐场游戏数据集驻留在诸如传统的R O M 存储器、硬盘驱动器与 CD -ROM驱动器，或网络文件系统之类任何类型的二级存储器媒体中。只要用不可修改的R O M 中储存的鉴别程序执行对游戏数据集进行鉴别，并且只要能证实那个R O M 是可靠的，那么在任何时候：或者在使用之前、程序运行期间。程序运行期间的固定时刻或当要求时，系统都可以从任何存储源中装入娱乐场游戏数据集并对它进行核实。

以本发明的安全方式可使大量存储器被利用，有助于建立既能提供各种各样的游戏又能提供高质量的单个游戏的娱乐场博奕系统。另外，对所有娱乐场游戏程序和固定数据软件的鉴别可以保证整个系统软件在游戏活动之前及此后固定时间内或随机时间内的完整性。

为了更全面地理解本发明的性质和优点，以下将参考附图作详细说明。

图1 是本发明系统的方框图；

图2 是用于说明只读存储器和大容量存储设备中的内容的示意图；

图3 是储存在R O M 中的鉴别程序和储存在大容量存储器单元中的游戏数据的更详细的示意图；

图4 是用以说明游戏数据集的准备的示意图；

图5 是用以说明对游戏数据集的鉴别程序的示意图；

图6 是用以说明另一种将软件安全装入系统的方法的示意图。

现在转到附图，图1 是本发明电子娱乐场博奕系统的方框图。如图所示，该系统由几个受软件控制的系统部件组成。这些系统部件包括一个微处理器1 2，它可以是任何通用微处理器，如英特尔公司公司的奔腾微处理器。一个主存储器单元1 3 被设置，它是一个容量在3 2 兆字节和6 4 兆字节之间的典型随机存取存储器，用于储存游戏活动过程所用的主要程序和图形元素，一个系统引导R O M1 4，用于提供系统第一次通电时所需的初始化软件，R O M1 4 中含有辅助只读程序，包括操作系统程序、有关驱动程序和下面将详细说明的鉴别程序。一个非易失性R A M1 7，它是一由电池支持的静态R A M，通过电力循环它能保持自己储存的内容，N V R A M1 7 内储存了有关游戏活动的重要信息，如玩家信贷数量、最终的游戏结果以及一些对理解本发明并不重要的诊断和出错信息。

在图1 所示系统中作为硬盘驱动单元1 8 的大容量存储器单元被连接到常规设计和操作的硬盘子系统1 9 上并受它控制。硬盘驱动单元1 8 给包括程序数据和图像数据（用于规定各种不同的娱乐场游戏或单个娱乐场变化的规则和用于规定图像类型和图像显示顺序）在内的游戏特定数据集提供存储器。硬盘驱动单元1 8 的容量随为给定系统提供的游戏数量和游戏变化以及每个特定游戏所要求的数据量而变。总的来说，一具体娱乐场游戏中的动作图像越多，该娱乐场游戏软件所要求的存储器也越多。4 G 字节容量的硬盘驱动单元1 8 一般就能提供足够的存储容量。硬盘子系统1 9 包括一个连接到P C I 总线2 0 上的用于控制硬盘

驱动单元1 8 的硬盘控制器。控制器1 9 最好支持随传输速度和传输量而选的S C S I - 2 。应当注意在图1 所示的系统中可以采用许多不同类型的基于局部的硬盘驱动单元，包括C D - R O M 存储器单元。还有，大容量存储器单元以及图1 中示出的其它部件不需要放置在游戏操纵台中：大容量存储器单元可以远离游戏操纵台，通过诸如以太网、R S 2 3 2 链路，或者一些其它的硬连线或无线网络连接到游戏操纵台上。后面的这种替代的配置包括具有合适的结构和功能特性的网络子系统2 1 ，它可以与以太网、R S 2 3 2 串行口或其它网络兼容。

视频子系统2 2 连接到P C I 总线上，并提供了在合适的监视器（没有示出）上以较高的帧速率（例如，每分钟3 0 帧）显示全彩色静止图像和显示M P E G 影片的能力。如果需要的话，可以将任选3 D 结构映像加到这个系统中。

