(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101610377 B
(45)授权公告日 2012.11.14

(21)申请号 200910133039.X

(22)申请日 2009.04.02

(30)优先权数据
2008-159868 2008.06.19 JP

(73)专利权人 株式会社日立制作所
地址 日本东京

(72)发明人 铃木贵之 渡边光信 小日向宣昭

(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 11038
代理人 许海兰

(51)Int.Cl.
H04N 5/913(2006.01)
G11B 20/00(2006.01)
G11B 20/10(2006.01)

审查员 夏刊

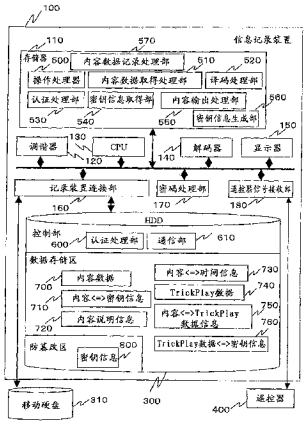
权利要求书 4 页 说明书 11 页 附图 13 页

(54)发明名称

内容重放装置、记录装置、记录重放装置及重放方法

(57)摘要

在为进行著作权保护等目的将加密密钥以某个间隔更改的重放内容的设备中，能够无问题地进行内容的重放和快进、快退等的特殊重放。预先准备用于进行特殊重放的数据和密钥信息，并用它们进行特殊重放。或者，定义加密密钥生成规则，根据该规则生成加密密钥。根据该规则预先准备所需要的密钥信息，无问题地进行重放和特殊重放。



CN 101610377 B

1. 一种重放装置，具备：

从记录媒体取得经加密的动画数据的数据取得部；

从所述记录媒体取得与所述动画数据对应的动画数据用密钥信息的密钥信息取得部；

用所述动画数据用密钥信息将所述经加密的动画数据译码的译码处理部；

将所述经译码的动画数据变换为图像信号和声音信号并输出的重放部；以及

受理来自用户的操作的操作输入部，

将能够用一个所述密钥信息所译码的所述动画数据的重放时间的上限定为预定的时间，

所述重放装置的特征在于：

进行特殊重放时，

所述数据取得部从所述记录媒体取得与重放中的与动画数据用密钥信息相应地被分割的所述动画数据对应的特殊重放数据，

所述重放部将该特殊重放数据变换成图像信号并输出，

所述特殊重放是重放速度快于普通重放的快进重放或快退重放，

所述特殊重放数据是特殊重放时使用的数据，

所述动画数据的动画数据用密钥信息是按所述预定的时间被更改，

所述特殊重放数据被加密并记录在所述记录媒体上，

所述密钥信息取得部从所述记录媒体取得与所述特殊重放数据对应的特殊重放数据用密钥信息，

所述译码处理部用所述特殊重放数据用密钥信息进行译码。

2. 权利要求 1 所述的重放装置，其特征在于：

所述动画数据是具有 I 帧、P 帧和 B 帧的动画数据，

所述特殊重放数据是所述动画数据所包含的 I 帧的集合。

3. 权利要求 2 所述的重放装置，其特征在于：

所述特殊重放数据被加密并记录在所述记录媒体上，

所述密钥信息取得部从所述记录媒体取得与所述特殊重放数据对应的特殊重放数据用密钥信息，

所述译码处理部用所述特殊重放数据用密钥信息进行译码，

能够用一个所述特殊重放数据用密钥信息译码的特殊重放数据，对应于能够用一个所述动画数据用密钥信息译码的多个动画数据。

4. 权利要求 1 所述的重放装置，其特征在于：

通过重放所述特殊重放数据的 I 帧进行所述特殊重放。

5. 权利要求 1 所述的重放装置，其特征在于：

在所述操作输入部受理特殊重放指示前，

所述密钥信息取得部取得与重放中的所述动画数据对应的所述特殊重放数据的所述特殊重放数据用密钥信息。

6. 权利要求 1 所述的重放装置，其特征在于：

所述特殊重放中，所述操作输入部受理了普通重放的指示时，

所述数据取得部和所述密钥信息取得部取得普通重放开始位置的所述动画数据和与该动画数据对应的动画数据用密钥信息，

该普通重放开始位置的动画数据和动画数据用密钥信息已取得时，所述重放部将与所述特殊重放数据对应的图像信号输出。

7. 权利要求 6 所述的重放装置，其特征在于：

从所述普通重放的指示的受理到所述普通重放的开始，以比所述特殊重放慢而比所述普通重放快的重放速度重放所述特殊重放数据。

8. 权利要求 7 所述的重放装置，其特征在于：

所述特殊重放数据含有与所述动画数据同时重放的声音数据，

从所述普通重放的指示的受理到所述普通重放的再开始，重放所述声音数据。

9. 一种重放装置，具备：

从记录媒体取得经加密的动画数据的数据取得部；

从所述记录媒体取得与所述动画数据对应的动画数据用密钥信息的密钥信息取得部；

用所述动画数据用密钥信息将所述经加密的动画数据译码的译码处理部；以及

将所述经译码的动画数据变换成图像信号和声音信号并输出的重放部，

将能够用一个所述密钥信息所译码的所述动画数据的重放时间的上限定为预定的时间，

所述重放装置的特征在于：

所述动画数据包括第一动画数据和具有所述第一动画数据所包含的图像数据的一部分的第二动画数据，

所述第一动画数据是与所述动画数据用密钥信息相应地被分割的动画数据，所述第二动画数据是与所述第一动画数据对应的特殊重放数据，

根据所述动画的重放速度，选择所述第一动画或所述第二动画进行重放，

所述特殊重放数据是特殊重放时使用的数据，

所述特殊重放是重放速度快于普通重放的快进重放或快退重放，

所述动画数据的动画数据用密钥信息是按所述预定的时间被更改，

所述特殊重放数据被加密并记录在所述记录媒体上，

所述密钥信息取得部从所述记录媒体取得与所述特殊重放数据对应的特殊重放数据用密钥信息，

所述译码处理部用所述特殊重放数据用密钥信息进行译码。

10. 权利要求 9 所述的重放装置，其特征在于：

如果指示的所述重放速度比预定的速度快，就重放所述第二动画数据，如果比所述预定的速度慢，就重放所述第一动画数据。

11. 一种记录装置，其特征在于，具备：

从外部接收动画数据的接收部；

将所述接收的动画数据加密的加密处理部；

将所述加密的动画数据记录在记录媒体上的数据记录处理部；以及

密钥信息生成部，

对于预定的时间的经加密的所述动画数据，将用于所述动画数据的译码的动画数据用密钥信息记录在所述记录媒体上，并且

记录用于所述动画数据的特殊重放的特殊重放数据，

所述密钥信息生成部生成用于对所述特殊重放数据进行译码的特殊重放数据用密钥信息，并记录在所述记录媒体上，

所述特殊重放是重放速度快于普通重放的快进重放或快退重放，

所述特殊重放数据是特殊重放时使用的数据。

12. 权利要求 11 所述的记录装置，其特征在于：

所述动画数据是具有 I 帧、P 帧和 B 帧的动画数据，

对于与被生成一个所述动画数据用密钥信息的多个所述动画数据对应的 I 帧的集合，生成一个所述特殊重放数据用密钥信息。

13. 一种记录重放装置，具备：

从外部接收动画数据的接收部；

将所述接收的动画数据加密的加密处理部；

将所述加密的动画数据记录在记录媒体上的数据记录处理部；

从所述记录媒体取得所述经加密的动画数据的数据取得部；

从所述记录媒体取得与所述动画数据对应的动画数据用密钥信息的密钥信息取得部；

用所述动画数据用密钥信息将所述经加密的动画数据译码的译码处理部；以及

将所述经译码的动画数据变换成图像信号和声音信号并输出的重放部，

用所述动画数据用密钥信息将所述动画数据译码并重放，

将能够用一个所述密钥信息所译码的所述动画数据的重放时间的上限定为预定的时间，

所述记录重放装置的特征在于：

在记录所述动画数据时，

生成第一动画数据用密钥信息，

用该第一动画数据用密钥信息和所述记录重放装置固有的信息生成第二动画数据用密钥信息，

与所述动画数据相对应地将所述第一和第二动画数据用密钥信息记录在所述记录媒体上，

在重放所述动画数据时，

从所述记录媒体取得所述第一动画数据用密钥信息，

从所述记录重放装置取得所述记录重放装置固有的信息，

从所述第一动画数据用密钥信息和所述记录重放装置固有的信息生成所述第二动画数据用密钥信息，

用所述第一和第二动画数据用密钥信息将所述动画数据译码并重放。

14. 权利要求 13 所述的记录重放装置，其特征在于，具备：

生成用于特殊重放的特殊重放数据的部分；以及

生成将所述特殊重放数据译码的特殊重放用密钥信息的部分，

在记录所述特殊重放数据时，

用该第一动画数据用密钥信息和所述记录重放装置固有的信息生成特殊重放数据用密钥信息，

与所述特殊重放数据相对应地将所述特殊重放数据用密钥信息记录在所述记录媒体上，

在重放所述特殊重放数据时，

从所述记录媒体取得所述第一动画数据用密钥信息，

从所述记录重放装置取得所述记录重放装置固有的信息，

从所述第一动画数据用密钥信息和所述记录重放装置固有的信息生成所述特殊重放数据用密钥信息，

用所述特殊重放数据用密钥信息将所述特殊重放数据译码并重放，

所述特殊重放是重放速度快于普通重放的快进重放或快退重放，

所述特殊重放数据是特殊重放时使用的数据。

15. 一种重放方法，包括：

数据取得部从记录媒体取得经加密的动画数据的步骤；

密钥信息取得部从所述记录媒体取得与所述动画数据对应的动画数据用密钥信息的步骤；

译码处理部用所述动画数据用密钥信息将所述经加密的动画数据译码的步骤；以及

重放部将所述经译码的动画数据变换成图像信号和声音信号并输出的步骤，

将能够用一个所述密钥信息所译码的所述动画数据的重放时间的上限定为预定的时间，

所述重放方法的特征在于：

在进行特殊重放时，

所述数据取得部从所述记录媒体取得与重放中的与动画数据用密钥信息相应地被分割的所述动画数据对应的特殊重放数据，

所述重放部将该特殊重放数据变换成图像信号并输出，

所述特殊重放是重放速度快于普通重放的快进重放或快退重放，

所述特殊重放数据是特殊重放时使用的数据，

所述动画数据的动画数据用密钥信息是按所述预定的时间被更改，

所述特殊重放数据被加密并记录在所述记录媒体上，

所述密钥信息取得部从所述记录媒体取得与所述特殊重放数据对应的特殊重放数据用密钥信息，

所述译码处理部用所述特殊重放数据用密钥信息进行译码。

内容重放装置、记录装置、记录重放装置及重放方法

技术领域

[0001] 本发明涉及在利用具有高著作权保护功能（安全强度）的可移动内容存储媒体时进行内容记录、重放的装置和方法。

背景技术

[0002] 近年在数字广播中，基于著作权保护的考虑，对内容附加「仅可复制一次」这样的限制信号进行加密，然后再提供。因此，在数字广播适用的记录装置中，将内容单独地加密后存储到硬盘驱动器 (HDD) 等的存储媒体中，以避免内容因非法利用或人为过失而流出。另外，在将记录在 HDD 中的内容写入 DVD 或蓝光光盘（注册商标）等媒体时遵守「仅可复制一次」所确定的规则，将 HDD 中记录的内容删除（移出功能）。

[0003] 但是，由于将内容存入硬盘时是独自加密，使得移动硬盘不能被使用，或者即使可用，也不能让其他设备使用，因此存在给使用者带来不便的问题。正是基于这样的背景，出现了搭载有著作权保护功能的移动硬盘「i VDR Secure」(注册商标)。i VDR Secure 可实现内容的著作权保护功能，其中包括 :根据著作权保护技术即 SAFIA(Security Architecture For Intelligent Attachment device)，包含加密内容数据及其译码密钥的密钥信息即 Usage Pass 的独立管理功能 ;以及保护所存储的 Usage Pass 不被非法访问的功能 ;以及具有 PKI(Public Key Infrastructure) 库的双方向认证的 Usage Pass 转送功能。而且，用该内容著作保护功能确定以音乐内容为对象的音乐播放器和以视频内容为对象的视频播放器中的规格。在视频播放器的情况下，将视频流分割的连续的 3072 字节的逻辑块被称为对准单位 (AU(Aligned Unit))，用该对准单位进行加密。另外，将连续的 512 个 AU 汇总的逻辑块被称为配置单位 (ALU(Allocation Unit))，该单位是用一个 Usage Pass 加密的最小单位。实现内容移出功能时，考虑到允许内容重复的时间为 1 分以下，在 SAFIA 中需用 1 分以下来更改 Usage Pass。（例如，参见专利文献 1（特开 2007-95204 号公报）、非专利文献 1(Recording and Playback Device for iVDR-TVRecording specification

