[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 5/92 (2006.01)
G06F 12/00 (2006.01)
G06F 12/14 (2006.01)
H04L 9/14 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200480003319.4

[43] 公开日 2006 年 3 月 8 日

[11] 公开号 CN 1745580A

[22] 申请日 2004.2.18
[21] 申请号 200480003319.4
[30] 优先权
[32] 2003. 3. 7 [33] JP [31] 061460/2003
[86] 国际申请 PCT/JP2004/001771 2004.2.18
[87] 国际公布 WO2004/080070 日 2004.9.16
[85] 进入国家阶段日期 2005.8.1
[71] 申请人 松下电器产业株式会社
地址 日本大阪府
[72] 发明人 松井义德

[74] 专利代理机构 永新专利商标代理有限公司
代理人 黄剑锋

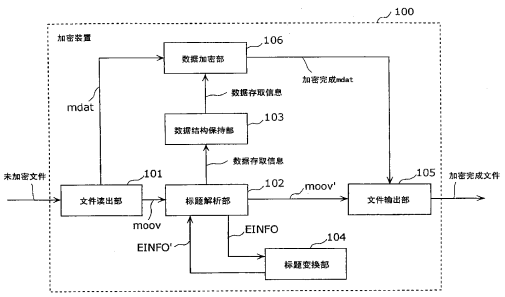
权利要求书 6 页 说明书 20 页 附图 18 页

[54] 发明名称

加密装置、解密装置及数据重放装置

[57] 摘要

本发明的加密装置(100)包括：文件读出单元(101)，用于取得由存放了编码的图像数据、声音数据及文本数据中的至少一个的数据部(mdat)、和存放了数据部的标题的标题部(moov)构成的文件；加密单元(106)，对文件的数据部中所存放的各数据中的至少一个进行加密；标题解析单元(102)，对文件的标题部进行解析，以取得标题部所包含的、表示在加密单元(106)中所加密的数据的编码方式的字段(EINFO)的值；标题变换单元(104)，根据预先确定的变换规则对所取得的值进行变换，并将字段的值改写为变换后的值；以及文件输出单元(105)，输出由包含值被改写了的字段(EINFO`)的标题部(moov`)、及存放了加密的数据的数据部(加密完成 mdat)构成的文件。



1、一种加密装置，对编码的图像数据、声音数据及文本数据中的至少一个进行加密，其特征在于，包括：

文件读出单元，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、和存放了上述数据部的标题的标题部构成的文件；

加密单元，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中的至少一个进行加密；

标题解析单元，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示在上述加密单元中所加密的数据的编码方式的字段中所描述的值；

标题变换单元，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；以及

文件输出单元，输出由包含上述值被改写了的字段的标题部、及存放了上述加密后的数据的数据部构成的文件。

2、如权利要求 1 所述的加密装置，其特征在于：

上述标题变换单元通过使上述取得的值进行位翻转来进行变换。

3、如权利要求 2 所述的加密装置，其特征在于：

上述标题变换单元根据上述加密单元中的加密方式，改变上述取得的值中位翻转的位置。

4、如权利要求 2 所述的加密装置，其特征在于：

上述标题变换单元根据上述加密单元中的加密方式，改变在位翻转中所采用的位翻转式。

5、如权利要求 1 所述的加密装置，其特征在于：

上述变换规则由将上述取得的值和上述变换后的值相对应地记录的变换表来表示。

6、一种解密装置，编码的图像数据、声音数据及文本数据中的至少一个被加密后，对该加密后的数据进行解密，其特征在于，包括：

文件读出单元，用于取得由存放了上述编码的图像数据、声音数

据及文本数据的数据部、和存放了上述数据部的标题的标题部构成的文件；

标题解析单元，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示上述加密的数据的编码方式及有关加密的信息的字段中所描述的值；

标题变换单元，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；

解密单元，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中加密的数据进行解密；以及

文件输出单元，输出由包含上述值被改写了的字段的标题部、及存放了上述解密后的数据的数据部构成的文件。

7、如权利要求 6 所述的加密装置，其特征在于：

上述标题变换单元通过使上述取得的值进行位翻转来进行变换。

8、如权利要求 7 所述的加密装置，其特征在于：

上述标题变换单元根据上述有关加密的信息，改变上述取得的值中位翻转的位置。

9、如权利要求 7 所述的加密装置，其特征在于：

上述标题变换单元根据上述有关加密的信息，改变在位翻转中所采用的位翻转式。

10、如权利要求 6 所述的加密装置，其特征在于：

上述变换规则由将上述取得的值和上述变换后的值相对应地记录的变换表来表示。

11、一种数据重放装置，编码的图像数据、声音数据及文本数据中的至少一个被加密后，对该加密的数据进行解密、并进行解码以重放，其特征在于，包括：

文件读出单元，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、和存放了上述数据部的标题的标题部构成的文件；

标题解析单元，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示上述加密的数据的编码方式及与加密有关的信息的

字段中所描述的值；

标题变换单元，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；

解密单元，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中加密的数据进行解密；以及

解码单元，参照上述值被改写了的字段，以判别上述数据的编码方式，并对上述已解密的数据进行解码。

12、如权利要求 11 所述的数据重放装置，其特征在于：

上述标题变换单元通过使上述取得的值进行位翻转来进行变换。

13、如权利要求 12 所述的数据重放装置，其特征在于：

上述标题变换单元根据上述有关加密的信息，改变上述取得的值中位翻转的位置。

14、如权利要求 12 所述的数据重放装置，其特征在于：

上述标题变换单元根据上述有关加密的信息，改变在位翻转中所采用的位翻转式。

15、如权利要求 11 所述的数据重放装置，其特征在于：

上述变换规则由将上述取得的值和上述变换后的值相对应地记录的变换表来表示。

16、一种加密方法，对编码的图像数据、声音数据及文本数据中的至少一个进行加密，其特征在于，包括：

文件读出步骤，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、和存放了上述数据部的标题的标题部构成的文件；

加密步骤，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中的至少一个进行加密；

标题解析步骤，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示在上述加密单元中所加密的数据的编码方式的字段中所描述的值；

标题变换步骤，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；以及

文件输出步骤，输出由包含上述值被改写了的字段的标题部、及存放了上述加密数据的数据部构成的文件。

17、一种解密方法，编码的图像数据、声音数据及文本数据中的至少一个被加密后，对该加密的数据进行解密，其特征在于，包括：

文件读出步骤，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、和存放了上述数据部的标题的标题部构成的文件；

标题解析步骤，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示上述加密的数据的编码方式及有关加密的信息的字段中所描述的值；

标题变换步骤，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；

解密步骤，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中加密的数据进行解密；以及

文件输出步骤，输出由包含上述值被改写了的字段的标题部、及存放了上述解密的数据的数据部构成的文件。

18、一种数据重放方法，编码的图像数据、声音数据及文本数据中的至少一个被加密后，对该加密的数据进行解密、并进行解码以重放，其特征在于，包括：

文件读出步骤，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、和存放了上述数据部的标题的标题部构成的文件；

标题解析步骤，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示上述加密的数据的编码方式及有关加密的信息的字段中所描述的值；