声音子系统2 3 连接到I S A 总线2 4 上，它具有播放音质高达1 6 位C D 音质的立体声的能力。通用输入/ 输出单元2 5 提供了与诸如手动开关和显示灯之类的游戏机械设备（没有示出）连接的接口。第一桥接电路2 7 在微处理器1 2 、R O M1 4 、主存储器1 3 和P C I 总线2 0 之间提供了一个接口。桥接电路2 7 最好是英特尔公司的T R I T O N 芯片构成的电路。第二桥接电路2 8 在P C I 在总线2 8 和I S A 总线2 4 之间提供了一个接口。桥接电路2 8 最好是英特尔公司的8 2 3 7 8 芯片。

图2 说明了系统R O M1 4 和大容量存储器单元中储存的信息种类。如图2 所示，在图1 系统中所用的R O M1 4 包括两个独立的R O M 元件：R O M2 9 和R O M3 0 。R O M2 9 必须是不可修改的设备，如东芝公司生产的5 1 2 K ×8 位的C 5 3 4 0 0 掩模编程R O M 。R O M3 0 最好是与R O M2 9 相似的不可修改的设备，也可以是其它类型的R O M ，如英特尔公司生产的2 9 F O 4 0 现场可编程闪速R O M 。R O M2 9 中含有系统初始化或引导码、鉴别程序、随机数发生器程序和执行/ 装入程序的起始部分。R O M3 0 中含有操作系统程序、系统驱动程序和下面将提到的执行/ 装入程序的剩余部分。大容量存储器单元中含有应用程序，它包括游戏图像和声音数据、游戏活动规则等，以及与每个

具体娱乐场游戏有关的标记。

图3 更详细地说明了鉴别程序和应用程序信息，如图所示，储存在不可修改的R O M 2 9 中的鉴别信息包括信息提要算法部分3 2，解密算法部分3 3，和解密密钥部分3 4。储存在R O M 2 9 中的信息提要算法部分3 2 包括一个散列函数例行程序的精确拷贝，该散列函数例行程序被用于根据可装入游戏数据集3 6 以下列所述的方式初始地计算信息提要。储存在R O M 2 9 中的解密算法部分3 3 包括一个用解密密钥部分3 4 对被加密的娱乐场游戏数据集标记进行解密时所需的算法。

解密密钥部分3 4 包括一个在鉴别程序中以下面所述的方式对任何加密标记3 7 进行解密时所要求的解密密钥。

图4 说明了加密数据集标记3 7 的产生方式。用散列函数4 1 对可装入娱乐场游戏数据集3 6 进行处理从而产生一个对可调入游戏数据集3 6 来说唯一的信息提要4 2。所用的散列函数可以是诸如MD 2、MD 4 和MD 5 散列函数以及S H S 散列函数之类的多个已知散列函数中的一个散列函数；或是能根据可变大小输入数据集产生一个专门的简缩位串的任何其它合适的散列函数。有关这些散列函数的进一步信息可参阅文献：“Answers To Frequently Asked Questions About Today's Cryptography”，Revision2 . 0，October5 , 1993，Published by RSA Laboratories, Redwood City, California, 及其参考部分中列出的文献，其中公开的部分特此作为参考资料的一部分。信息提要4 2 产生以后，用专有加密密钥4 4 以加密程序4 3 对信息提要4 2 进行加密从而产生信息提要的标记3 7。在优选实施例中，采用了由R S A 数据保密公司开发的双密钥（专有/公共密钥）加密技术。美国专利N o. 4 , 2 0 0 , 7 7 0 , 4 , 2 1 8 , 5 8 2 和4 , 4 0 5 , 8 2 9 公开并说明了这项技术，也将其引用在此作为参考。然后，将信息提要4 2 的标记3 7 与可调入数据集3 6 一起存入到大容量存储器单元中。