[0004] (http://www.safia-lb.com/doc/spec/SAFIA_RPD_TV_V120_20080221.pdf))。

[0005] 如此，在将依据 SAFIA 的 i VDR Secure 用作存储媒体的记录装置中，在重放 i VDR Secure 中存储的内容时，在记录装置本体和 i VDRSecure 之间相互认证，用记录装置本体和 i VDR Secure 之间的 UsagePass 转送协议建立加密通信路径，安全地读出 Usage Pass，并将另行读出的加密内容用存放在 Usage Pass 内的加密密钥译码，将经译码的数据交给解码器来实现普通重放。但是，记录装置本体和 i VDR Secure 中，由于使用处理性能不是充分高的机内系统的 CPU，因此可能需花费大量时间将 Usage Pass 安全地读出，这时，在普通重放中存在因 Usage Pass 的读出时间来不及而造成乱画面的可能性。另外，在多个供货商提供 i VDR Secure 的情况下，存在将 Usage Pass 安全读出所需的时间在各供货商之间不尽相同的可能性。进行快进快退的特殊重放时，需要以对应于倍速的速度将 Usage Pass 和内容读出。与数字广播对应的内容被称为 MPEG2 TS，进行特殊重放时，至少在 1 分钟内显示称为 I 帧的多个 (n) 帧，而且需要每隔某个时间摘录显示的帧（若为 X 倍速，则按 y/n 在 x

分时间内选择 y 帧，以在 1 分后显示 X 分后的帧）。这需要与读出不到 1 分就变化的 Usage Pass 并行进行，若读出 UsagePass 花费的时间多，实现特殊重放就会有困难。

[0006] 在采用 SAFAIA 这样的著作权保护功能的装置中，用以从存储媒体安全地读出密钥信息的处理由存储媒体中内置的 CPU 执行，因此，在密钥信息的取得需要时间的情况下，译码不能赶上内容显示，重放的图像时而中断。例如，若取得时间为 1 秒左右，普通重放时没有问题，但对于内容而言译码所需的密钥信息不是一个，而是以某个间隔更改的，因此在特殊重放时，需要取得与存有选择的 I 帧的内容的位置对应的密钥信息来进行译码。因而，若要取得与内容取得时重放的内容对应的密钥信息，该取得处理会需要时间，就会有跟不上内容显示而不能进行平滑的重放或特殊重放的问题。

发明内容

[0007] 为了解决上述课题，将特殊重放时利用的数据作为另一文件保存，在特殊重放时用该数据来实现重放处理。该 TrickPlay 信息在 iVDR Secure 内加密存储，以保护权利人的内容。这样通过另行保存特殊重放用数据，即使在加密密钥信息以某个间隔更改的情况下，与普通重放时的重放时间相比，也能够将更大范围的数据与一个加密密钥相对应。

[0008] 或者，为了解决上述课题，通过将 TrickPlay 数据用密钥信息和普通重放用密钥信息相关联来消除加密密钥取得时间。

[0009] 本发明能够在密钥信息以某个间隔更改的加密内容的重放时和快进 / 快退这样的特殊重放中，进行平滑重放和特殊重放。

[0010] 通过参照附图的如下描述，本发明的这些及其他特征、目的和优点将变得更加明显。

附图说明

[0011] 图 1 是本发明一实施例的硬件 / 软件结构图。

[0012] 图 2 概略表示本发明一实施例的录像处理 (1)。

[0013] 图 3 概略表示本发明一实施例的录像处理 (2)。

[0014] 图 4 概略表示本发明一实施例的录像处理 (3)。

[0015] 图 5 表示与本发明一实施例的内容数据和特殊重放数据对应的密钥信息。

[0016] 图 6 是本发明一实施例的内容数据和特殊重放数据之间的关联图。

[0017] 图 7 概略表示本发明一实施例的重放处理。

[0018] 图 8 表示本发明一实施例的 n 倍速显示方法。

[0019] 图 9 表示本发明一实施例的速度过渡时的画面显示方法 (1)。

[0020] 图 10 表示本发明一实施例的速度过渡时的画面显示方法 (2)。

[0021] 图 11 表示本发明一实施例的速度过渡时的画面显示方法 (3)。

[0022] 图 12 表示本发明一实施例的速度过渡时的画面显示和声音提供方法。

[0023] 图 13 表示本发明一实施例的内容用密钥信息和特殊重放用密钥信息之间的相关联。

[0024] 图 14 表示一例本发明一实施例的加密密钥生成规则。

[0025] 图 15 表示一例与本发明一实施例的加密密钥相对应的方法。

具体实施方式

[0026] 以下，用附图说明本发明的实施例。再有，本实施例中，描述作为以某个间隔更改密钥信息的内容保护方法利用 SAFIA 的情况，如果是采用同样的内容保护技术，则本发明不受 SAFIA 的限定。

[0027] 【实施例 1】

[0028] 图 1 表示与实现本发明的一实施例中的具有著作权保护功能的移动硬盘（例如 i VDR Secure）对应的记录装置的硬件结构和软件结构。记录装置可内置于电视机中，也可内置于 PC 和 DVD 录像机中，因此，在以下的实施例中，将基于 i VDR Secure 的记录装置作为信息处理装置描述。另外，将记录、保存内容的移动硬盘（i VDR Secure）和普通硬盘作为信息记录装置描述。

[0029] 信息处理装置 100 中，作为软件设有：读出加密内容的内容数据取得部 510；将内容译码的译码处理部 520；取得密钥信息后暂时保存、利用的密钥信息取得部 540；为保持高安全性而在信息处理装置 100 和信息记录装置 300、310 之间进行认证的认证处理部 530；受理来自用户的请求的操作处理部 500；将内容数据实际输出到解码器等的输出装置 140 的内容输出处理部 550；生成密钥信息的密钥信息生成部；以及将内容记录到记录装置 300、310 的内容数据记录处理部，作为硬件（除了执行软件处理的 CPU130 之外）设有：取得录像用信息的调谐器 120；将取得并记录的数据作为图像信号、声音信号输出的解码器 140；将解码器输出的图像信号、声音信号实际播放的扬声器和与电视机的面板部分相当的显示部 150；用以与作为信息记录装置的 HDD 等连接的记录装置连接部 160；辅助加密、译码处理的加密处理部 170；以及受理来自用户的操作的遥控器接收部 180 等。本实施例的信息处理装置设有显示部，与电视机成为一体，但是，也可将电视机作为独立单元，这种情况下，取代显示部 550 而设有将图像信号、声音信号输出到装置外部的外部输出部（未图示）。

[0030] 另外，信息记录装置 300 和 310 具有同样的结构，该结构大体可分为控制部、数据存放部、防篡改区等三部分。控制部是控制信息记录装置 300 和 310 的部分，在进行数据交换的通信部 610 和 I VDR Secure 这样的实现高安全等级的装置中设有认证处理部 600。记录的信息有：保存在数据存放部中的加密的内容数据 700；收存有与该内容关联的信息的内容说明信息 720；表现内容和时间的对应关系的内容⇔时间信息 730；以及取得为了将内容译码所需的密钥信息时使用的内容⇔密钥信息 710。另外还有：快进、快退等的 TrickPlay（称为特殊重放）时使用的特殊重放数据 740；记载与该特殊重放数据和内容之间的对应关系的内容⇔特殊重放数据信息 750；以及取得在特殊重放加密时使用的密钥的特殊重放数据⇔密钥信息 760。再有，密钥信息 800 也存放在信息记录装置 300、310 内，由于密钥信息是重要且不应容易取得并更改的信息，因此存放在防篡改区。即使在普通的 HDD 不设这样的防篡改区的情况下，若有免费复制的等不需要加密的内容和进行单独加密的内容，也可能会存在不理会密钥信息等而在数据存储区域保存并使用。

[0031] 这里，例如是 i VDR Secure，作为密钥信息的 Usage Pass 存放在信息记录装置中的防篡改区，相当于图 1 的密钥信息 800。另外，防篡改区不能简单地访问，为进入该区域取出密钥信息，需要在信息处理装置 100 和信息记录装置 300 或 310 之间认证，在确保了安全的通信路径后才能进行数据交换。通过这样的方式，存储内容的安全性得到了提高。

[0032] 另外，作为在信息处理装置 100 和信息记录装置 300 之间使用的通信部，在 i VDR Secure 这样的硬盘驱动器中一般使用 ATA 接口和 SCSI 接口，并无特别的限定，今后也会考虑利用红外通信和有线 / 无线 LAN 或蓝牙（注册商标）等网络。

[0033] 若内容未被加密，则从信息记录装置 300 或 310 读出，并将内容数据传送给显示部 150，从而实现内容的重放处理。若是加密后存放的内容，则取得该内容和与内容的位置对应的密钥信息，一边用该密钥将内容译码一边将译码后的内容数据送到输出装置。

[0034] 在 i VDR Secure 中使用的 SAFIA 电视录像规格中规定，最长 1 分时间内必须更改 Usage Pass。需要将内容和与其重放位置对应的特定的密钥信息读出，并用该密钥信息将内容译码。即，SAFIA 中作为密钥信息的 Usage Pass 必须经多个 ALU 逐个更改来确定。该多个 ALU 是不到 1 分钟的重放图像部分的内容。另外，为了将 Usage Pass 从 i VDRSecure 读出，在信息处理装置和信息记录装置之间将 Usage Pass 加密后进行交换。但是，若使用信息记录装置和信息处理装置中搭载的内部 CPU，则由于信息记录装置中的加密处理和信息处理装置中的译码处理需要时间，且在必要时取得对应于内容的密钥信息，会有跟不上实际的重放处理动作的情况。

[0035] 而且，图像内容中与「某个时间间隔」相当的内容量，在重放时间上长期地看是一定的，但构成内容的图像帧，如果是 MPEG 等现行的主流动画形式，则由「I 帧」「P 帧」「B 帧」的 3 种数据构成。I 帧的长度比 P 或 B 帧大得多。从而，I 帧重放时读出的内容量突然提高。另外，I 帧并不具有一定的大小。因而，i VDR Secure 中，不能指定用一个 Usage Pass 加密的 I 帧的个数。

[0036] 考虑这些制约因素，将特殊重放用数据与内容数据分开提供。这些数据是特殊重放数据 740、内容⇔特殊重放数据信息 750 和特殊重放数据⇔密钥信息 760。除了与对应于该特殊重放用数据的内容相关联之外，与普通的内容数据同样地处理、加密并保存。作为特殊重放数据，例如可以是仅将包含 MPEG2 数据的 I 帧抽出的重放数据。为了将该数据存放在 i VDR Secure 中，特殊重放用数据也按 SAFIA 规格存放。不过，将该数据照原样输入解码器时的重放时间，能够以比普通内容短的时间重放，因此，相对于普通重放时的内容位置而言，加密密钥的有效范围在多倍的时间长度上有效。因此，即使密钥信息的取得稍有延迟，也能在需要时用另行准备的特殊重放数据提供成为显示对象的数据，顺利进行特殊重放。

[0037] 以下，就使用 i VDR Secure 时准备了特殊重放用数据的情况进行说明，对于具有著作权保护功能的信息记录装置，在一个内容中密钥信息被多次更改且其取得需要时间的情况下，本处理是适用的。

[0038] 图 2、图 3、图 4 表示本方式中的录像时的处理。根据图示的处理，将内容和特殊重放用数据加密后存入 i VDR Secure。图 2 主要说明内容的加密处理。

[0039] 首先，通过用户的遥控器操作和预先设定的录像请求的预约，系统开始录像处理。从录像处理开始后一直到用户请求录像停止或经过预定的时间录像结束的期间，在录像信息处理部中连续地接收要记录的内容数据。停止时，接受录像停止请求并进行通知（步骤 S1000）。取得了内容数据 1000 后，进行内容的加密处理。如果内容是免费复制内容这样的无需加密的内容，就将取得的内容直接存入 i VDR Secure（步骤 S2300）。用地面波数字等方式广播的内容需要普通加密处理，因此，在作了加密处理后进行记录。此时，如果已有加

密所需的密钥信息，就用该密钥进行内容的加密（步骤S2100），并记录经加密的内容（步骤S2300）。但是，如果加密密钥不存在或正处在密钥的更新定时，则密钥信息生成部560重新生成加密所需的密钥信息（步骤S2000），然后用该信息对内容进行加密（步骤S2100），之后，内容数据记录处理部570在记录装置300、310上进行记录（步骤S2300）。另外，如果更新了加密密钥信息，就将该信息记录在i VDR Secure中（步骤S2200），重放时将该密钥信息取出加以利用。通过这一系列流程，能够每隔某个设定的期间更新加密密钥信息，同时记录内容。

[0040] 在内容数据记录时，一边记录内容一边生成并记录其他的必要信息（步骤S3000）。用图3对此进行说明。将内容数据1000作为输入，分别生成并记录内容说明信息720、内容⇔时间信息730和特殊重放所需的数据（步骤S3100、步骤S3200、步骤S3500、步骤S3600、步骤S4000）。再有，在SAFIA规格中，内容说明信息720的Program Info，内容⇔时间信息730的Access Unit Info和Alloc Unit Info与这些信息相当。