标题变换步骤，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；

解密步骤，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中加密的数据进行解密；以及

解码步骤，参照上述值被改写了的字段，以判别上述数据的编码

方式，并对上述已解密的数据进行解码。

19、一种程序，用于对编码的图像数据、声音数据及文本数据中的至少一个进行加密的加密装置，其特征在于，该程序使计算机执行以下步骤：

文件读出步骤，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、和存放了上述数据部的标题的标题部构成的文件；

加密步骤，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中的至少一个进行加密；

标题解析步骤，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示在上述加密单元中所加密的数据的编码方式的字段中所描述的值；

标题变换步骤，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；以及

文件输出步骤，输出由包含上述值被改写了的字段的标题部、及存放了上述加密的数据的数据部构成的文件。

20、一种程序，用于解密装置，其中该解密装置在编码的图像数据、声音数据及文本数据中的至少一个被加密后，对该加密的数据进行解密，其特征在于，该程序使计算机执行以下步骤：

文件读出步骤，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、及存放了上述数据部的标题的标题部构成的文件；

标题解析步骤，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示上述加密的数据的编码方式及有关加密的信息的字段中所描述的值；

标题变换步骤，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；

解密步骤，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中加密的数据进行解密；以及

文件输出步骤，输出由包含上述值被改写了的字段的标题部、及

存放了上述解密的数据的数据部构成的文件。

21、一种程序，用于数据重放装置，其中该数据重放装置在编码的图像数据、声音数据及文本数据中的至少一个被加密后，对该加密的数据进行解密、并进行解码以重放，其特征在于，该程序使计算机执行以下步骤：

文件读出步骤，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、和存放了上述数据部的标题的标题部构成的文件；

标题解析步骤，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示上述加密的数据的编码方式及有关加密的信息的字段中所描述的值；

标题变换步骤，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；

解密步骤，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中加密的数据进行解密；以及

解码步骤，参照上述值被改写了的字段，以判别上述数据的编码方式，并对上述已解密的数据进行解码。

22、一种记录媒体，记录有文件，计算机可以读取，其特征在于：

上述文件中包括：

编码的图像数据、声音数据及文本数据中至少一个被加密后，存放该加密的数据的数据部；及

存放上述数据部的标题的标题部；

在上述标题中，包含表示上述加密的数据的编码方式及与加密有关的信息的字段。

加密装置、解密装置及数据重放装置

技术领域

本发明涉及将数据服务器及存储器上所保持的加密/未加密数据文件进行解密/加密，以转移到其他数据服务器及存储器上的解密装置/加密装置，以及输入加密/未加密数据文件进行解码重放的数据重放装置。作为与加密相对的概念一般采用解码这样的用语，但是本说明书中，由于与编码相对的概念采用解码，所以与加密相对的概念采用解密这个术语进行说明。

背景技术

对图像、声音及文本等数字数据进行多路的国际标准方式有在ISO/MPEG（International Organization Standardization / Moving Picture Experts Group：国际标准化组织/运动图像专家组）、及作为确定第3代移动体 W-CDMA 通信的国际标准规格的团体的 3GPP（The Third Generation Partnership Project）等中标准化的文件格式（例如 ISO/IEC 14496-12、ISO/IEC 14496-14、及 3GPP TS26.234 等）。

图 1 是表示按上述规格确定的文件的构成的一个例子的图。

如图 1 中所示，文件 900 由标题部（“moov”）901、及数据部（“mdat”）902 构成。

标题部 901 包含与多路后的数字数据的媒体数相同数量或在该数量以上的轨道框（track box）（“trak”）903。另外，各个轨道框 903 包含一个取样详细信息存放框（“stsd”）904，取样详细信息存放框 904 至少包含一个条目（“entry”）905。条目 905 由条目大小（ENT_SZ）906、条目信息（EINFO）907、及其他字段构成，条目信息 907 包括条目类型（ENT_TP）908 及预约字段（RSV_6）909。

条目大小 906 是用字节数指定条目 905 大小的字段。

条目类型 908 是表示数字数据编码方式的字段。若根据上述规

格，则例如当是 MPEG4 视频编码方式时，在条目类型 908 中描述为 0x6D703476（mp4v），而当是 MPEG4 音频编码方式时，在条目类型 908 中描述为 0x6D703461（mp4a），当是 ITU-T H.263 视频编码方式时，在条目类型 908 中描述为 0x73323633（s263），当是 AMR 声音编码方式时，在条目类型 908 中描述为 0x73616D72（samr），当是时间文本编码方式时，在条目类型 908 中描述为 0x74783367（tx3g）等。

预约字段 909 是作为将来扩充区域而被预约的字段，是为规格修改等而设置的。

在数据部 902 中，对图像、声音及文本等数字数据进行多路后进行存放。这里，对各数据的存取信息，在轨道框 903 中，作为从文件 900 前头的偏移值而给出。例如，当对某个图像数据的存取信息是 12,450 字节以及在轨道框 903 中被指定时，将是在离文件 900 前头 12,450 字节的位置处，存放该图像数据。

然而，近些年来随着宽带网的普及，使高质量的动态图像数据传输成为可能，从而可提供收费动态图像数据传输服务。在提供视听价值高的动态图像数据传输服务时，从著作权等无形财产权保护的观点考虑，对数据加密是必不可少的，当前，即使 ISO/MPEG 等也提出了建立存放了加密后的数据的文件格式的规格的方案。

图 2 是表示在 ISO/MPEG 中现在提案的现有加密文件格式中数据结构的一部分的图。该现有的加密文件格式中的数据结构，例如已在日本专利申请特开 2002-304805 号公报中公开。

如图 2 中所示，在现有的加密文件格式中，提出了在条目 910 中附加了所谓加密信息框（“einf”）911 的数据结构的方式。根据该方式，在现有的条目类型 908 的描述中，对于描述为 mp4v 及 s263 等的视频编码方式，共同描述为 0x656E6376（encv），而对于描述为 mp4a 及 samr 等的声音编码方式，共同描述为 0x656E6361（enca）。

另外，加密后的条目类型 908 尽管集中在 encv 及 enca 等上，但是原来的条目类型 908，即加密前在条目类型 908 中描述的 mp4v 及 samr 等将在处于“einf”911 中的原始格式框（“frma”）912 的数据

格式字段 915 中描述。

从而，通过参照该数据格式字段 915，可以判别编码方式，在条目类型 908 中，通过描述为特有的 encv 及 enca 等，可以判别加密的有无。另外，在进行了加密的情况下，还需要表示使用了怎样的加密方式的信息，对此，采用在“einf”911 中所包含的方案框（“schm”）913 的方案类型字段 916、方案版本字段 917 进行描述，通过参照这些字段，可以判别加密方式及其版本。此外，在“einf”911 中，包含具有方案特定数据字段 918 的方案信息框 914 等。

图 3 是为了说明以现有的加密文件格式对某个未加密文件加密后的情况下文件的标题部的区别的图。

在图 3 中，分别表示了加密前（未加密时）的“stsd”904、及加密后（加密时）的“stsd”920。首先，未加密时的条目大小 906 表示为 0x000000F3（10 进制为 243），即表示为是 243 字节，条目类型 908 表示为是 0x6D703476（mp4v）。另一方面，加密时的条目大小 906 为 0x0000011B（10 进制为 283），即表示为是 283 字节，条目类型 908 表示为是 0x656E6376（encv）。另外，在加密时的“stsd”920 中附加了“einf”911，在“einf”911 的框类型（B0X_TP）字段 921 中，描述为 0x65696E66（einf）。另外，在未加密时的条目类型 908 中描述的 0x6D703476（mp4v）被复制到“einf”911 中的“frma”912 的数据格式字段 915 中。