图5 说明了按照本发明执行的鉴别程序。当调入鉴别程序时（看下面），将

可装入娱乐场游戏数据集3_6 从大容量存储器单元传送到主存储器1_3 中 (除了它已经在主存储器1_3 中之外) , 然后用信息提要算法3_2 计算娱乐场游戏数据集3_6 的信息提要。信息提要算法3_2 所用的散列函数4_1 与制造商在准备原始信息提要4_2 时所用的散列函数相同。结果为根据大容量存储器单元中当前储存的娱乐场游戏数据集3_6 算出的信息提要的一个未加密版本4_6 。用与专有密钥 (其被用于初始地对娱乐场游戏数据集3_6 的信息提要4_2 进行加密) 相匹配的公共解密密钥3_4 对加密数据集标记3_7 进行解密。然后将用解密密钥3_4 解密后的信息提要4_7 与根据娱乐场游戏数据集3_6 计算出的信息提要4_6 进行比较。如果这两个信息提要匹配, 那么就认为娱乐场游戏数据集3_6 是可靠的因而游戏活动可以进行。如果这两者不匹配, 那么就认为或者是娱乐场游戏数据集3_6 不可靠或者是标记3_7 不可靠。因而禁止游戏活动并可以采取适当的措施: 例如, 用合适的信息系统向保卫人员发送警报 (声音报警、闪光灯或从游戏操纵台发送到中央安全区的网络信息) 。

为了保证不会因R OM3_0 中的装入程序被篡改而越过鉴别程序, 因此将装入程序的起始部分装入到不可修改的R OM2_9 中。装入程序的这个起始部分要求在任何娱乐场游戏活动开始以前先调入鉴别程序。由于装入程序的这个起始部分被放置在不可修改的R OM2_9 中并且在具体的娱乐场游戏应用数据集3_6 被装入主程序器1_3 之前无娱乐场游戏活动, 因此, 不会因R OM3_0 中的软件被篡改而越过鉴别程序。

由于对游戏数据集3_6 和标记3_7 的鉴别是委托R OM2_9 中的内容来做的, 因此必须要有一个对R OM2_9 中的内容进行核实的程序。为此目的, 可以为R OM2_9 中的鉴别程序计算一个信息提要, 该信息提要与用于产生该信息提要的散列函数一起被娱乐场经营者或博奕委员会 (或这两者) 以保密方式保存起来。该散列函数可以与用于计算娱乐场游戏数据集的信息提要4_2 的散列函数相同或者不同。这样, 用目前在已有技术设备中所用的方法就可以方便地检查R OM2_9 的可靠性, 即, 直接根据R OM2_9 中的内容计算信息提要并将这样计算出的

信息提要与信息提要的保管版本进行比较。如果博奕委员会提出要求或者娱乐场经营者觉得需要，那么系统还可以显示各单个具体数据集3 6 的信息提要4 2 或显示加密标记版本3 7 以供审查。另外，系统可以通过网络子系统2 1 就地传送或向远处（如博奕委员会的办公室）传送这些信息。被显示或被传送的信息提要可以包括解密后的版本或计算出的版本（或这两者）。

用不可修改的R O M2 9 中储存的信息提要程序3 2 、解密程序3 3 和解密密钥3 4 以上述方式执行的鉴别程序还被用于鉴别图1 所示系统中的所有存储器设备中的内容，如R O M3 0 中的内容（见图2 ）、N V R A M1 7 中储存的固定数据内容和程序内容，以及在网络子系统2 1 、视频子系统2 2 、声音子系统2 3 、P C I -I A S 接口2 4 和G P I O 单元2 5 中存储的任何存储器设备的程序内容和固定数据内容。这些单元中任何存储器设备中储存的各个程序或固定数据集都有一个相关标记，该相关标记是根据原始程序的信息提要或固定数据集使用一个散列函数进行加密的，该散列函数最好与在准备娱乐场游戏数据集的信息提要时所用的散列函数相同。在允许任何这样的程序或固定数据集参与系统操作以前，那个程序或固定数据集必须经过鉴别程序以保证根据该程序或固定数据集的当前版本计算出的信息提要与对该程序或固定数据集相关的加密标记解密后得到的信息提要相一致。另外，可以在固定时刻或任意时刻（当提出要求时）以与上述关于娱乐场游戏数据集的鉴别过程基本相同的方式对每个这样的程序或固定数据集进行鉴别程序。因此，在使用那个具体软件之前，系统中所有软件的完整性都得到了检查从而可以了解任何对娱乐场博奕系统的软件部分的非法修改。

将软件安全装入到系统的另一种可供选择的方法如图6 所示。在这个实施例中，基本输入/ 输出系统（B I O S ）软件储存在R O M5 0 中，两个R O M中的第一R O M构成了系统引导R O M1 4 （图1 ）。引导码、操作系统码（O S ）、O S 驱动程序和安全装入程序都储存在第二R O M5 *2 中。包括图形与声音驱动程序、系统驱动程序、资金管理程序、第二安全装入程序和标记一起在内固定应用程序5 4 储存在大容量存储器1 8 中（图1 ）。