[0041] 特殊重放用数据的做成处理如图4所示。再有，图4的一系列处理是步骤S4000的具体化。将内容数据作为输入取得，并将特殊重放用数据抽出（步骤S4100）。在内容数据为MPEG2数据时，例如I帧的信息与该数据相当。此外，若有特殊重放所需的数据，则取得该信息。在不需要对内容数据加密时，该特殊重放用数据也可不加密地进行记录（步骤S4600）。广播内容中，许多情况下该数据也加密并存储，但这也与内容时相同，若有加密密钥就用它对数据进行加密（步骤S4300），并将数据存储（步骤S4600）。若加密密钥不存在，或正处在切换定时，则生成加密用密钥信息（步骤S4200），用该信息进行数据的加密和记录（步骤S4300、S4600）。另外，将做成的加密密钥信息存到i VDR Secure的防篡改区（步骤S4500），再做成作为加密密钥信息和特殊重放用数据之间的关联信息的特殊重放数据⇔密钥信息760并加以记录（步骤S4400）。

[0042] 而且，在生成特殊重放数据的同时做成并记录内容⇔特殊重放数据信息750（步骤S4700）。实际上在进行特殊重放时，用该信息取得内容重放位置和特殊重放数据之间的对应关系，将数据提供给解码器。

[0043] 这里，就特殊重放用数据可相对于内容实现多倍密度的情况进行说明。特殊重放用数据的显示速度因解码器的性能而异。假设解码器的性能是f（帧/秒），则显示一个I帧所要的时间为1/f（秒）。假设在作为对象的MPEG2流中每Di（秒）插入I帧，通过在普通重放时以Di秒期间显示一个I帧，可实现与普通重放同等的显示速度（但是，由于只显示I帧，不能显示出动画效果）。因此，每一个I帧的显示时间为普通重放时的1/(Di×f)（再有，解码器必须满足1/f＜Di。若不满足，则不能进行普通重放）。如此，通过另行做成特殊重放专用数据(Trick Play Data)，能够根据SAFIA规格，与普通重放时间相比，用一个加密密钥对应Di×f倍的数据。图5对以上描述作了图示。在记录装置从广播等得到的内容数据3000中，存储有I10、I20、…I110、…等多个I帧的信息。根据SAFIA规格，不到1分钟就需要更改加密密钥。图5中，在分别用加密密钥$K_1$1500和加密密钥$K_2$1600将内容加密后，将最初的加密密钥对应区间和下一个加密密钥对应区间存入i VDRSecure。此时，只将I10等的I帧的信息抽出，同时做成特殊重放用数据4000。如上说明，进行一个I帧显示所要的时间可为1/(Di×f)（秒）的时间。从而，对于特殊重放用数据的加密密钥$K_trick_1$2000的对应区间，如图5所示，与普通重放相比，能够使时间上更宽的范围对应于一

个加密密钥。

[0044] 如以上所述，通过另行准备特殊重放用数据，能够使 1 个加密密钥对应于比普通重放时大的时间范围。因此，能够用比内容数据少的加密密钥取得多的特殊重放用数据。

[0045] 另外，重放时需要根据内容数据的位置指定对应的特殊重放用数据的位置进行数据读出。表现该对应关系的信息是内容数据⇔特殊重放数据信息 750，在录像处理的步骤 S4700 中生成。步骤 S4700 中生成的内容数据、特殊重放信息 750 的详细说明如图 6 所示。表 5000 详细表示了内容数据⇔特殊重放信息 750，表中相关联地记录了内容数据中的 I 帧的开始位置信息和到下一位置信息的长度，以及特殊重放数据中对应的 I 帧的开始位置信息和该 I 帧自身的长度信息。图 6 的上部给出该表的图示。内容数据 3000 中的 I 帧 I200、I210 对应于特殊重放数据 4000 中的 I300、I310，I200 和 I300、I210 和 I310 是同样的数据，只是存储位置不同。该图中，根据 I200 的内容前端的位置信息对应于表 5000 左端的「start」，左起第 2 个「size」相当于从 I200 的前端到 I210 的长度。另外，从特殊重放数据的前端到 I300 的位置信息对应于表 5000 的「TrickData Point」的「start」，I300 自身的长度对应于表 5000 右端的「size」。这样，通过对应于内容数据中的 I 帧的信息和特殊重放数据之间的位置关系进行记录，能够在重放时一开始就立即取得对应的特殊重放数据。另外如图 6 所示，本实施例中，内容数据中的 I 帧的开始位置和到下一 I 帧的长度，以及特殊重放数据中的 I 帧的开始位置和 I 帧的长度作为表中的项目作了说明，但是，实际上也可分别记录 I 帧的开始位置和结束位置的信息，对于内容数据的 I 帧信息，可将 I 帧开始位置及该 I 帧的长度或 I 帧的结束位置存储等，并将存储的数据与各自的数据内的位置信息相关联。至于如何利用此信息，取决于特殊重放时进行怎样的处理。也就是说，图 6 的表 5000，即内容数据⇔特殊重放信息 750 的详细结构，设定为能够保持特殊重放时需要的充分信息的结构。

[0046] 通过以上的处理，录像时能够与内容数据平行地生成特殊重放数据。若以 SAFIA 规格为例，该特殊重放数据可以作为与内容数据关联的 Named Stream 保存，也可以作为别的内容保存（例如可采用这样的结构，若内容文件名为「PROG1234.AVS」，则能够以「TRIC1234.AVS」这样的文件名或其他信息立即取得各自内容的对应关系）。在作为别的内容保存时，若使得用 SAFIA 规格定义的文件结构得到保持，就能够以与普通内容同样的形式存入 i VDR Secure。

[0047] 以下说明：在存在以上数据的状态下进行重放，在特殊重放时所需的密钥取得时间不成问题。

[0048] 图 7 用活动图表示重放处理的流程。首先，用户通过操作遥控器等指定想要视听的内容（步骤 S11000）。重放对象的内容一被指定，其信息就被通知到系统的操作处理部 500(S11010)。接到该信息（步骤 S10000），信息存储装置 100 中的操作处理部 500 开始处理，进行重放准备。若对象内容被加密，则视听时需要有进行译码的加密密钥。因此，向内容数据取得处理部 510 传送内容的读出位置，同时向密钥信息取得部 540 指示：取得对应于读出位置的加密密钥信息（步骤 S10010）。之后，只要没有来自用户的请求，系统侧就继续进行重放处理（步骤 S10030）。同时系统侧继续受理用户操作 (S10020)。重放处理中，会有在重放对象内容的终端到达前以用户指示来通知进行重放处理更改的情况。具体而言，就是接受用户通过遥控器操作等作出的快进、快退、停止等的指示（步骤 S12000）。这种情

况下，根据被指示的内容向系统侧发送更改重放处理的指示（S12010）。也就是通知系统进行「普通重放（步骤 S10030）」、「使用特殊重放数据的特殊重放（步骤 S10040）」、停止等中的任一个处理。受理了处理的系统使状态转移，以进行按照该指示的处理，使状态迁移。再有，也有不用特殊重放数据来进行特殊重放的情况（例如，暂停、慢速、逐帧播放、比预定速度慢的重放速度的快进、快退等）。本实施例中，将这些处理视为普通重放，将比预定速度快的重放速度即快进和比预定速度快的反向重放速度即快退作为特殊重放。

[0049] 如此，通过用户指示进行从普通重放到特殊重放，或从特殊重放到普通重放的转移。在特殊重放时，若到达了内容的终端，则不等待用户指示就结束处理（步骤 S10040）。

[0050] 以下，就使用录像时做成的特殊重放数据的特殊重放进行说明。为了实现 n 倍速的快进、快退，若能将普通重放中显示的数据简单地以 1/n 的时间显示就可实现。但是现实情况是，由于图像数据量大，难以从重放对象的全部数据实时地取得 1/n 的数据。有这样的情况，若为 MPEG 数据，仅用 I 帧的信息，通过在每单位时间使各个 I 帧分散地播放来进行特殊重放。如果再以某个间隔更改加密密钥，就会在其加密密钥取得处理和暗译码处理上耗费时间，难以将 I 帧在实现特殊重放的间隔显示。因而，本方式中另行准备了特殊重放数据。

[0051] 具体而言，若某个图像内容中插入一个 I 帧的间隔为 Di（秒），则为了进行 n 倍的特殊重放，以 1/(n ×Di)（秒）显示一个 I 帧即可。但是，解码一个 I 帧的速度因实际使用的解码器而异。若解码器的处理能力为 1 秒间可解码 f 个 I 帧，则 I 帧显示间隔的最小值成为 1/f（秒）。因此，在 n 倍的特殊重放执行时中，

[0052] $1/(n \times Di) < 1/f$

[0053] 若成立，则将 I 帧的显示间隔设为 1/f（秒），同时以 1 秒期间不超过 f 个的方式从特殊重放数据中选择应显示的 I 帧，就能实现特殊重放。图 8 表示该状况。相反地，若上式不成立，则将 I 帧的显示间隔设为 1/(n×Di)（秒），显示全部的 I 帧即可。

[0054] 另外，由于本方式中的特殊重放数据也是加密后存储，为了进行译码需取得密钥信息。因而，作为本专利课题的「因密钥信息的取得和暗译码需要时间而处理失败」问题，在特殊重放数据取得时也会发生。然而，如本方式这样，通过将特殊重放数据与内容数据分开地做成并存储，特殊重放数据的加密单位（从普通重放时间上考虑）就能够成为以 SAFIA 规格限制的 1 分以上的单位进行加密（由于重放特殊重放数据时可用不到 1 分重放，并未超出 SAFIA 规格）。因此，预先取得并译码与特殊重放数据对应的密钥信息，用该信息作为「缓冲」，即使下一密钥的读入和译码处理需要时间，也能不使特殊重放失败地进行。重放开始是从内容用加密密钥和特殊重放用加密密钥双方均未被保持的状态开始的，在最初的图像被显示之前，至少需要内容用加密密钥的取得和译码处理的时间（另外还需要内容数据的取得、重放开始位置确定处理等的时间），但在重放开始后，通过在不妨碍内容重放的范围内预先取得特殊重放用加密密钥，可提供对于用户操作而言平滑的模式过渡。

[0055] 如此，在从重放过渡到特殊重放时，对应于普通重放中的内容数据，（接着）预先取得成为必要的特殊重放用密钥信息，在特殊重放中也可以通过预先取得密钥信息，使从重放向特殊重放的过渡平滑。另外，特殊重放也可以通过显示多个 I 帧来平滑地显示。但是相反地，在从特殊重放返回到普通重放时会出现问题。这是由于用户并不关注在何处从特殊重放向普通重放过渡，指定普通重放所需的加密密钥的定时是「来自用户的向普通重

放过渡的指示被受理之时」。若在该定时执行取得普通重放所需的加密密钥的处理，该取得处理需要时间，这是让用户感觉「响应性差」的要因。因而，以下就缓和用户不满的方法进行说明。

[0056] 图 9 表示从特殊重放向普通重放过渡的处理。如图所示，以 n 倍速在正向进行特殊重放时，设一个 I 帧的显示间隔为 Td，各 I 帧的信息按速度从特殊重放数据中选择（被选的帧是 I200、I210、I220）。这里，假设在 I 帧 I300 被显示时因用户操作而接到普通重放指示。此时，通过内容⇔特殊重放数据信息 750 取得与 I300 对应的内容位置，从该位置取得内容信息，同时取得、译码与该位置对应的密钥信息并提供数据，普通重放就可开始。但是，实际上该密钥取得处理需要时间。因而，显示了 I 帧 I300 后，在比密钥信息的取得和译码处理所需的时间更长的时间多余地显示 I 帧。但是，多余地显示的 I 帧以紧邻 I300 的帧中的多个为对象。另外，将接到普通重放过渡指示后的 I 帧的显示间隔从当初设定的间隔（本例中为 Td（秒））慢慢缩短。图 9 的例中，返回普通重放时显示的 I 帧的个数是 I300 之外还有 3 帧，设各显示间隔为 T_{t1}、T_{t2}、T_{t3}、T_{t4}，使各显示间隔满足下式。

[0057] $Td > T_{t1} > T_{t2} > T_{t3} > T_{t4}(\geq 1/f)$

[0058] 然后，普通重放的开始从比最后显示的 I 帧 I330 的另一个的相邻帧 I340 的前端位置起进行。如此，通过选择重放速度更改时的显示间隔和显示对象的 I 帧，在用户的眼中，从特殊重放向普通重放的过渡时一个图像的显示间隔慢慢地加快，该图像的变化看起来很平缓。也就是说，在观看感觉上可以给用户以追上重放速度更改的印象。通过将这样的数据提供给解码器来改变图像的显示间隔，与直到图像显示时都没有任何图像变化的情况相比，用户更容易认可，这可视为是没有太多不舒适感的容易接受的表现方法。另外，从特殊重放过渡到普通重放，本例中可在 $T_{t1}+T_{t2}+T_{t3}+T_{t4}$（秒）内实现。若此时间超过密钥信息取得处理所需的时间，就可能需要更改速度，以不使用户感到加密密钥取得时发生的延迟。

[0059] 但是，如果在原来的内容中的 I 帧的插入间隔为 Di（秒）时，每多个速度变化过渡时的显示用 I 帧的显示间隔不到 Di（秒），看起来会有过渡期间被慢速显示，在普通重放开始后才以普通速度显示的感觉。此时，尽管用户已作了「普通重放」的速度更改指示，但一旦「慢」下来后，再成为普通重放的速度，用户看起来就会有动作不正常的感觉。为了解决该问题，在速度低于 Di 时，将过渡时显示的 I 帧不是从紧邻的帧开始，可以空出某个左右间隔来进行显示，如图 10 所示。具体地，速度更改期间中显示 n 个 I 帧时，第 k 个帧中成为 Tk < Di 的情况下，将本应选择的第 k+1 个 I 帧跳过下式表示的 n_j 个 I 帧来选择。