但是，上述现有的文件格式，由于加密时和未加密时的标题部的数据大小发生了变化，所以必须对数字数据的存取信息全部更新，这会产生种种问题。

具体说明如下，当对未加密文件加密时，由于附加了“einf”911，所以如图 4 中所示，未加密时和加密时，在标题部 901 及标题部 931 的大小上产生差异，文件大小在未加密时的文件 900 和加密时的文件 930 间是不同的。

从而，在加密装置/解密装置中，除了加密/解密处理之外，还需要再生成标题部的处理，这样，存在加密装置/解密装置的处理负荷加大的问题。

另外，如前文已说明的，对各数据的存取信息，在轨道框 903 中的字段中作为从文件前头起的偏移值而被给出，但是加密文件中，由于在数据部 932 之前的标题部 931 的大小增加，所以数据部 932 的开始位置就会偏离。

从而，当加密装置/解密装置将未加密时的文件 900 变换成加密后的文件 930 的情况下，或者将加密时的文件 930 变换成未加密的文件 900 的情况下，存在必须更新全部对数据的存取信息的问题。而且这种对数据的存取信息的更新，即使是只选择一部分信道进行加密/解密处理时，对并非加密/未加密处理对象的信道也必须进行。

特别是，在作为文件的记录媒体，使用 DVD 等光盘的情况下（例如，DVD 记录器等），由于文件因加密/解密的文件大小发生变化，所以引起光盘上的数字数据的记录位置也必须变更的问题。

另外，由于文件大小变更，在根据存储卡的规格不同，管理各文件的文件大小信息的情况下，其管理信息也需要相应更新。

发明内容

为此，本发明鉴于这些问题而做出，其目的在于提供一种加密装置，其不改变文件大小就可以对未加密数据进行加密，另外，本发明的目的在于提供一种解密装置，其不改变文件大小就可以对加密的数据进行解密。

为了达到上述目的，本发明的加密装置，对编码的图像数据、声音数据及文本数据中的至少一个进行加密，其特征在于，包括：文件读出单元，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、及存放了上述数据部的标题的标题部构成的文件；加密单元，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中的至少一个进行加密；标题解析单元，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示在上述加密单元中所加密的数据的编码方式的字段中所描述的值；标题变换单元，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；以及文件输出单元，对由包含上

述值被改写后的字段的标题部、及存放上述加密后的数据的数据部构成的文件进行输出。这样，在对编码数据进行加密时，由于根据预定的规则对文件的标题中所包含的表示编码方式的字段的值进行改写，所以不改变文件的标题的大小，就可以在文件的标题中指定加密前的编码方式及加密的有无。另外，由于也不需要重放标题部，及变更数据的记录位置，所以装置的处理负荷也可以较少。

此处，上述标题变换单元，最好通过使上述取得的值进行位翻转来进行变换；另外，上述标题变换单元，根据上述加密单元的加密方式，改变在上述取得的值中使位翻转的位置，并且上述标题变换单元，最好根据上述加密单元的加密方式，改变在位翻转中所采用的位翻转式。这样，由于根据加密方式可以改变位翻转的位置，及改变位翻转式，所以不改变文件大小，也可以由文件的标题指定加密方式及加密方式的版本号等。

另外，本发明所涉及的解密装置为，编码的图像数据、声音数据及文本数据中的至少一个已进行加密，对该加密的数据进行解密，其特征在于，包括：文件读出单元，用于取得由存放了上述编码的图像数据、声音数据及文本数据的数据部、及存放了上述数据部的标题的标题部构成的文件；标题解析单元，对上述文件的标题部进行解析，以取得上述标题部所包含的、表示上述加密的数据的编码方式及有关加密的信息的字段中所描述的值；标题变换单元，根据预先确定的变换规则对上述取得的值进行变换，并将上述字段中所描述的值改写为上述变换后的值；解密单元，对上述文件的数据部中所存放的上述编码的图像数据、声音数据及文本数据中加密的数据进行解密；以及文件输出单元，对由包含上述值被改写后的字段的标题部、及存放了上述解密的数据的数据部构成的文件进行输出。这样，由于将文件的标题中所包含的表示编码方式和有关加密的信息的字段的值，根据规定的规则，改写为表示编码方式的字段，所以不变更文件大小，就可以对加密的数据进行解密。

本发明不仅可以实现这样的加密装置或解密装置，也可以实现解密后对编码数据进行解码重放的数据重放装置，既可以实现为以这样

的加密装置、解密装置或数据重放装置所具有的特征手段为步骤的加密方法、解密方法或数据重放方法，又可以实现为使计算机执行这些步骤的程序。而且，这样的程序当然也可以通过 CD-ROM 等记录媒体及因特网等传输媒体进行信息发送。

如上所述，根据本发明所涉及的加密装置，由于通过对文件标题所包含的表示编码方式的字段的值按预定的规则进行改写，指定加密前的编码方式、加密的有无、加密方式及加密方式的版本号，所以不变更文件大小，就可以对未加密数据进行加密。另外，由于图像、声音、文本等数据从文件前头起的存放位置不变化，所以不必变更对数据的存取信息。还由于只改写标题部的一部分即可，所以与根据现有文件格式规格动作的加密装置相比，可以大幅度削减标题部的处理量。另外，可以获得即使对光盘上的文件进行加密时，也没必要变更数据的记录位置，以及根据存储卡的规格不同而需要对保持文件大小信息的管理信息进行更新也不再需要等效果。

另外，根据本发明所涉及的解密装置，由于对文件的标题中所包含的表示编码方式和有关加密的信息的字段的值按预定的规则进行改写，所以可以使加密的数据在解密之前和解密之后，文件大小相同，所以可以大幅度削减标题部的处理量。

另外，根据本发明所涉及的数据重放装置，即使输入加密后的文件时，也可以通过加密判别装置，用一个数据字段判别加密的有无和编码方式。另外，由于变换成与现有的未加密时的文件格式互换的格式，所以对标题解析处理可以利用现有的方法。从而可取得与现有技术相比可提供廉价的数据重放装置的效果。

附图说明

图 1 是表示由规格决定的现有文件的构成的一个例子的图。

图 2 是表示现有的加密文件格式中的数据结构的一部分的图。

图 3 是为了说明以现有的加密文件格式对未加密文件加密后的情况下的文件标题部的区别的图。

图 4 是为说明在未加密时和加密时文件大小不同的图。

图5是表示本发明实施方式1所涉及的加密装置功能构成的方框图。

图6（a）是表示变换表第1例的图。

图6（b）是表示变换表第2例的图。

图6（c）是表示变换表第3例的图。

图7是表示同一装置上的标题变换部的处理动作的第1例的流程图。

图8是加密前的文件和由加密装置100进行的加密处理后的文件的比较图。

图9是加密前的文件和由加密装置100进行的第2加密处理后的文件的比较图。

图10是表示位翻转表的一个例子的图。

图11是表示同一装置上的标题变换部的处理动作的第2例的流程图。

图12是位翻转前的条目类型和位翻转后的条目类型的比较图。

图13是表示本发明实施方式2所涉及的解密装置功能构成的方框图。

图14是表示同一装置上的标题变换部的处理动作的第1例的流程图。

图15是表示同一装置上的标题变换部的处理动作的第2例的流程图。

图16是表示本发明实施方式3所涉及的数据重放装置功能构成的方框图。

图17是表示同一装置上的加密判断部的处理动作的流程图。

图18是表示本发明所涉及的加密装置、解密装置及数据重放装置的应用例的图。

具体实施方式

本发明所涉及的加密装置、解密装置及数据重放装置，在ISO/MPEG的文件格式（MP4文件格式）中，通过数据部的加密/解

密，使标题部的大小及文件大小不变，并且根据可以设定加密的文件解密所需要的加密的有无、编码方式的判别的数据格式进行操作。

下面，参照附图对本发明的实施例进行说明。在本实施例中，作为加密或解密的数据主要采用图像数据进行说明，但这并不意味排除音频数据及文本数据等其他媒体数据的加密或解密。