当系统第一次通电启动或当系统热启动时，C P U 1 2 将开始执行来自R O M5 0 中的B I O S 码。B I O S 负责对系统母板和外围卡进行初始化。在B I O S 完成初始化以后，它跳到R O M5 2 的引导码中使自引导程序将操作系统程序、操作系统驱动程序和安全装入程序拷入到R A M 中。

一旦被拷入到R A M 中，操作系统程序就开始工作，并且R O M5 2 中储存的安全装入程序被用于从硬盘1 8 装入固定应用程序5 4 。固定应用程序的标记储存在硬盘上，该标记用于在装入过程中以核实固定应用程序的合法性。

固定应用程序5 4 启动后，它被用于装入其它所有的应用程序。固定应用程序中的安全装入程序通过计算该标记以及通过将计算出的标记与储存在硬盘中的与上述应用程序有关的标记进行比较来检查被装入的应用程序的合法性。

本发明的一个显著优点（已有技术系统不具备的）在于可鉴别娱乐场游戏数据集的方式。在已有技术系统中，只有当游戏活动的结果要求支付超过一给定阈值的数额时方对娱乐场游戏数据集鉴别，这样在取出R O M 以及对R O M 中的内容进行核实期间需要停止游戏活动。在本发明的系统中，可以用许多方式检查一给定娱乐场游戏数据集的可靠性。例如，每当游戏被从大容量存储器单元装入到主存储器1 3 时，游戏数据集3 b 就能自动经受图5 所示的鉴别程序。这样，当玩家为游戏活动在系统上选择一个娱乐场游戏时，用上述鉴别程序而必要取出R O M2 9 就可以自动检查储存在大容量存储器单元中的那个游戏的可靠性。还有，如果需要的话，可以根据投币游戏操纵杆的移动、硬币投入的检测结果、硬币的支付情况和信贷的配给情况或其它任何可检测的有关游戏活动的事件来启动鉴别程序。还可以通过提供请求程序，在游戏操纵台上发出请求时或从远处通过网络发出请求时检查一给定娱乐场游戏数据集3 6 的可靠性。这一程序可以用游戏台上的手动开关（仅供指定人员使用，用于启动鉴别程序的手动开关）来启动。另一方面，可以使图1 的所示的系统可被构成响应在远处（例如在娱乐场的安全场所或别的安全场所）产生的并且通过与网络子系统2 1 连接的网络发送到游戏操纵台上的请求命令。

本发明的另一个优点在于本发明系统的游戏数据集存储器的容量不是受R O M容量的限制而是受大容量存储器单元的容量限制。因此，可以设计高清晰度、高动作图像和高音质立体声游戏在本发明系统上运行。还有，由于大容量存储器单元不必是只读设备，也不必放置在游戏操纵台上，因此本发明在游戏内容的安排和更改方面具有很大的灵活性。例如，为了改变一具体娱乐场游戏或一组游戏中的图形图像，可以产生新的娱乐场游戏数据集和新的标记并通过交换硬盘驱动器、替换硬盘（对只读硬盘单元来说）、或者将新数据写入到媒体中使新的娱乐场游戏数据集和新的标记存入到大容量存储器单元中。在联网的大容量存储器应用中，可以对受网络文件服务器控制的文件作这些更改。由于娱乐场游戏数据集必须经历鉴别程序测试（或者是定期测试或者是按请求测试），因此不可靠的数据集不可能不被发现。因此本发明开辟了既适合于易修改的具有灵活显示方式和灵活规则的游戏又不损害系统的基本安全性的电子娱乐场博奕系统领域。事实上，由于本发明能定期（对于每次移动操纵杆时）和在任何时候（当提出要求时）对所有游戏数据集进行鉴别而不会干扰正常的游戏活动（除非两种信息提要不匹配），因此大大增强了系统的安全性。