[0060] $n_j \geq (Di/Tk)-1$

[0061] 在之后的 I 帧选择中，若满足了上式，就不会有用户看起来「慢」的现象发生。再有，如此在速度过渡时选择 I 帧的情况下，选择的 I 帧之间的间隔与 T_{t1}、T_{t2}、T_{t3}、T_{t4}、... 的间隔相一致地选择，能够进行使用户更无不舒适感的显示。图 10 的例中，按照 I300 和 I310 之间空开 4 个 I 帧、I310 和 I320 之间空开 2 个 I 帧、I320 和 I330 之间及 I330 和 I340 之间空开 1 个 I 帧的方式选择。

[0062] 图 9、图 10 是对于 Td（秒）大的情况的图示。实际上 Td 可取最小值 1/f（秒）。这种情况下，不可能通过硬件来设定更小的 T_{t1} 等比 Td 小的值。另外，在 Td 取最小值的情况下，图像的显示间隔非常短，用户所看到的图像极速变化，会给人闪烁的印象。在这种情况下，就不是如以上说明的将时间间隔缩短，而是将 T_{t1} 等的值慢慢增大，如图 11 所示。另外，

此时满足下式。

[0063] $Td(=1/f) < T_{t1} < T_{t2} < T_{t3} < T_{t4}(\leqslant Di)$

[0064] 如此，通过改变显示速度，使图像的显示速度和图像的变化间隔这二者都显得平缓。这也可以给用户以追赶重放速度更改的印象。普通重放用加密密钥取得和译码所需的时间也与图9的情况相同。图9、图10和图11给予用户相同的效果，只是由于相对时间不同而在表现上有差别。再有，即使在图11的情况下，速度过渡期间显示间隔一旦超出Di(秒)，也会形成给用户带来不舒适感的显示。为此，即使在将显示间隔延长的情况下，也可以不是如图10所示那样从与接到指示时显示的I帧的紧邻的帧开始进行处理，而是使普通重放从稍前的I帧开始进行。或者，可以调节I帧的选择个数和显示时间，以不超出Di。

[0065] 以上，用图9、图10、图11说明了通过更改I帧的显示间隔，使用户不从观看感觉上意识到普通重放过渡时的加密密钥取得和译码所需时间的构成。图中用正向进行说明，反向的特殊重放也同样可以实现。在这些例中，通过在图像显示方法上作改动来缓和用户对于所发生的等待时间的感觉，但是，也可以通过声音来实现。具体而言，录像时不只是记录I帧来做成特殊重放数据，还将到下一I帧为止的声音数据一并记录。在从特殊重放向重放过渡时利用该数据，从普通重放开始位置稍前的声音开始输出。图11给出了其图示。声音数据S320、S330分别是与I帧I320、I330对应的声音数据。这样，不仅提供图像数据而且同时提供声音数据，虽然在过渡期间会有图像和声音的失配发生，但由于能够在重放指示后立即利用声音数据，能够实现使用户更有舒适感的过渡。另外，如果难以提供如图9、图10、图11说明的图像数据，也可将显示的I帧图像固定为一个，先提供声音。这样，可以通过让声音先到达来减轻用户的不舒适感。

[0066] 再有，进行多余的图像数据的显示和声音数据的提供时，具体显示的I帧个数设为多少、过渡期之间的显示间隔设成如何等，需要另行调节到令用户容易接受。至于区分图9、图10和图11的显示间隔，需要根据用户容易接受的显示间隔加以定义。

[0067] 【实施例2】

[0068] 上述的图像数据显示方法和声音数据输出方法是不让用户意识到加密密钥信息取得或译码处理延迟的方法。可以认为，无论用那种方法均能够使重放速度的更改在用户看起来没有不舒适感地被接受，但是，总是得容许重放速度更改时发生的延迟时间。因而，以下就不受加密密钥取得时间的影响的方法进行说明。由于i VDR Secure中的处理延迟原因在于加密密钥取得处理，利用本方式能够立即处理重放速度更改。

[0069] 图13是表示缩短加密密钥取得处理时间的构成图。如图所示，假设以内容⇔密钥信息710为例有密钥K1000，以特殊重放数据⇔密钥信息750为例有密钥K2000。这里，为了迅速进行从特殊重放向普通重放的过渡，将K2000和K1000相关联。如前面所说明，若以重放时间衡量，与普通重放数据相比特殊重放数据可用一个加密密钥应对几倍的数据。若设该倍数为n，特殊重放用密钥信息表现的范围也相当于n份普通重放用密钥信息的数据。严格地说，由于SAFIA规格需要以ALU单位来保存数据，因此根据特殊重放数据的量多少有些变动。以下的说明中考虑这种可能性：对于1个特殊重放用加密密钥生成用来成为n个普通重放用加密密钥的加密密钥数据。

[0070] 因此，如果具有从该1个特殊重放用加密密钥取得n个普通重放用加密密钥的构成，则从特殊重放向普通重放过渡时就能够即刻切换处理。也就是，如果设第i个普通重放

用加密密钥为 Key_i，第 α 个特殊重放用加密密钥为 $KeyT_\alpha$，普通重放用加密密钥有可能通过下式中 f 表现的关联，从特殊重放用加密密钥取得普通重放用加密密钥。

[0071] $Key_i = f(KeyT_\alpha)$

[0072] 当然，可期望上述的计算时间比加密密钥取得所需的时间短。另外，如果密钥信息的个数有限，则采取不用计算式而做成对应表来求出的方法也可以。至于具体用什么计算式来进行关联，可根据各供货商、各设备而变更。另外，可利用只在各供货商内部使用的数值或依赖于设备的序号等，使得其只能在特定置位使用，或者能够使密钥流出和算法被破解的风险降低，能够使加密的强度提高。若能够这样从特殊重放用加密密钥 K2000 关联到普通重放用加密密钥K199，就能用特殊重放的显示位置和内容⇔特殊重放数据信息750即刻取得普通重放所需的加密密钥，因此能够向用户提供能够无延迟地实现重放速度更改的系统。也就是，能够通过预先定义录像时（内容记录时）中使用的加密密钥的生成规则，消除重放时（内容利用时）发生的问题。

[0073] 再有，从普通重放向特殊重放的过渡需要另行取得特殊重放数据用加密密钥的时间，但是，普通重放时能够在不妨碍内容的重放的范围内预先取得密钥信息，因此，除了重放刚开始时，密钥信息能够经常处于可使用状态。因而，可以不进行从普通重放用加密密钥取得特殊重放用加密密钥的关联而无延迟地进行处理。当然，也可进行双向的关联来消除处理延迟。

[0074] 而且，若能从特殊重放用加密密钥算出普通重放用加密密钥，则能够不用特殊重放数据 740 进行特殊重放。这是因为，能够从一个特殊重放用加密密钥取得多个普通重放用加密密钥，因此从内容数据 700 只取出特殊重放所需的数据（具体而言即 I 帧的信息）就可进行处理。也就是说，在通常情况下，由于没有做成特殊重放用数据，必须取得内容数据特殊重放用数据。但是，为了将该数据译码，必须取得多个加密密钥信息，这时，因密钥取得处理需要时间而不能进行特殊重放。为了避免该问题，提出了另行做成特殊重放数据的方式。再将这一想法推进，如果将特殊重放用加密密钥和普通重放用加密密钥相关联，就能够一次取得多个密钥，没有特殊重放用数据也能利用内容数据进行特殊重放。这样，即使没有特殊重放数据 740、内容⇔特殊重放数据信息 750 和特殊重放数据⇔密钥信息 760 这 3 种信息，也能无延迟地进行特殊重放。图 14 表示该例，以下说明其流程。

[0075] 录像时，以如下的方式确定加密密钥的生成规则。

[0076] (1) 对于最初的密钥，或第 n+1 个密钥（图 13 中 n = 5），用随机数等将无关联性的数值用作加密密钥。

[0077] (2) 以后，到第 n 个密钥都通过将前面的密钥信息作为输入而求出密钥生成函数 F。例如，设第 i 个普通重放用加密密钥为 Key_i，将第 α 个特殊重放用加密密钥设为 $KeyT_\alpha$，将 [i/n] 设为不超过 n 的整数时，密钥生成函数可表达为下式。

[0078] $$Key_i = f(KeyT_{\left[\frac{i}{n}\right]}, i)$$

[0079] 通过定义这样的密钥生成函数 F，在重放时也能利用密钥生成函数 F 从一个加密密钥取得多个加密密钥。再有，本例中描述了将成为密钥的加密密钥以 n 个间隔更改的示例，但该间隔也可以是可变的。另外，在成为密钥的加密密钥以外，根据前一个加密密钥取得加密密钥，但是，也可利用「第几个密钥信息」的信息来生成、取得加密密钥。而且，可利

用各设备的序号等设备上固有的信息，在作了录像的设备上从一个加密密钥生成多个加密密钥，但不能在其他设备上使用而可分别从存储媒体取得加密密钥。根据以上所述，通过满足对于某特定位置的加密密钥是在其他加密密钥生成时被使用的信息、某生成规则可在某一定区间（该区间可为可变）中适用这两项满足的条件，内容密钥能够消除取得加密密钥所需的延迟时间。生成规则的算法和区间的长度等，可考虑各种各样的方式，仅由各安装者知道即可。即使不知道此规则，作为普通的 SAFIA 内容使用也没有问题。

[0080] 这样，通过制定内容密钥 710 的生成规则，能够开发基本无需意识到重放时加密密钥取得所需时间的系统。此外，上述的实施例中以在规格要求的范围更改密钥为前提作了描述，但是，如果能够用其他方法来保证安全的话（例如利用设备固有的序号，而通常又难以取得该信息），也可使用加密密钥完全相同或在一定区间相同的加密密钥。也就是说，只要能够满足要求的安全强度，可完全连续地使用加密密钥。

[0081] 【实施例 3】

[0082] 另外，在 SAFIA 中这是不可能实现的，因为其中记载：对规格上「连续的内容数据设定密钥信息」，但是，在 SAFIA 以外的实现「具有根据某时间或数据量更改加密密钥的构成的内容保护功能」的系统中，通过如图 15 所示的加密处理，可将密钥信息的取得、译码所需的时间造成的延迟推迟。以下说明图 15 的方法。首先，内容中存在进行特殊重放时使用的 I 帧的信息 I400、I410、...。作为对内容的加密单位，不是在内容的连续区域，而是分为「I 帧」和「I 帧以外部分」进行加密处理。图 14 中，加密密钥 Kn 成为对应于由 I400、I410、I420、I430 包围的 3 个区域的加密密钥。同样地，Kn+1 是对应于由 I430、I440、I450、I460 包围的 3 个区域的加密密钥，用该密钥进行加密。

[0083] 接着要说明的是，作为特征信息的 I 帧 I400、I410、I420、I430、I440、I450 用 Ktrick_n 的加密密钥加密并保存，I460 以后的若干 I 帧的信息用 Ktrick_n+1 的信息加密。即使以某一定间隔更改加密密钥，只用 I 帧重放时的重放时间不同，因此，与在一个加密密钥上进行的普通重放相比，能够与更多个数的 I 帧相对应。因而，能够用一个 I 帧用加密密钥对时间上更广范围的内容进行特殊重放。

[0084] 这样，可通过用另外的加密密钥只对内容内部的某个特征区域加密，另行准备密钥信息，通过增加内容、密钥信息的信息量，可不用保持特殊重放用数据地进行处理。

[0085] 尽管我们已经展示并描述了几个根据本发明的实施例，但应当明白，在不偏离本发明范围的条件下所公开的实施例允许变化和修改，因此，我们无意受到文中展示和描述的细节的约束，但有意将所有这些变化和修改涵盖在后附的权利要求范围内。