（实施方式 1）

首先，采用图 5～图 12 说明作为本发明实施方式 1 的加密装置。

图 5 是表示本实施方式 1 所涉及的加密装置功能构成的方框图。

如图 5 中所示，加密装置 100 包括：文件读出部 101、标题解析部 102、数据结构保持部 103、标题变换部 104、文件输出部 105 及数据加密部 106。

文件读出部 101，是输入根据 MP4 文件格式存放了图像、声音及文本等数据的未进行加密的文件（未加密文件）的处理部，根据标题解析部 102 的指示，读入未加密文件，将文件的标题部（“moov”）输出给标题解析部 102。

标题解析部 102 是解析“moov”的处理部，将“moov”中所包含的各条目的 EINFO 输出给标题变换部 104，并将对存放在未加密文件中的图像、声音、文本等数据的存取信息（数据存取信息）输出给数据结构保持部 103。另外，当标题解析部 102 从标题变换部 104 取得由变换 EINFO 而得到的 EINFO`时，生成插入了 EINFO`的“moov`”，输出给文件输出部 105。

数据结构保持部 103 是用于保持表示分别对图像、声音、文本等数据从文件前头起的存放位置的数据存取信息的 DRAM 及 SDRAM 等存储器。

标题变换部 104 是为了能够判别加密的有无及编码方式而将 EINFO 变换成 EINFO`的处理部，具有变换时参照的变换表，从标题解析部 102 取得 EINFO，并根据变换表变换成 EINFO`后，将 EINFO`输出给标题解析部 102。

数据加密部 106 是进行数据加密的处理部，从文件读出部 101 取得文件的数据部（“mdat”），采用数据结构保持部 103 中保持的数

据存取信息，对数据进行加密，并将进行了加密的数据部（加密完成的 mdat）输出给文件输出部 105。

文件输出部 105 是从标题解析部 102 取得“moov`”，从数据加密部 106 取得加密完成的 mdat，将这些一体化后输出加密完成文件的处理部。

在此，关于标题变换部 104 具有的变换表，在图 6 中示出了多个例子进行说明。

图 6（a）是表示变换表的第 1 例的图。

在图 6（a）中，表示了左侧的变换表 A104a、及右侧的变换表 B104b。此处变换表 A104a 及变换表 B104b 通过#序号分别对应起来，并且意味着如果在未加密的文件 EINFO 中所包含的条目类型中描述为 0x6D703476(“mp4v”)的值，则将该值变换成 0x65703476(“ep4v”)的值。即，在图 6（a）中，构成为将未加密的文件 EINFO 中所包含的条目类型的前头的字符全部变换为 0x65（“e”）。

此外，如图 6(b)中所示，也可以构成为对于条目类型的前头字符，将英文小写字母 m 变换成英文大写字母 M（0x6D→0x4D）。这样，将未加密时 mp4v、mp4a、s263、samr 等条目类型的值，在加密时变换成 Mp4v、Mp4v、S263、Samr 等。另外，如图 6（c）中所示，也可以使条目类型的前头字符全部为 0x00。即，加密一侧和解密一侧只要是按唯一确定的规则进行变换，采用怎样的变换规则都可以，例如，可以不是前头字符而是对任意字符进行变换，也可以对 2 个以上字符进行变换。另外，也可以是更换字符顺序的变换规则。

下面，对标题变换部 104 的具体操作例进行说明。此处，设标题变换部 104 采用图 6(a)中所示的变换表，在条目类型中描述为 mp4v。

图 7 是表示标题变换部 104 的处理动作的第 1 例的流程图。

首先，标题变换部 104 输入从标题解析部 102 所输出的 EINFO（S102）。

然后，标题变换部 104 读出 EINFO 中所包含的条目类型（ENT_TP）（S104），判断 ENT_TP 的前头字节 ENT_TP[0]是否是 0x65（ASCII 码表示 e）（S106）。

在此，如果是 0x65（S106 的是），则说明有关该信道的图像数据已经加密完成，不必变更 EINFO 的值，所以可以省略从步骤 S108 到步骤 S112 的处理。在本实施方式 1 中，将 ENT_TP 的前头字节是否是 0x65 作为加密有无的判断基准。

另一方面，当不是 0x65 时（S106 的否），标题变换部 104 从变换表 B104b 中检索 ENT_TP 中描述的值（S108）。在图 6（a）中，变换表 B104b 至少具有 0～3 四个备选，这些值当用 ASCII 码表示时，各条目分别是，#0 为 mp4v、#1 为 mp4a、#2 为 S263、#3 为 samr。这些值分别是表示在 ISO/MPEG 及 3GPP 规格中规定的编码方式的规定值。

标题变换部 104 根据步骤 S108 中的检索结果，判断是否检测出了一致的值（S110）。在此，由于 ENT_TP 的值是 mp4v，所以标题变换部 104 判断与变换表 B104b 的#0 条目一致（S110 的是）。当未检测出一致时（S110 的否），标题变换部 104 原样保持在 ENT_TP 中描述的值，进入步骤 S114。

然后，标题变换部 104 将 ENT_TP 的值置换成与变换表 A104a 中相同的#0 条目的值 0x65703476（“ep4v”）（S112）。

最后，如上所述将变换路径 ENT_TP 值的 EINFO`输出到标题解析部 102，结束处理动作（S114）。

图 8 是加密前的文件和由加密装置 100 进行加密处理后的文件的比较图。

在图 8 中，分别表示了在加密前（未加密时）文件 110 的“moov”111 中所包含的取样详细信息存放框（“stsd”）113、及加密后（加密时）文件 120 的“moov”121 中所包含的“stsd”123，未加密时的 ENT_TP 116 的前头字节的值（6D）及加密时的 ENT_TP 126 的前头字节的值（e）进行了变换。

这样，将作为在未加密时用于描述编码方式的字段的 ENT_TP 116 的值，在对数据加密时进行变换，可以将加密时的文件 120 的 ENT_TP 126 作为表示编码方式和加密有无的字段。

另外，如本图所示，条目大小（ENT_SZ）115 的值，在未加密

时的文件 110 和加密时的文件 120 中未变化。这意味着尽管进行加密处理，“moov” 111 和“moov” 121 之间大小不变化，即，文件 110 和文件 120 中的文件大小相等。

在以上的说明中，尽管假设了数据加密所使用的加密方式是固定的，但是即使加密方式是可变时，加密装置 100 在标题变换部 114 中也可以设定加密方式及其版本号等。这时，可以考虑采用上述文件格式的预约字段（RSV_6），描述加密方式及其版本号。