尽管以上所述全面完整地公开了本发明的优选实施例，但在不脱离本发明的真实精神和范围的前提下可以采用各种改型、替代结构和等同物。例如，尽管优先选择R S A 公共/专有密钥加密技术（由于这种技术的公知的显著优点），但如果需要的话，可以采用单个专有密钥加密技术。在采用这种技术的系统中，单个密钥将代替公共密钥3 4 被储存在R O M2 9 中。还有，一给定应用程序3 6 的信息提要4 2 和标记3 7 不必根据整个娱乐场游戏数据集来计算。例如，对某些娱乐场游戏来说，当将来允许改变其游戏图形、声音或两者时，最好提供一个固定的规则集。对这种娱乐场游戏来说，或许仅根据应用程序3 6 的规则部分计算信息提要4 2 和标记3 7 就足够了。在其它情况下，当将来允许改变游戏活动的规则时保持娱乐场游戏的图像和伴音部分不变是所期望或方便的。对于这种娱乐场游戏，可以根据应用程序3 6 的图形和伴音部分计算信息提要4 2 和标记3 7 。

还可期望根据一给定应用程序^{3 6} 的规则，图形或声音部分的子集或根据一给定应用程序^{3 6} 的其它一些子集计算信息提要^{4 2} 和标记^{3 7}。因此，以上所述不应当被解释为对本发明范围的限制，本发明范围由附属权利要求来规定。