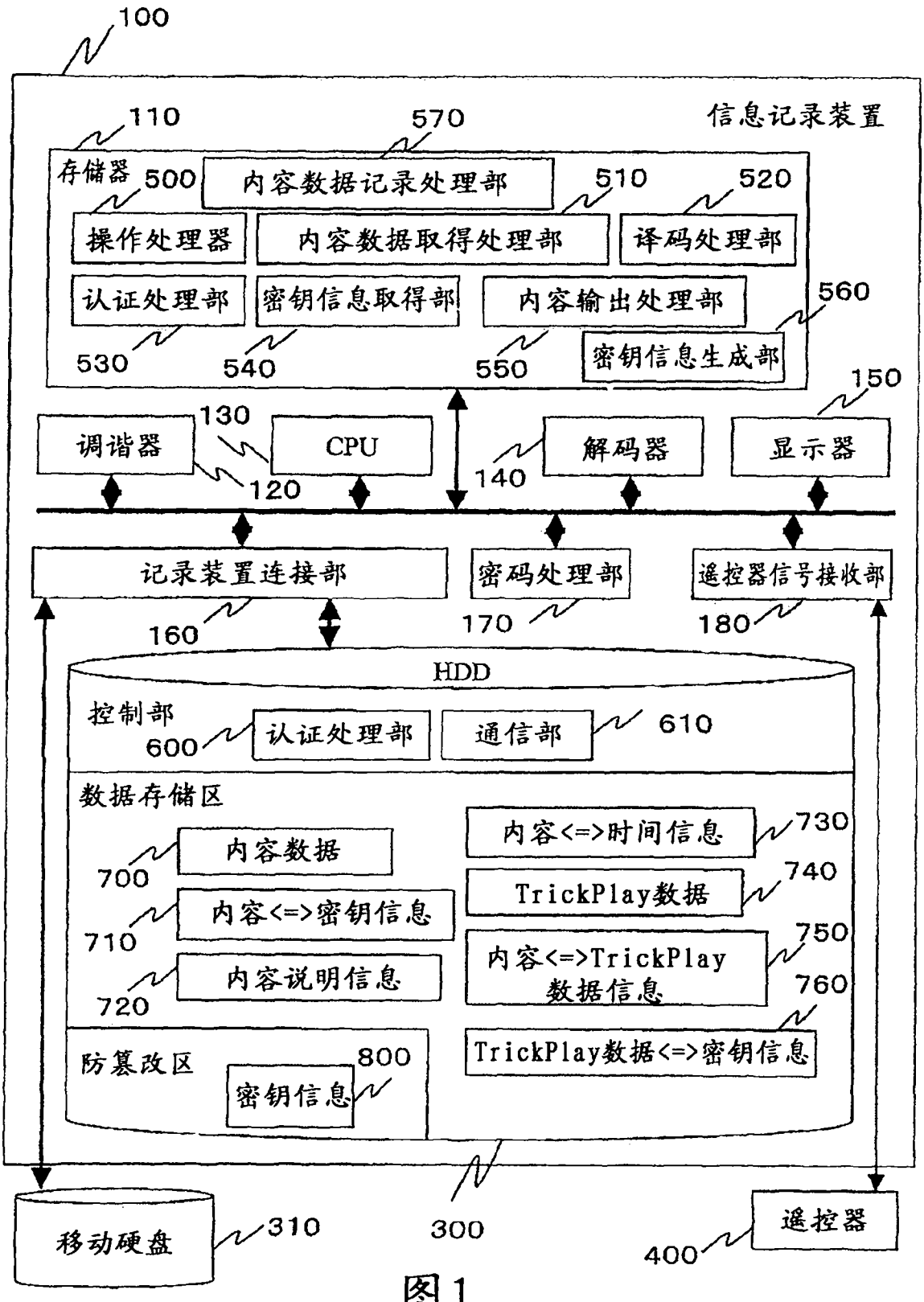

100
信息记录装置
110
570
存储器
500
内容数据记录处理部
510
520
操作处理器
内容数据取得处理部
译码处理部
认证处理部
密钥信息取得部
内容输出处理部
560
530
540
550
密钥信息生成部
150
调谐器
130
CPU
解码器
显示器
120
140
记录装置连接部
密码处理部
遥控器信号接收部
160
170
180
HDD
控制部
600
认证处理部
通信部
610
数据存储区
内容数据
700
730
内容<=>时间信息
740
TrickPlay数据
710
内容<=>密钥信息
750
内容<=>TrickPlay
数据信息
720
内容说明信息
760
TrickPlay数据<=>密钥信息
防篡改区
800
密钥信息
移动硬盘
310
300
遥控器
400

图1

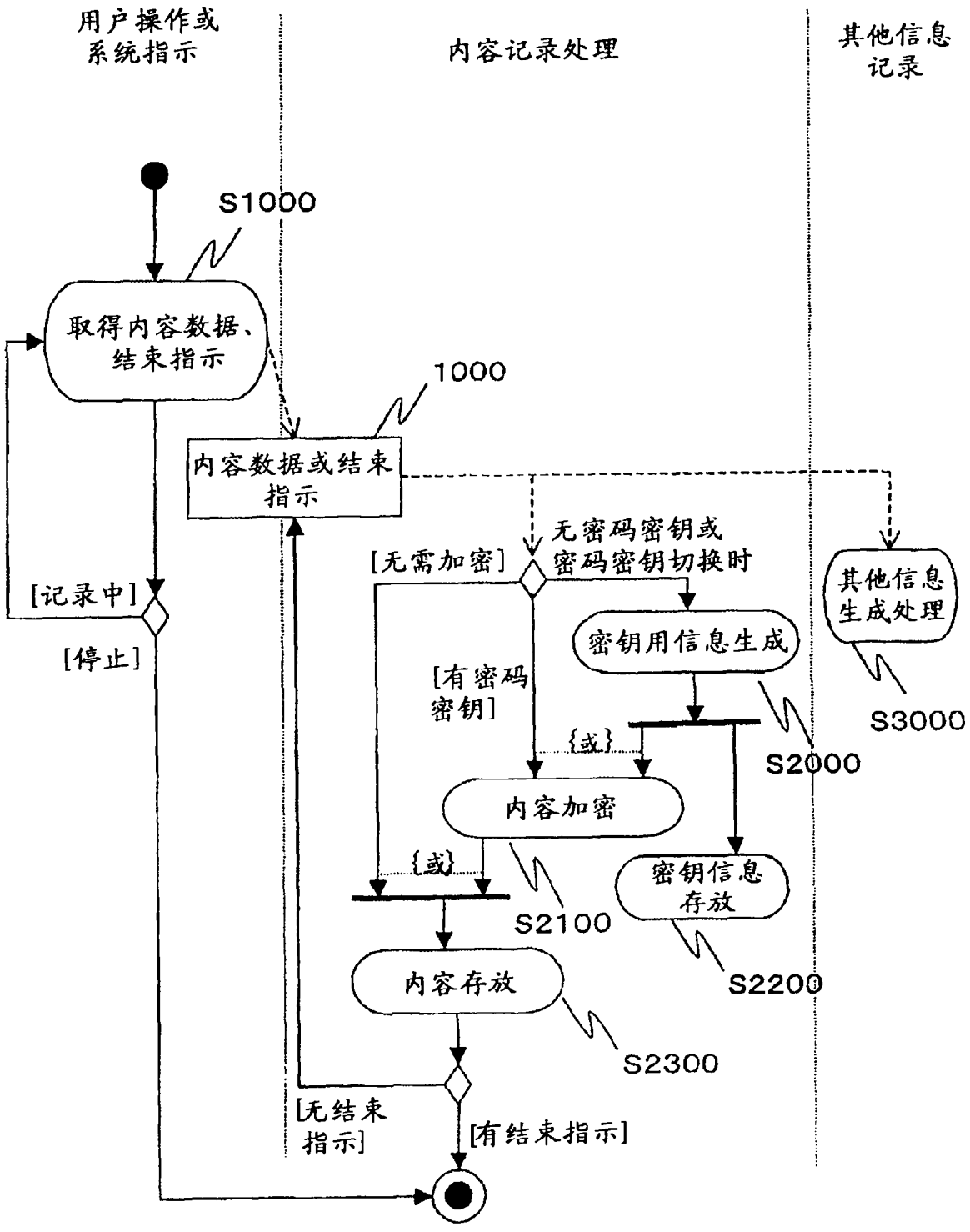

用户操作或
系统指示
内容记录处理
其他信息
记录
S1000
取得内容数据、
结束指示
1000
内容数据或结束
指示
无密码密钥或
密码密钥切换时
[无需加密]
其他信息
生成处理
[记录中]
[停止]
密钥用信息生成
[有密码
密钥]
S3000
{或}
S2000
内容加密
{或}
密钥信息
存放
S2100
S2200
内容存放
S2300
[无结束
指示]
[有结束指示]

图 2

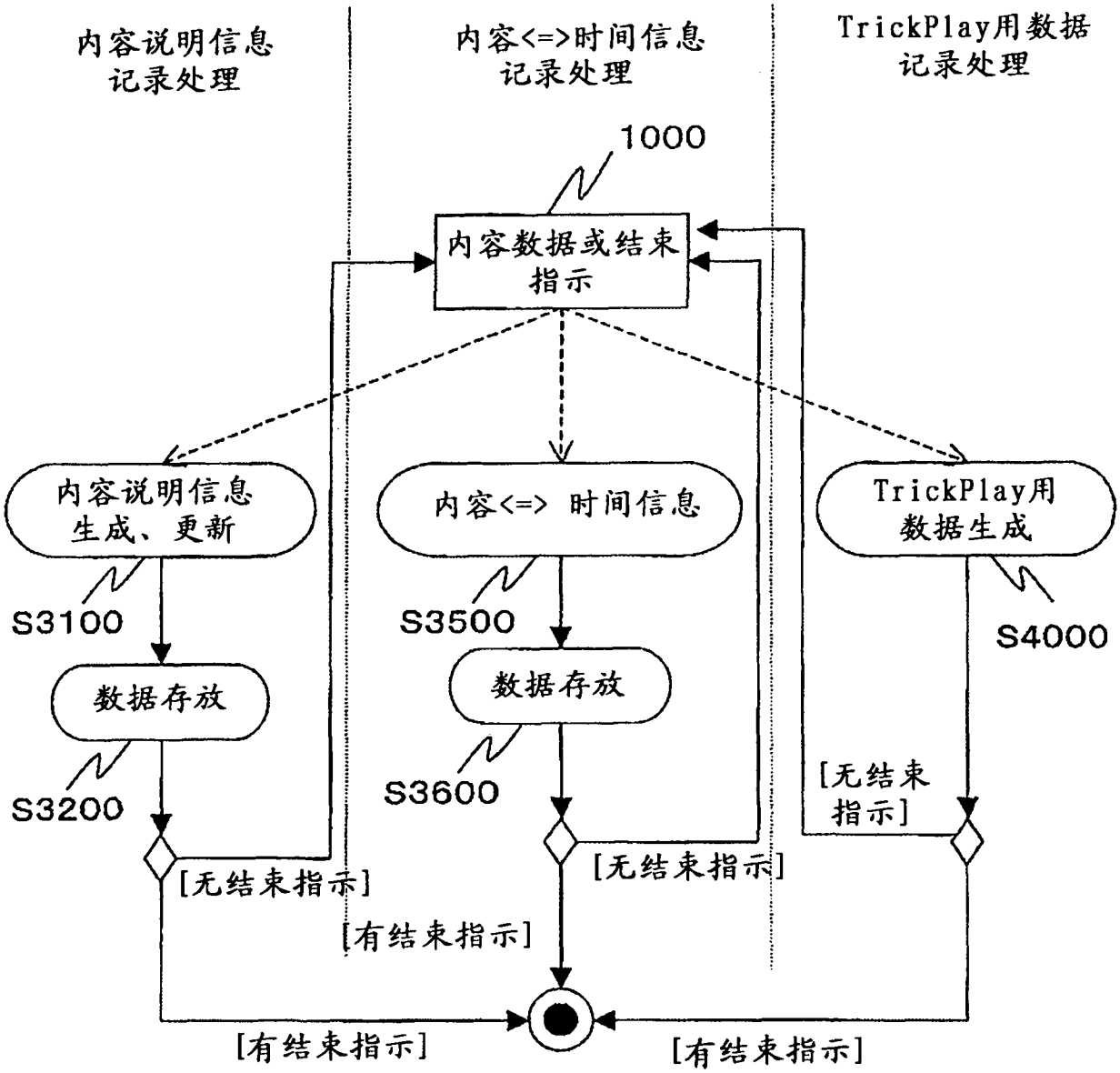

内容说明信息
记录处理
内容<=>时间信息
记录处理
TrickPlay用数据
记录处理
1000
内容数据或结束
指示
内容说明信息
生成、更新
内容<=> 时间信息
TrickPlay用
数据生成
S3100
S3500
S4000
数据存放
数据存放
S3200
S3600
[无结束指示]
[无结束指示]
[无结束指示]
[有结束指示]
[有结束指示]
[有结束指示]