即，由于预约字段是值为 0 的 6 字节的字段，所以标题变换部 104 在图 7 中所示的流程图的步骤 S112 中，将 ENT_TP 置换成变换表 A104a 的值之后，例如设定使用 4 字节表示加密方式的方案类型字段（SC_TYPE），及使用 2 字节表示加密方式的版本号的方案版本字段（SC_VER），以描述预先赋予的加密方式及其版本号的值，将 EINFO`输出给标题解析部 102。

图 9 是加密前的文件和由加密装置 100 进行第 2 加密处理后的文件的比较图。

在图 9 中，在未加密时的文件 130 的“stsd” 130 所包含的预约字段 136，在加密时的文件 140 的“stsd” 143 中，变换成方案类型字段（SC_TYPE）146、和方案版本字段（SC_VER）147。

与图 8 一样，ENT_SZ 134 的值在未加密时的文件 130 和加密时的文件 140 中未变化。

这样，通过采用预约字段，加密装置 100 不改变文件大小，就可以生成能表示加密方式及其版本号等信息的加密文件。

然而，预约字段是作为将来的扩充区域而设置的，另外由于能使用的字节大小限定在 6 字节，所以加密装置 100 也可以在标题变换部 104 中，为表示编码方式、加密的有无、加密方式、及其版本号等而采用其他的方法变换 EINFO。在此，作为其他方法，对位翻转进行说明。

当使用位翻转时，标题变换部 104 保持多个记录了位翻转式的位翻转表，根据编码方式及加密方式，选择预先确定的位翻转式，根据该式，变换 EINFO 的 ENT_TP 值。

图 10 是表示位翻转表的一个例子的图。

如图 10 中所示，位翻转表 104g 对按每个编码方式及加密方式而不同的位翻转式进行列表记录。在本图中，表示在 ENT_TP 中描述的编码方式是 mp4v，当采用加密方式 1 对数据加密时，采用^A 的位翻转式，使 mp4v 进行位翻转，变换 ENT_TP 的值。

在本图中，未图示出加密方式的版本号，但是当也考虑加密方式的版本号时，例如只要用各版本号区分加密方式 1，分配不同的位翻转式即可。

图 11 是表示同一装置上的标题变换部的处理动作的第 2 例的流程图。此处与上述的情况一样，假设在 ENT_TP 中描述为 mp4v，执行按加密方式 1 进行的数据的加密。

首先，标题变换部 104，输入从标题解析部 102 所输出的 EINFO（S202）。

然后，标题变换部 104 读出 EINFO 中所包含的 ENT_TP（S204）。

接着，标题变换部 104 从位翻转表 104g 中检索在 ENT_TP 中描述的表示编码方式的值（S206），判断是否检索出了一致的值（S208）。此处，由于 ENT_TP 的值是 mp4v，所以标题变换部 104 判断在位翻转表 104g 中有一致的值（S208 的是）。当判断没有一致的值时（S208 的否），则标题变换部 104 原样保持 ENT_TP 所描述的值，转到步骤 S214。

再接着，标题变换部 104 根据由位翻转表 104g 所设定的位翻转式，使 ENT_TP 的值进行位翻转（S210）。在此，由于通过加密方式 1 进行了数据加密，所以标题变换部 104 从位翻转表 104g 中采用位翻转式^A，使 ENT_TP 的值进行位翻转。

然后，标题变换部 104 将 ENT_TP 的值置换成位翻转后的值（S212），最后，将变换了 ENT_TP 值的 EINFO`输出到标题解析部 102，处理动作结束（S214）

图 12 是位翻转前的条目类型和位翻转后的条目类型的比较图。

在图 12 中，表示了在未加密时的 ENT_TP 150 的前头 4 位 151 中描述了 0110 的值，最后 4 位 152 中也描述 0110 的值。这是因为当

用 ASCII 码的 16 进制表示 mp4v 时，是 0x6D703476，所以用二进制表示作为前头 4 位和最后 4 位的值的 6 的缘故。

另外，在本图中，表示前头 4 位 151 由于通过^1111（^f）进行位翻转，所以在加密时的 ENT_TP 160 前头 4 位 161 中描述了 1001 的值，最后 4 位 152 由于通过^1010（^a）进行位翻转，所以在加密时的 ENT_TP 160 的最后 4 位 162 中描述 1100 的值。

这时，前头 4 位 151 根据加密方式变更位翻转式，最后 4 位 152 根据加密方式的版本号变更位翻转式，从而可以表示加密方式是可变的情况、及加密方式的版本号等。

即，在 ENT_TP 中，使位翻转的位的位置按每个加密方式及版本号分开，另外，位翻转式也设置多个，由此可以使比采用上述的预约字段表示时更多的加密信息，在加密时和未加密时不改变文件大小进行表示。

这样，根据本实施形态 1 所涉及的加密装置，通过置换文件标题中所包含的表示编码方式的字段的值，并进行位翻转，可以在不变更文件大小的情况下，在文件的标题中指定加密前的编码方式、加密的有无、加密方式及加密方式的版本号等。

另外，在现有的 ISO/MPEG 的 MP4 文件格式中不可能用一个数据字段指定加密的有无和编码方式，但通过本实施方式 1 所涉及的加密装置却成为可能。

另外，由于图像、声音、文本等数据从文件的前头起的存放位置不发生变化，所以不必变更对各数据的存取信息，对于文件的标题只进行 EINFO 的 4 个字节（ENT_TP）的改写即可，与根据现有的文件格式规格动作的加密装置相比，可以大幅度削减标题的处理量。

另外，还由于文件大小不变化，所以即使像 DVD 记录器等那样，对光盘上的文件进行加密时，也可以期待不必变更数据的记录位置，因存储卡的规格而保持所需要的文件大小信息的管理信息也不必进行更新等各种效果。

（实施方式 2）

下面，采用图 13～图 15 说明本发明实施方式 2 的解密装置。

本实施方式 2 所涉及的解密装置，是根据上述实施方式 1 中说明的文件格式输入加密的文件，输出解密后的文件的装置，由于很多方面与上述实施方式 1 说明的加密装置是相同的，故主要以有差异的部分为中心进行说明。

图 13 为显示本实施方式 2 的解密装置的功能构成的框图。

如图 13 中所示，解密装置 200 包括：文件读出部 201、标题解析部 202、数据结构保持部 203、标题变换部 204、文件输出部 205 及数据解密部 206。

文件读出部 201 是输入上述实施方式 1 所涉及的加密装置 100 生成的文件（加密完成的文件）的处理部，根据标题解析部 202 的指示，读入加密完成文件，将文件的标题部（“moov`”）输出给标题解析部 202。

标题解析部 202 是解析“moov`”的处理部，将“moov`”中所包含的各条目的 EINFO`输出给标题变换部 204，并将存放在加密完成文件中的图像、声音、文本等数据存取信息输出给数据结构保持部 203。另外，当标题解析部 202 从标题变换部 204 取得由变换 EINFO` 所得到的 EINFO 时，生成插入了 EINFO 的“moov”，输出给文件输出部 205。标题解析部 202 还从标题变换部 204 取得对数据解密所需要的加密有无、加密方式及加密方式版本号等加密信息，并输出给数据解密部 206。