说 明 书 附 图

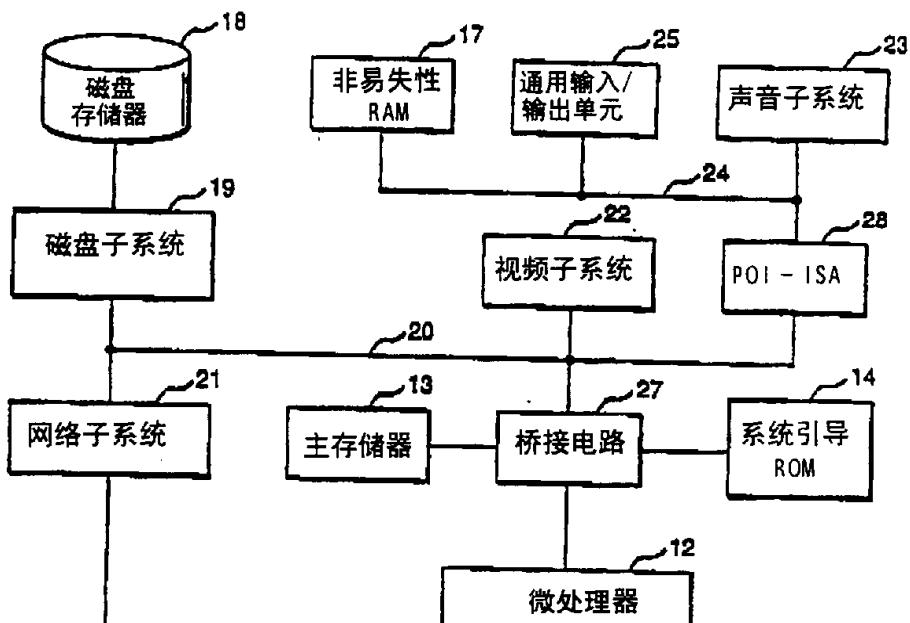


图1

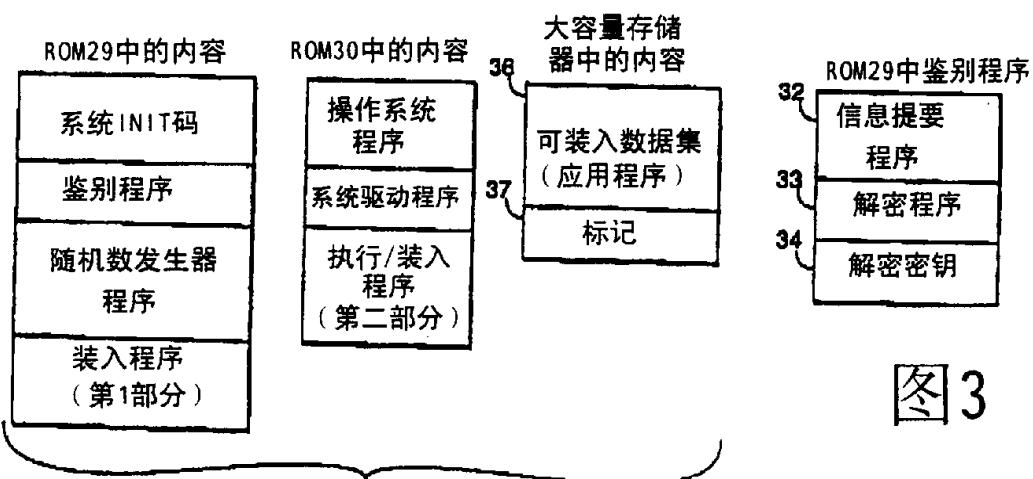


图2

图3

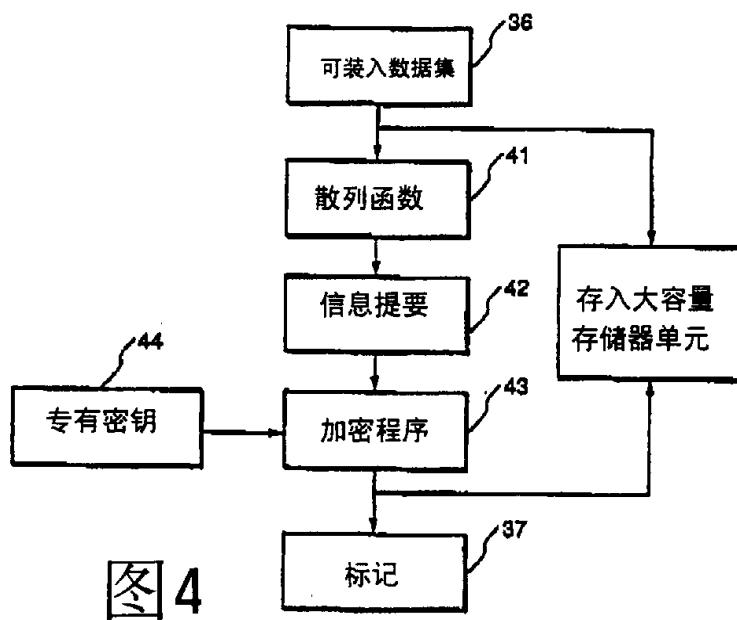


图4

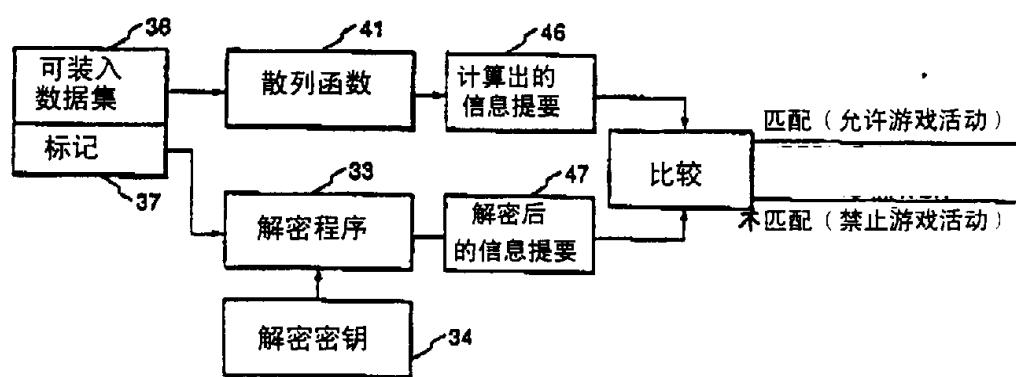


图5

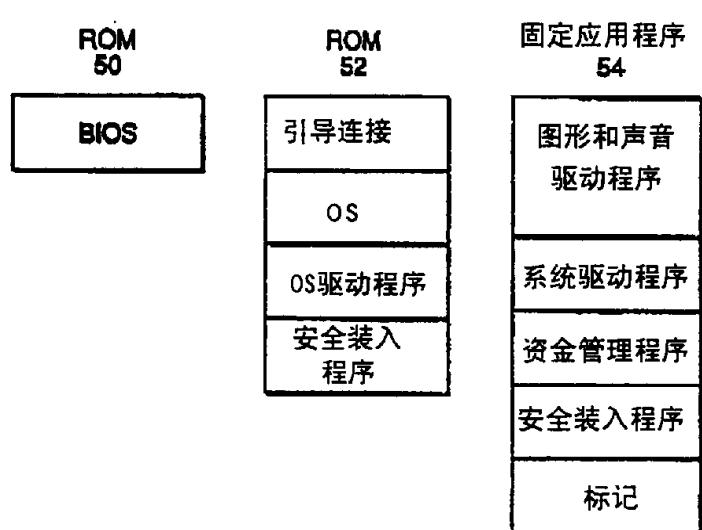


图 6