图 3

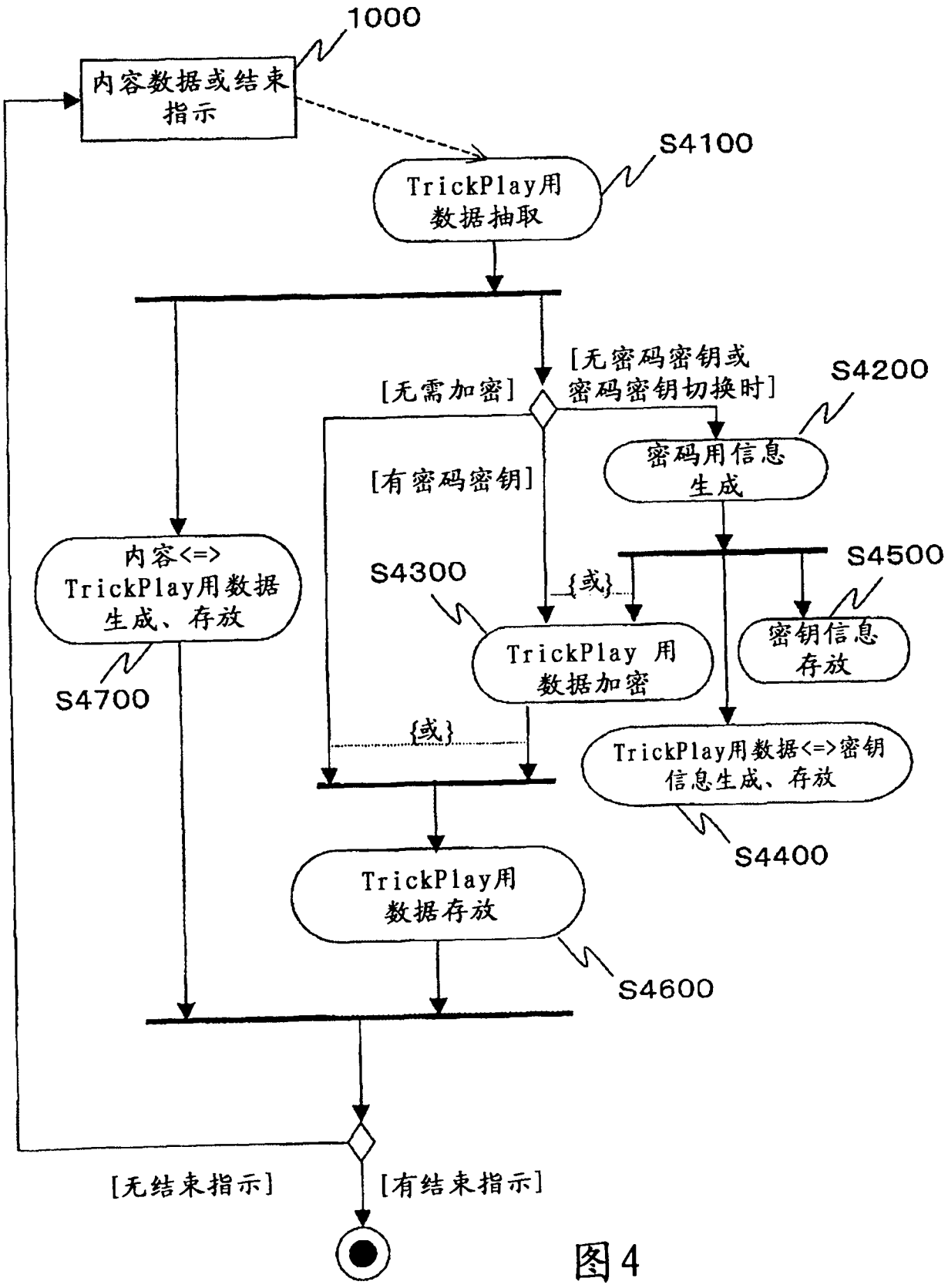

1000
内容数据或结束指示
S4100
TrickPlay用数据抽取
[无密码密钥或密码密钥切换时]
[无需加密]
S4200
密码用信息生成
[有密码密钥]
内容<=>TrickPlay用数据生成、存放
S4300
{或}
S4500
TrickPlay 用数据加密
密钥信息存放
S4700
{或}
TrickPlay用数据<=>密钥信息生成、存放
S4400
TrickPlay用数据存放
S4600
[无结束指示]
[有结束指示]

图4

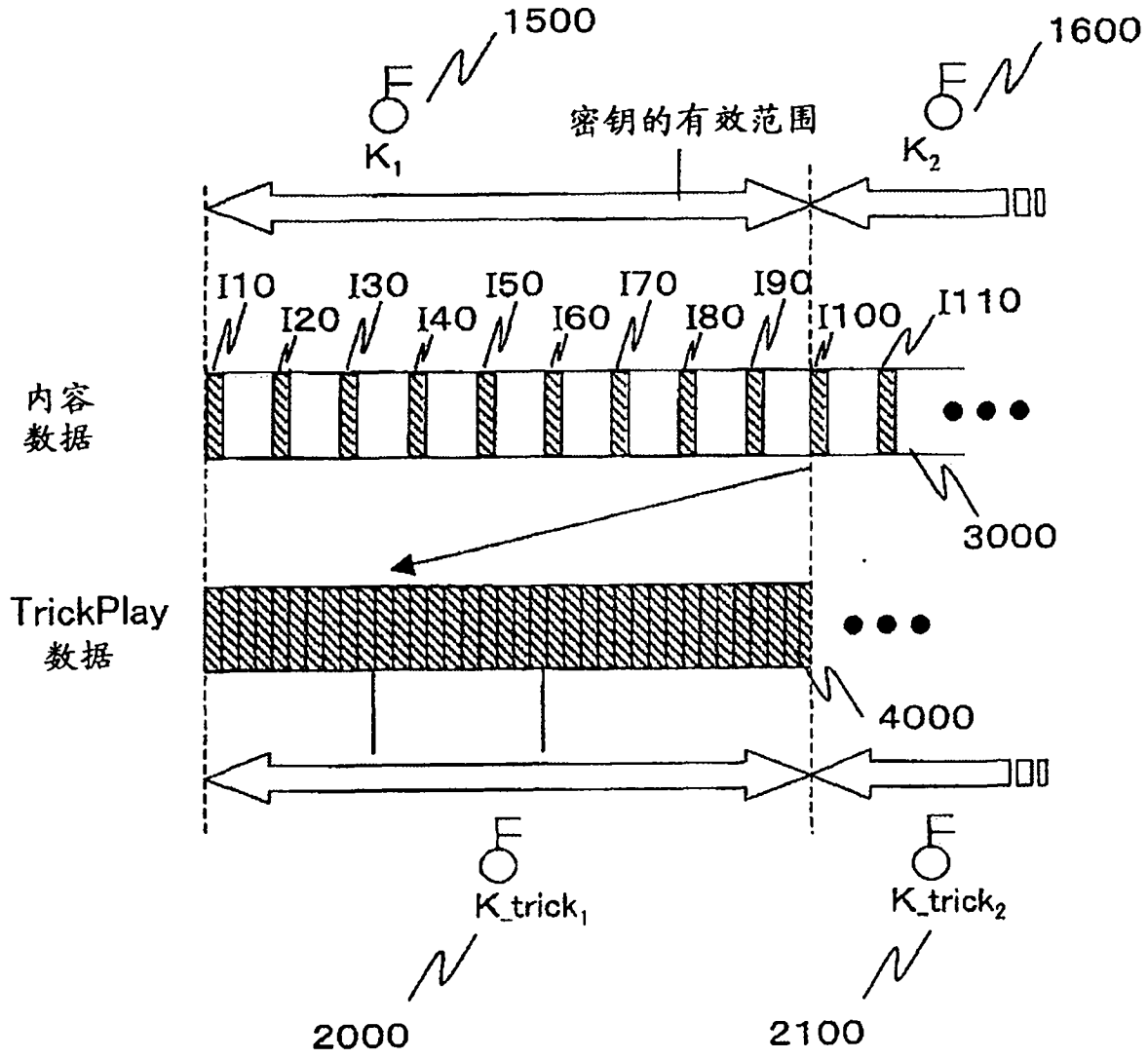
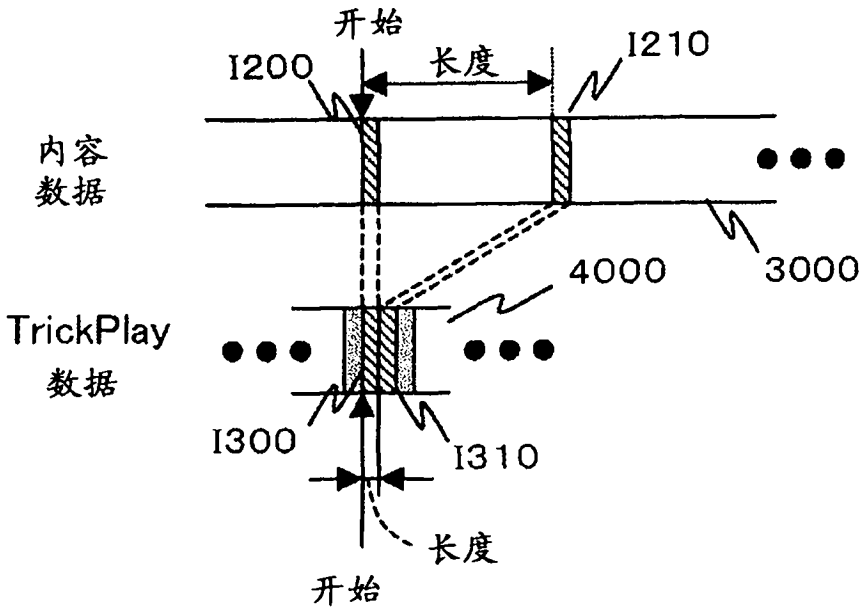

1500
1600
密钥的有效范围
K1
K2
I10
I20
I30
I40
I50
I60
I70
I80
I90
I100
I110
内容
数据
3000
TrickPlay
数据
4000
K_trick1
K_trick2
2000
2100

图 5



5000

内容点		TrickData数据点	
开始	长度	开始	长度

图 6

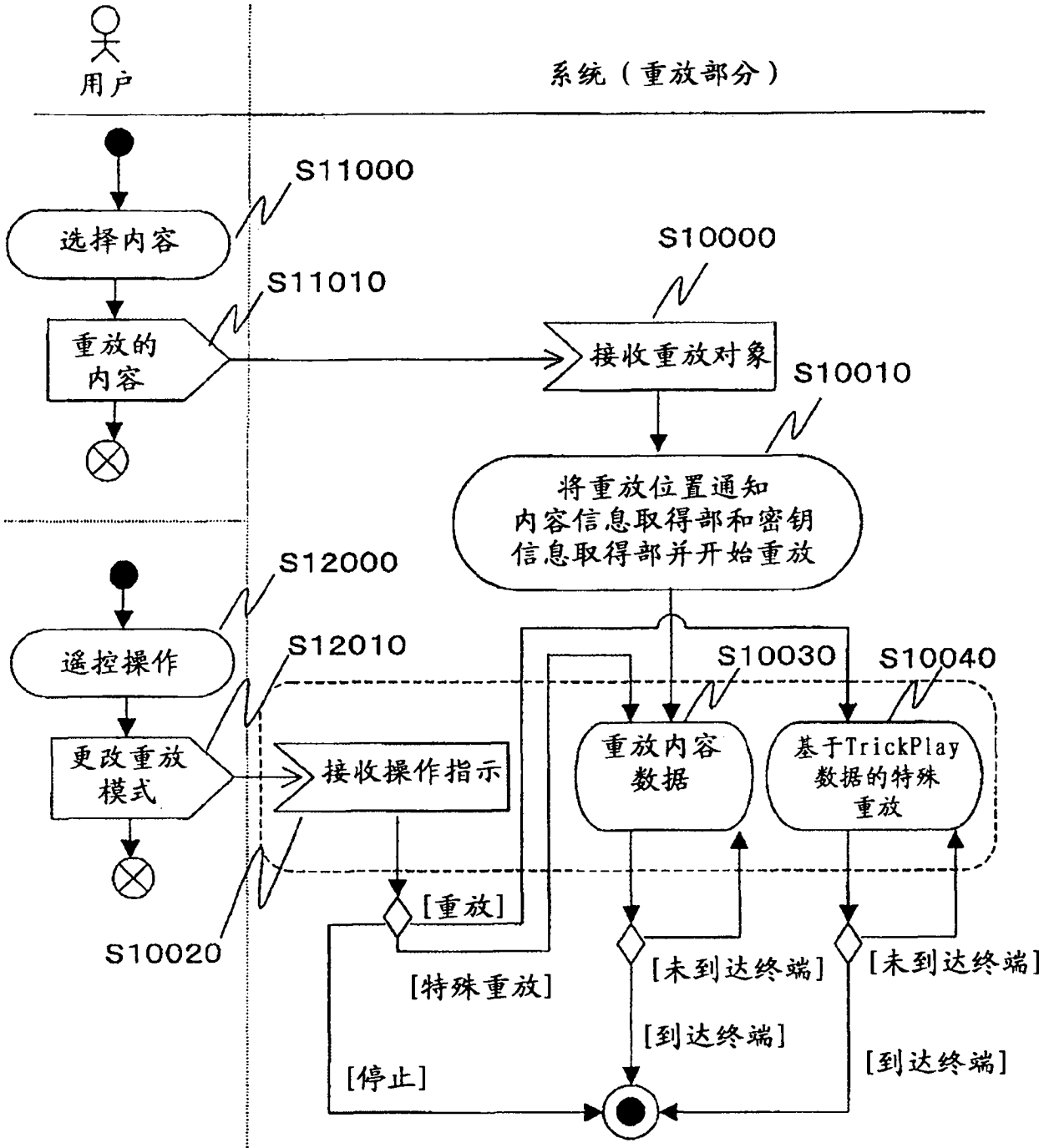

用户
系统（重放部分）
S11000
选择内容
S11010
重放的内容
S10000
接收重放对象
S10010
将重放位置通知内容信息取得部和密钥信息取得部并开始重放
S12000
遥控操作
S12010
更改重放模式
接收操作指示
S10020
S10030
重放内容数据
S10040
基于TrickPlay数据的特殊重放
[重放]
[特殊重放]
[停止]
[未到达终端]
[到达终端]
[未到达终端]
[到达终端]