数据结构保持部 203 是用于保持数据存取信息的 DRAM 及 SDRAM 等存储器。

标题变换部 204 是判别加密的有无及编码方式，以将 EINFO`变换成 EINFO 的处理部，具有变换时参照的变换表，从标题解析部 202 取得 EINFO`，并根据变换表变换成 EINFO 后，将 EINFO 输出给标题解析部 202。

数据解密部 206 是对数据的加密进行解除（解密）的处理部，从文件读出部 201 取得加密完成的 mdat，利用从标题解析部 202 所输出的加密信息和在数据结构保持部 203 中所保持的数据存取信息，对数据进行解密，并将解密了的数据部（mdat）输出给文件输出部 205。

文件输出部 205 是从标题解析部 202 取得“moov”，从数据解密部 206 取得 mdat，将这些一体化后输出解密完成文件，即未加密文件的处理部。

下面，对标题变换部 204 的具体动作例进行说明。在此，与上述实施方式 1 一样，假设利用图 6（a）中所示的变换表进行，在条目类型中描述为 ep4v。

图 14 是表示标题变换部 204 的处理动作的第 1 例的流程图。

首先，标题变换部 204 取得从标题解析部 202 所输出的 EINFO`（S302）。

然后，标题变换部 204 读出 EINFO`中所包含的 ENT_TP（S304），判断 ENT_TP 的前头字节 ENT_TP[O]是否是 0x65（S306）。

在此，如果不是 0x65（S306 的否），则说明有关该信道的图像数据已经进行了解密，或者未加密，不必变更 EINFO`的值，所以可以省略从步骤 S308 到步骤 S312 的处理。在本实施方式 2 中，将 ENT_TP 的前头字节是否是 0x65 作为加密有无的判断基准。

另一方面，当是 0x65 时（S306 的是），标题变换部 204 从变换表 A104a 中检索 ENT_TP 中描述的值（S308）。在图 6（a）中，变换表 A104a 至少具有 0～3 四个备选，这些值当用 ASCII 码表示时，分别为：#0 条目为 ep4v、#1 条目为 ep4a、#2 条目为 e263、#3 条目为 eamr。这些值分别是将在 ISO/MPEG 及 3GPP 规格中规定的表示编码方式的规定值的前头字节变换成 0x65(ASCII 码表示 e)所得到的。

标题变换部 204 根据步骤 S308 中的检索结果，判断是否检索出了一致的值（S310）。在此，由于 ENT_TP 的值是 ep4v，所以标题变换部 304 判断与变换表 A104a 的#0 条目一致（S310 的是）。当未检索出一致时（S310 的否），则标题变换部 104 原样保持在 ENT_TP 中描述的值，进入步骤 S314。

然后，标题变换部 104 将 ENT_TP 的值置换成与变换表 B104b 中相同的#0 条目的值 0x6D703476（“mp4v”）（S312）。

最后，如上所述将变换了 ENT_TP 值的 EINFO 输出到标题解析部 202，结束处理动作（S314）。

如上述实施方式中说明的那样，采用预约字段描述加密方式及其版本号时，在图 14 中所示的流程图的步骤 S312 中，将 ENT_TP 置换成变换表 B104b 的值后，将 SC_TYPE 及 SC_VER 的字段设置为 0，将 EINFO 输出给标题解析部 202。这是因为 SC_TYPE 及 SC_VER 在未加密文件中不设定的缘故。

另外，如上述实施方式中所述，当为了采用位翻转表示编码方式、加密有无、加密方式、及其版本号等而变换 EINFO 时，标题变换部 204 进行以下操作。

图 15 是表示标题变换部 204 的处理动作的第 2 例的流程图。此处与上述的情况一样，假设在 ENT_TP 中描述为 ep4v，按加密方式 1 进行数据的加密。

首先，标题变换部 204 输入从标题解析部 202 输出的 EINFO`（S402）。

然后，标题变换部 204 读出 EINFO`中所包含的 ENT_TP（S404）。

接着，标题变换部 204 将在 ENT_TP 中描述的表示编码方式及加密方式的值，应用在位翻转表 104g 中所记录的各位翻转式上，检算再位翻转后的值是否是表示编码方式的值（S406），对于利用各位翻转式算出的再位翻转后的值，判断是否有与表示编码方式的值一致的值（S408）。此处，由于 ENT_TP 的值是 ep4v，由加密方式 1 进行的数据加密，所以标题变换部 204 判断通过位翻转表 104g 的位翻转式^A 进行再位翻转的值，与 mp4v 一致（S408 的是）。当判断没有一致的值时（S408 的否），标题变换部 204 原样保持 ENT_TP 中所描述的值，进入步骤 S414。

再接着，标题变换部 204 根据由位翻转表 104g 所设定的位翻转式，使 ENT_TP 的值进行再位翻转（S410）。在此，标题变换部 204 从位翻转表 104g 中采用位翻转式^A，使 ENT_TP 的值进行再位翻转。

然后，标题变换部 204 将 ENT_TP 的值置换成位翻转后的值（此处为 mp4v）（S412），最后，将变换了 ENT_TP 值的 EINFO 输出到标题解析部 202，处理动作结束（S414）

在图 15 中所示的步骤 S406 及步骤 S408 中，标题变换部 204 也

可以进行以下的检算及判断。此处，假设未加密时的 ENT_TP 是以 ASCII 码可以表示的范围的值进行描述的，加密方式是在^A（=ff000000）、^A`（=ffff0000）及^A"（=ffff00ff）的位翻转式所确定的 3 种中，使用^A 的加密方式。

当在未加密时的 ENT_TP 中描述为 mp4v（0x6D703476）时，在加密时的 ENT_TP 中，作为 mp4v 通过^A（=ff000000）的位翻转式进行翻转的结果，描述成？p4v（0x92703476）。此处“？”表示 ASCII 码不能表示的代码。

标题变换部 204，当读出 EINFO`中所包含的 ENT_TP 时，在步骤 S406 中，将“？p4v”（0x92703476）分别应用到上述 3 种位翻转式进行检算时，则可得到对^A（=ff000000）为 mp4v（0x6D703476）、对^A`（=ffff0000）为 m?4v（0x6D8F3476）、而对^A"（=ffff00ff）为 m?4?（0x6D8F3489）的值。

即，标题变换部 204，以未加密时的 ENT_TP 可以用 ASCII 码表示的范围的值描述为前提，在步骤 S408 中，^A`及^A"的检算结果，剩有不能用 ASCII 表示的代码，而只是^A 的检算结果用 ASCII 表示，所以判断为用^A 的加密方式进行了加密。

这样，根据本实施方式 2 所涉及的解密装置，可以使解密前及解密后的文件大小相同，与上述实施方式 1 一样，与现有的解密装置相比，可以削减标题的处理量，即使是对光盘上的文件进行解密时，也可以得到不必变更数据记录位置等的效果。

（实施方式 3）

下面，采用图 16 及图 17，对本发明实施方式 3 所涉及的数据重放装置进行说明。

该数据重放装置是根据上述实施方式 1 及 2 说明的文件格式输入文件，并加密的情况下，对数据进行解密，以解码，并对数据重放输出的装置。

图 16 是表示本实施方式 3 所涉及的数据重放装置功能构成的方框图。

如图 16 中所示，数据重放装置 300 包括：文件读出部 301、标

题解析部 302、数据结构保持部 303、加密判断部 304、SW（开关）305、数据解密部 306、数据解码部 307 及数据重放部 308。本图中所示的数据重放装置 300 是在图 13 中所示的实施方式 2 所涉及的解密装置 200 的功能方框图中，附加 SW 305、数据解码部 309 及数据重放部 308，并将标题变换部 204 置换成加密判断部 304 的装置，到解密位置的基本处理动作与上述实施方式 2 所涉及的解密装置 200 的处理动作相类似。

另外，该数据重放装置 300 无论文件是否已经加密，都可以对输入的文件进行解码/重放。即，当通过加密判断部 304 检测出加密时，连接 SW 305 的 S1 和 S2，通过数据解密部 306 进行解密后，将“mdat”输出给数据解码部 307，另一方面，当通过加密判断部 304 未检测出加密时，连接 SW 305 的 S1 和 S3，不使用数据解密部 306，直接将“mdat”输出到数据解码部 307。

加密判断部 304 是判别加密的有无及编码方式等的处理部，通过从标题解析部 302 取得 EINFO 或 EINFO`，判断所输入的文件是已加密完成的文件还是未加密文件。而且，如果是加密完成文件，则加密判断部 304 将使 S1 和 S2 连接的连接信号输出给 SW 305，并且将指示数据解密的解密指示信号输出给数据解密部 306。另一方面，如果是未加密文件，则加密判断部 304 将使 S1 和 S3 连接的连接信号输出给 SW 305。加密判断部 304 在输出解密指示信号时，还将加密方式等加密信息也一起输出到数据解密部 306。

SW 305 是根据来自加密判断部 304 的连接信号而动作的开关。

数据解码部 307 是对编码数据进行解码的处理部，取得已解密完成的 mdat，对由规定的编码方式编码的 mdat 进行解码，将已解码完成的数据输出给数据重放部 308。

数据重放部 308 是对解码完成的数据进行重放，以输出给显示装置的处理部。

加密判断部 304 的具体动作如图 17 的流程图所示。该流程图与图 14 中所示的表示解密装置 200 的标题变换部 204 动作的流程图大体相同，只是增加了步骤 S514 及步骤 S518 这一点不同。步骤 S514

为，在是加密了的数据的情况下，加密判断部 304 输出使 SW 305 的 S1 和 S2 连接的连接信号的步骤，而步骤 S518 为，在是未加密数据的情况下，加密判断部 304 输出使 SW 305 的 S1 和 S3 连接的连接信号的步骤。

另外，虽然在图 17 的流程图中未示出，但是加密判断部 304 也可以判断作为与 ENT_TP 相邻的数据字段的表示加密方式的 SC_TYPE、及表示加密方式版本号的 SC_VER，并判断是否对应于所指定的加密方式。

另外，加密判断部 304，也可以在图 15 中所示的表示解密装置 200 的标题变换部 204 的动作的流程图中，进行使图 17 的流程图中的步骤 S514 和步骤 S518 相组合的处理动作，并通过位翻转，对编码方式、加密有无、加密方式及加密方式的版本号等所表示的文件进行解密，并进行解码以重放。

（应用例）

在此，参照图 18 对本发明所涉及的加密装置、解密装置及数据重放装置的应用例进行说明。

图 18 是表示本发明所涉及的加密装置、解密装置及数据重放装置的应用例的图。

本发明所涉及的加密装置、解密装置及数据重放装置，通过因特网等通信网络 402，应用于接收从提供动态图像数据等内容的内容服务器 401 发送的 MP4 文件等的手提电话机 403、个人计算机 404 及 PDA 405 等。而且，这些手提电话机 403、个人计算机 404 及 PDA 405，对接收到的 MP4 文件进行加密后，记录在存储卡 406 及 DVD-RAM 407 等记录媒体中，以及从存储卡 408 等记录媒体读出并重放加密后的 MP4 文件。

这样，本发明所涉及的加密装置、解密装置及数据重放装置，在图像发送系统等中，可以作为对 MP4 文件加密以进行记录、或解密以进行重放的 MP4 文件记录装置或重放装置使用。

以上，基于各实施方式对本发明所涉及的加密装置、解密装置及数据重放装置进行了说明，但是本发明并不限于这些实施方式等。

例如，在上述各实施方式中，着眼于包含一个数据的信道进行了说明，但是也可以在文件中对多个信道（分别包括图像、声音、文字等）进行多路，这时，标题变换部 104、204、及加密部 106、解密部 206、306，可以对各信道进行个别动作。

另外，在上述各实施方式中，对采用标题部和数据部形成一体的文件进行了说明，但是也可以是标题部和数据部分离后的各自不同的文件。

另外，上述各实施方式对以硬件构成的例子进行了说明，但是也可以使处理的一部分或全部通过在 CPU 及 DSP 等平台上操作的软件程序进行动作。另外，上述软件程序也可以记录在软盘、CD-ROM 及存储卡等上携带，在各种装置上起动软件程序，执行基于这些实施方式的动作。

另外，在上述实施方式 1 中，是以 ENT_TP 的前头字节为加密的有无的判断基准，但是这只不过是一个例子，也可以考虑各种方法。不过，关于方法，需要在加密文件格式的规格中预先确定。例如，既可以变换前头字节以外的字节，也可以对 2 个以上的字节进行变换，只要适当考虑的变换规定进行了标准化，就可以在 ENT_TP 中保持编码方式的信息，并可以判断加密的有无。这样，通过预先确定规则，与现有的文件格式相比，可以容易地应对新的数据类型。在现有的文件格式中，只能应对在图像、声音及 MPEG4 系统所规定的 3 个系统数据，但是如果使用根据预先确定的规则变换表示编码方式的 ENT_TP 的方法，则也可以容易适用于 3GPP 规定的文本编码方式（对于 tx3g，例如以 ex3g 表示加密）。

另外，在上述各实施例中将输入文件作为 ISO/MPEG4 的文件格式（MP4 文件）进行了说明，但是也可以适用于其他的文件格式。

本发明产业上利用的可能性在于，本发明所涉及的加密装置、解密装置及数据重放装置，可以很好地用于取得存放了视频数据及音频数据等媒体数据的 MP4 文件，加密后存放在记录媒体中，或对存放了加密的视频数据及音频数据等媒体数据的 MP4 文件进行解密重放的带有动态图像重放功能的手提电话机及个人计算机等。