图7

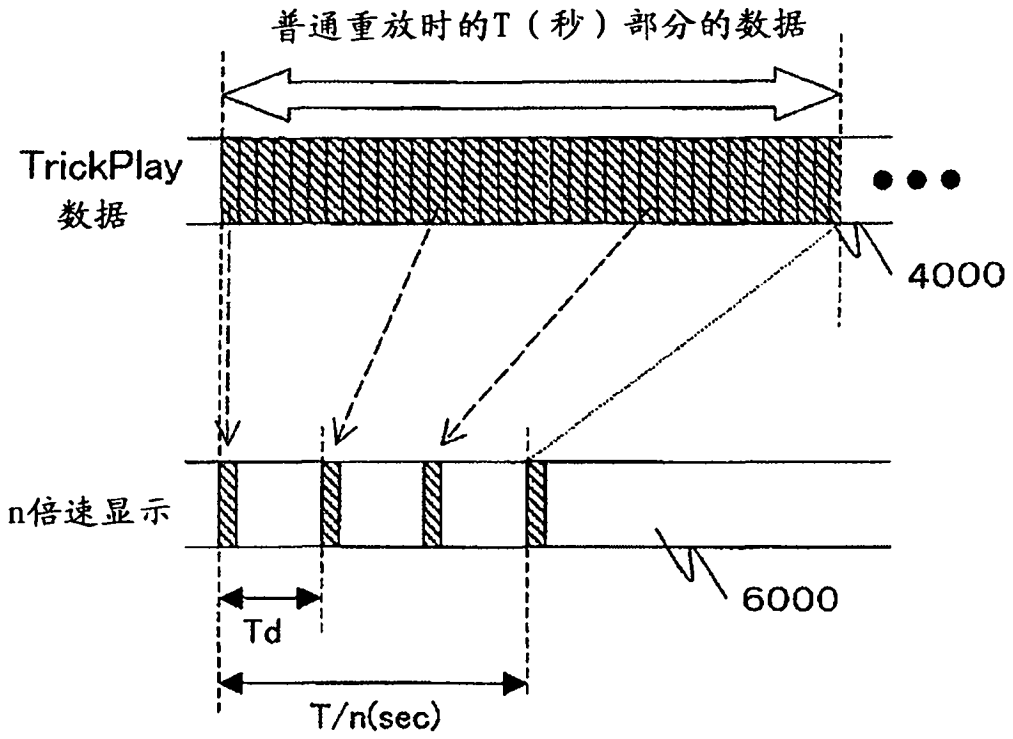


图 8

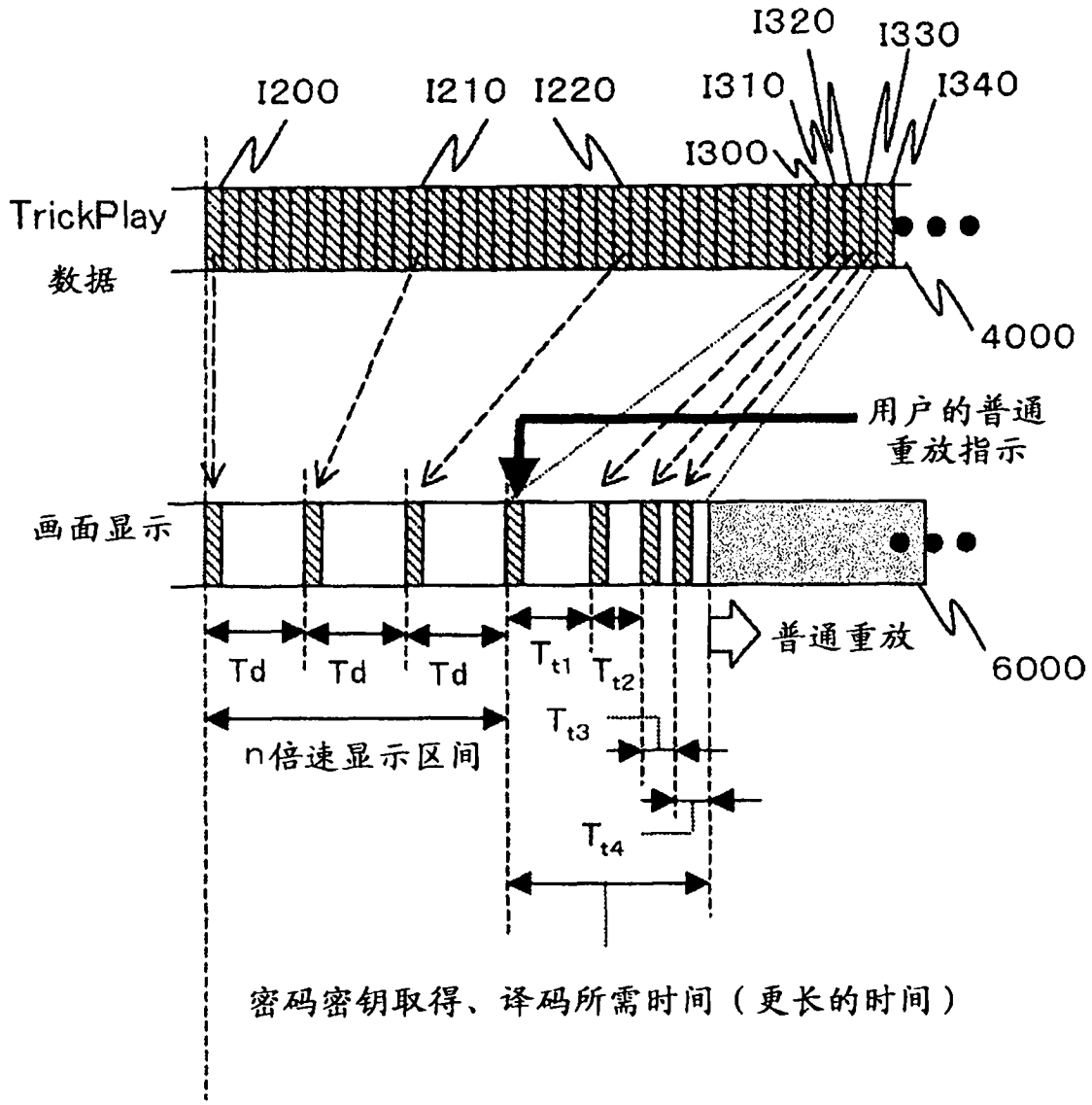

I320
I330
I200
I210
I220
I310
I340
I300
TrickPlay
数据
4000
用户的普通
重放指示
画面显示
普通重放
6000
Td
Td
Td
T_{t1}
T_{t2}
T_{t3}
n倍速显示区间
T_{t4}
密码密钥取得、译码所需时间（更长的时间）

图 9

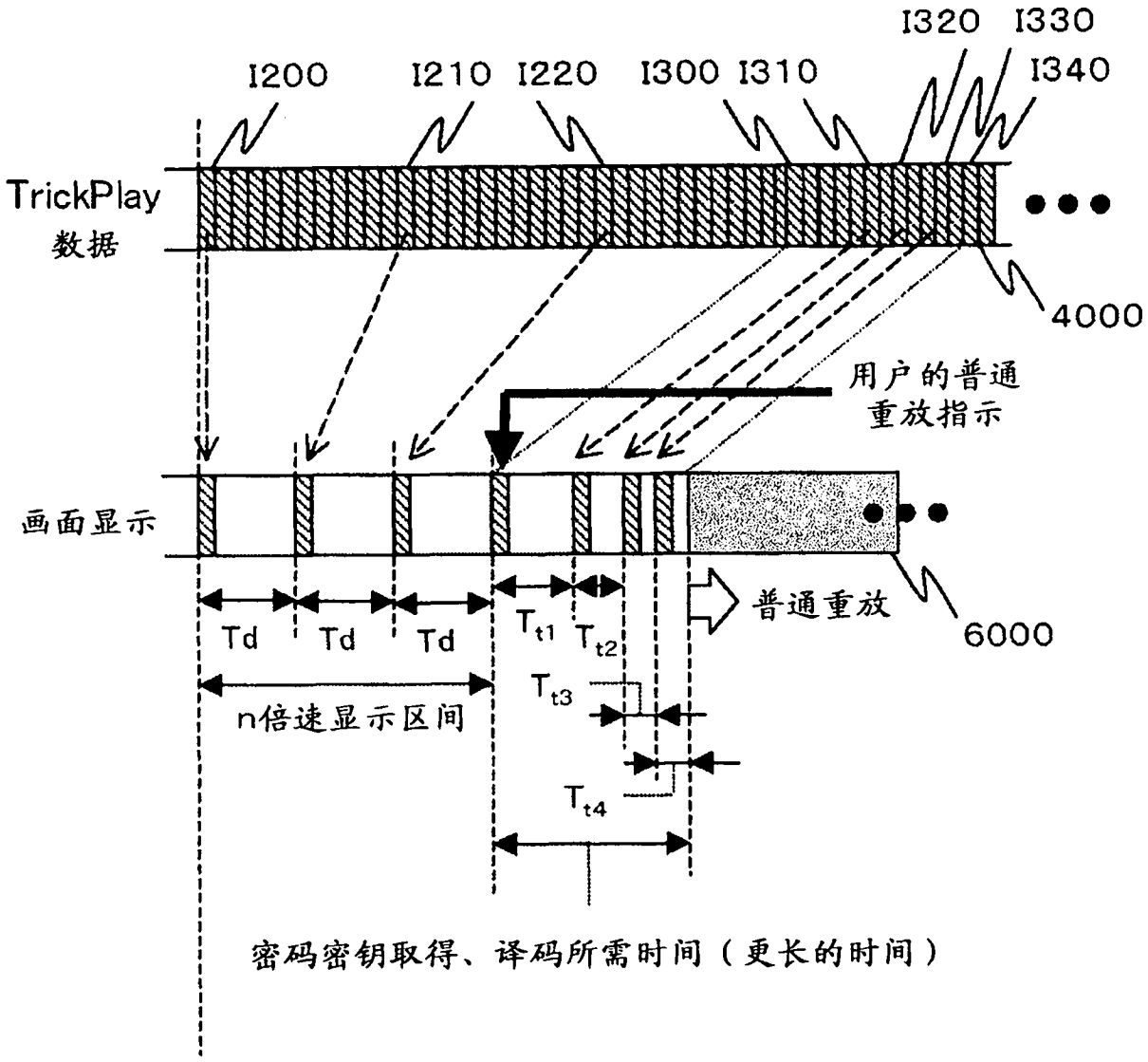

I320
I330
I200
I210
I220
I300
I310
I340
TrickPlay
数据
4000
用户的普通
重放指示
画面显示
普通重放
6000
Td
Td
Td
T_{t1}
T_{t2}
T_{t3}
T_{t4}
n倍速显示区间
密码密钥取得、译码所需时间（更长的时间）

图 10

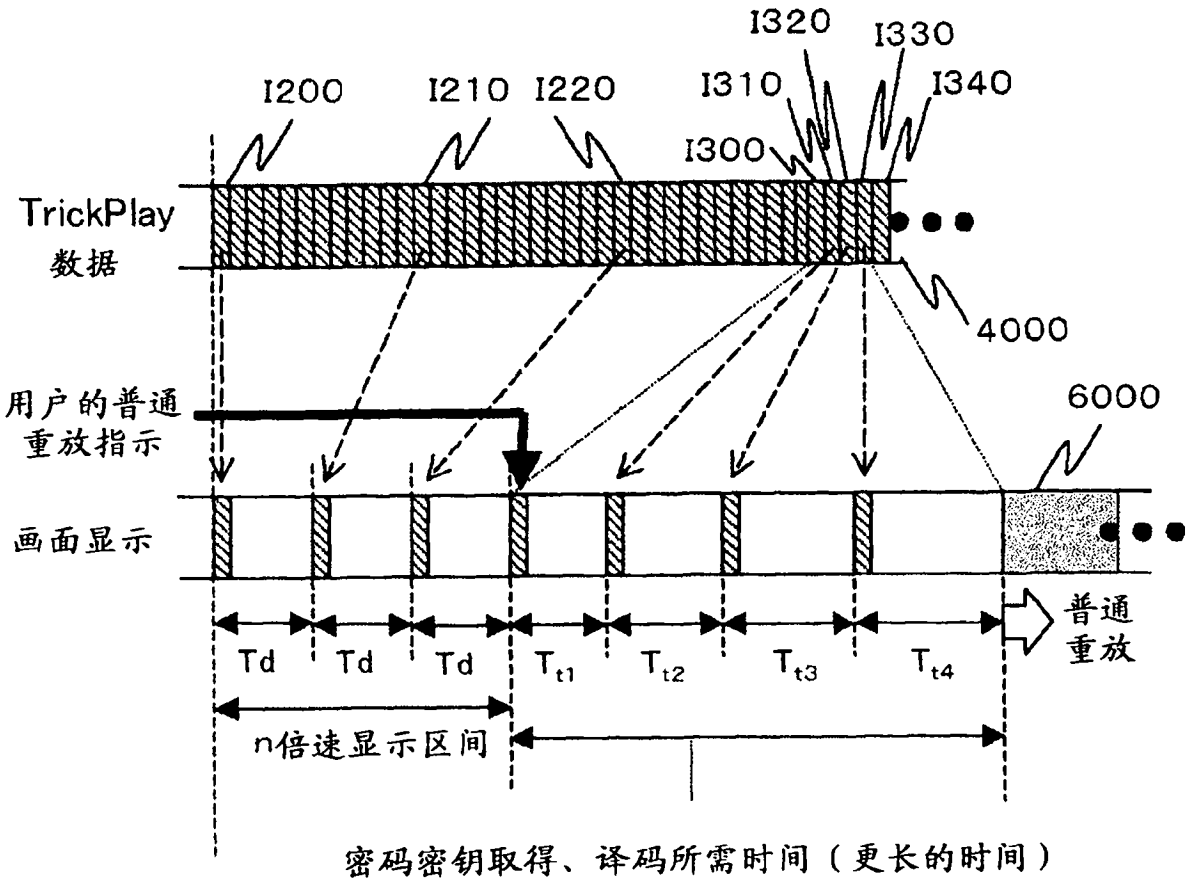

I320
I330
I200
I210
I220
I310
I340
I300
TrickPlay
数据
4000
用户的普通
重放指示
6000
画面显示
普通
重放
Td
Td
Td
T_{t1}
T_{t2}
T_{t3}
T_{t4}
n倍速显示区间
密码密钥取得、译码所需时间（更长的时间）

图 11

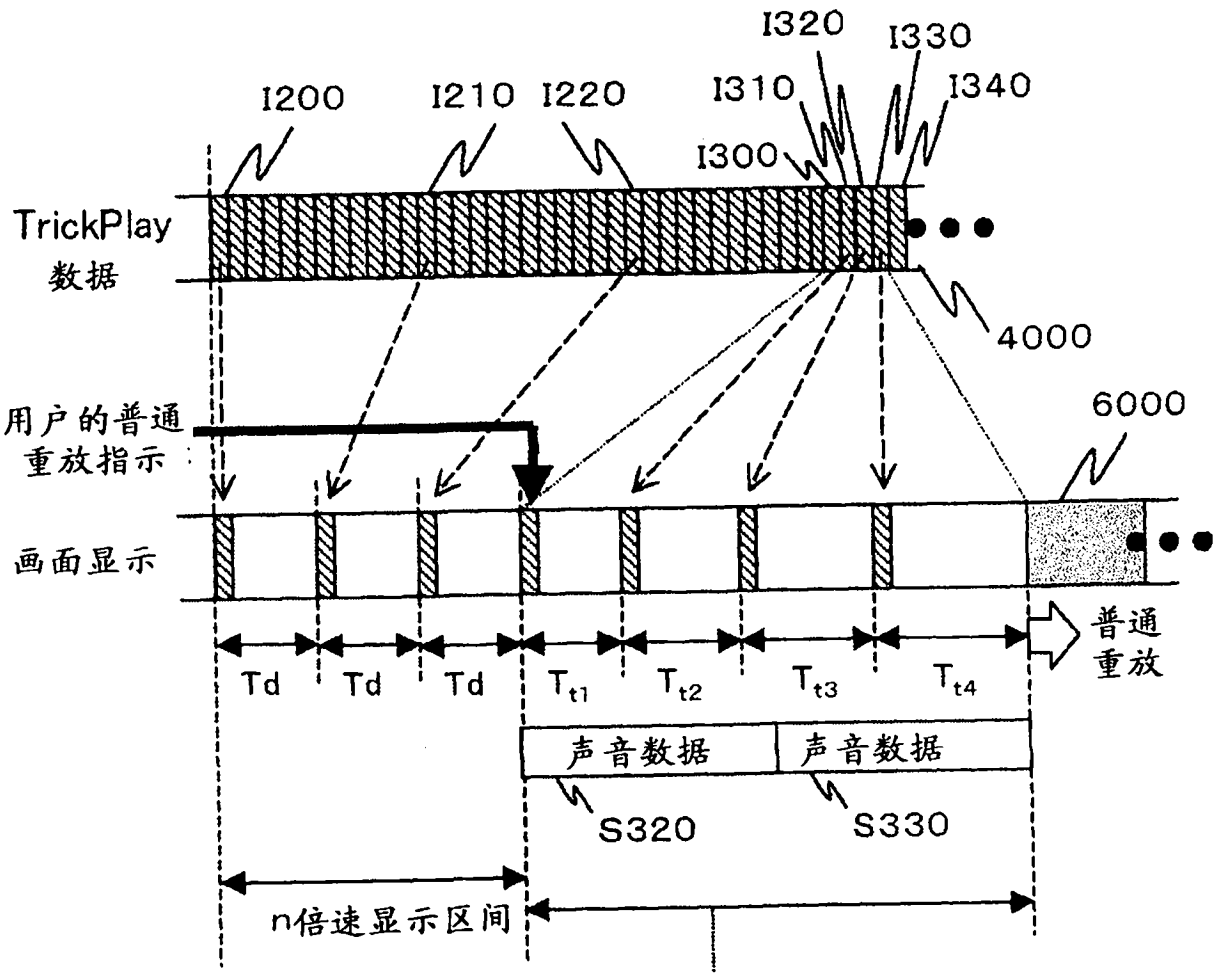

I320
I330
I200
I210
I220
I310
I340
I300
TrickPlay
数据
4000
用户的普通
重放指示
6000
画面显示
普通
重放
Td
Td
Td
T_{t1}
T_{t2}
T_{t3}
T_{t4}
声音数据
声音数据
S320
S330
n倍速显示区间
密码密钥取得、译码所需时间（更长的时间）

图 12

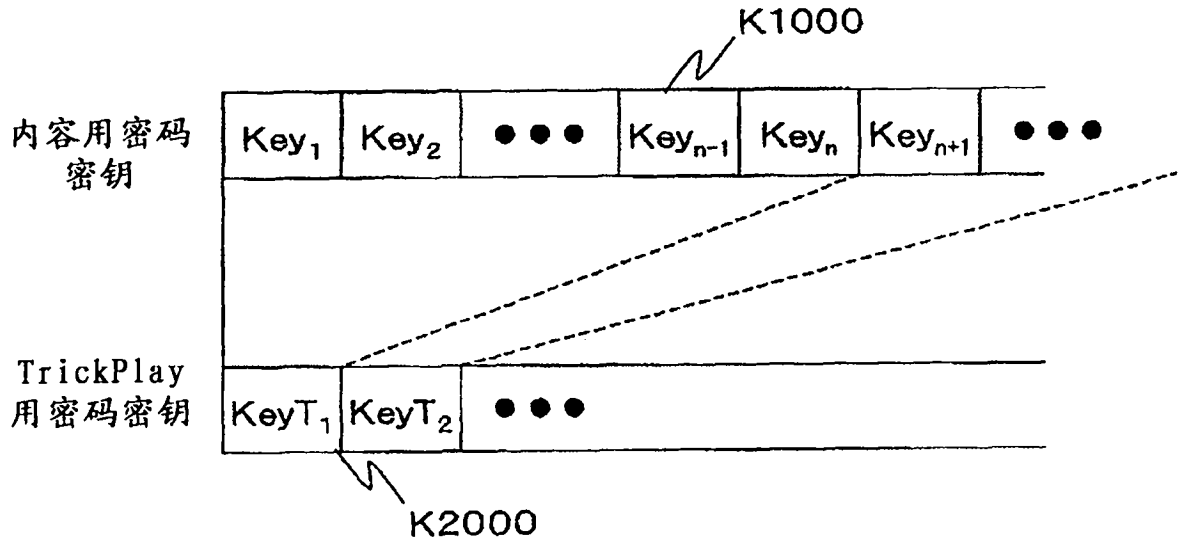

K1000
内容用密码
密钥
Key_1
Key_2
Key_{n-1}
Key_n
Key_{n+1}
TrickPlay
用密码密钥
$KeyT_1$
$KeyT_2$
K2000

图 13

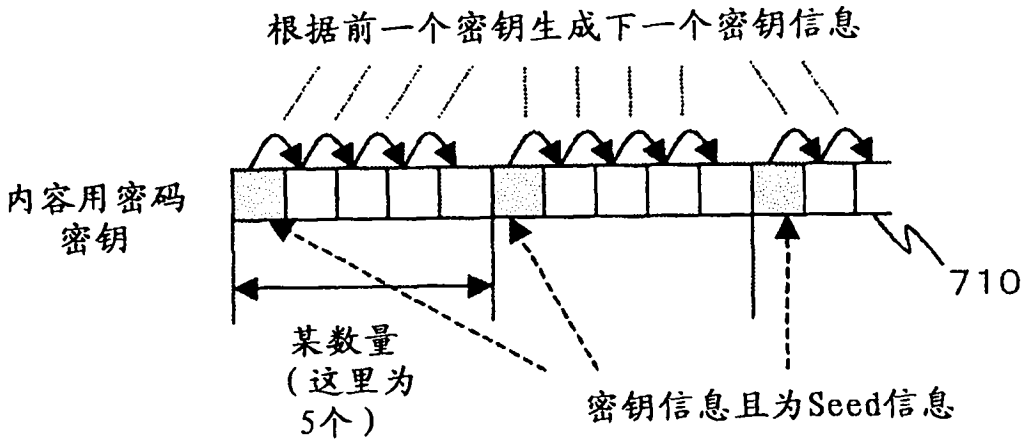

根据前一个密钥生成下一个密钥信息
内容用密码
密钥
710
某数量
（这里为
5个）
密钥信息且为Seed信息

图 14

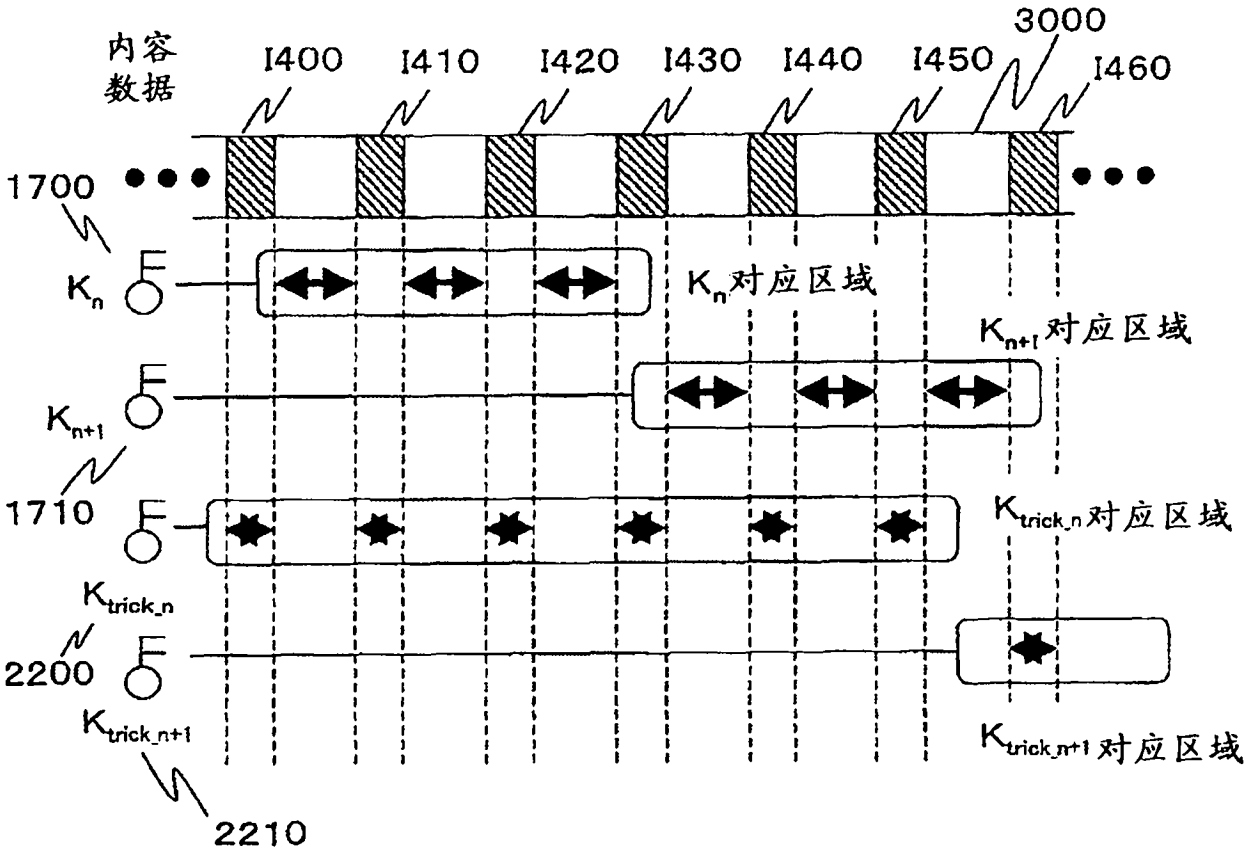

内容
数据
I400
I410
I420
I430
I440
I450
3000
I460
1700
Kn
Kn对应区域
Kn+1对应区域
Kn+1
1710
Ktrick_n对应区域
Ktrick_n
2200
Ktrick_n+1
Ktrick_n+1对应区域
2210

图 15