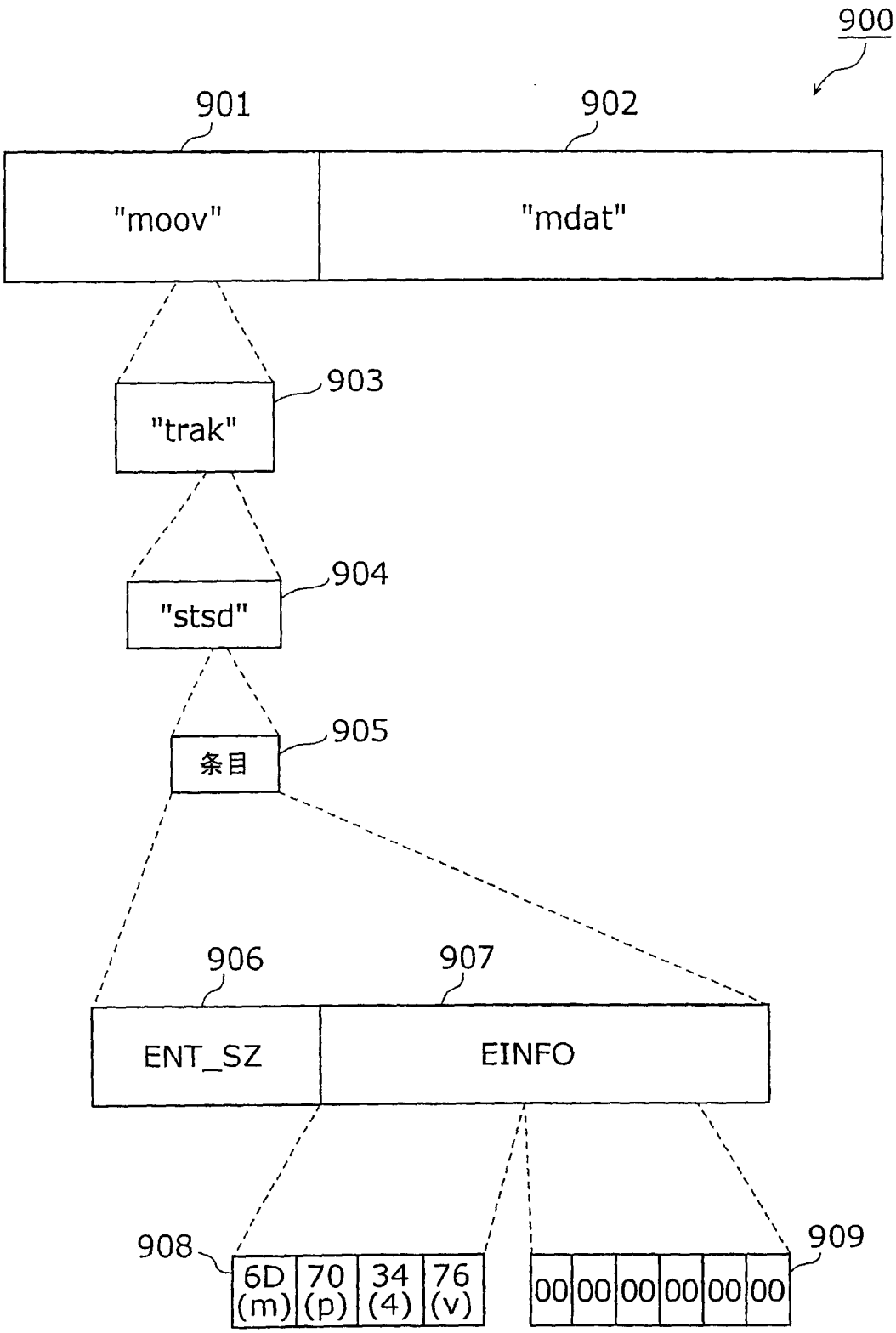

900
901
902
"moov"
"mdat"
903
"trak"
904
"stsd"
905
条目
906
907
ENT_SZ
EINFO
908
6D (m)
70 (p)
34 (4)
76 (v)
909
00 00 00 00 00 00

图1

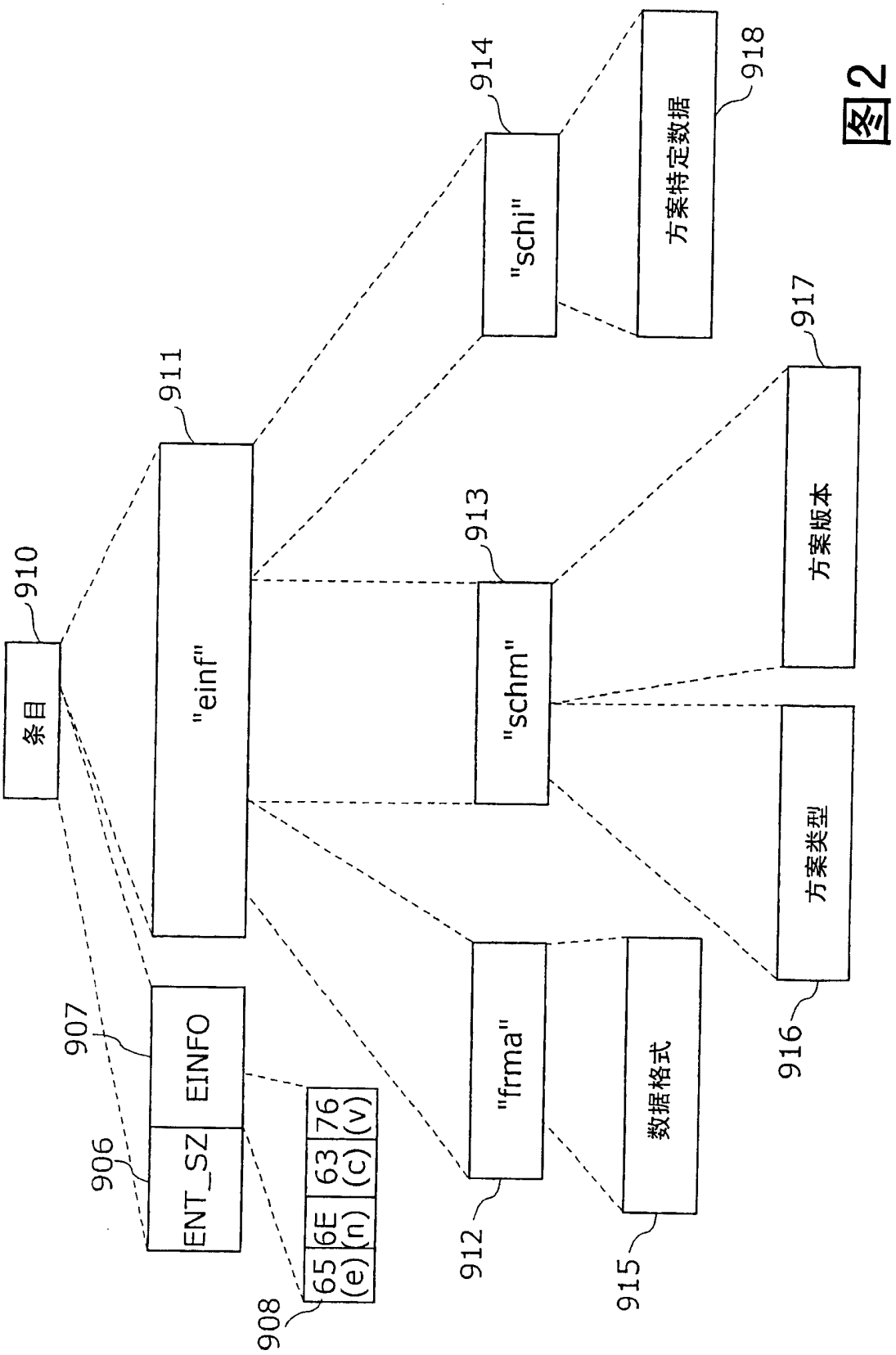

910
条目
911
"einf"
907
EINFO
906
ENT_SZ
908
65 (e)
6E (n)
63 (c)
76 (v)
914
"schi"
918
方案特定数据
913
"schm"
917
方案版本
912
"frma"
915
数据格式
916
方案类型

图2

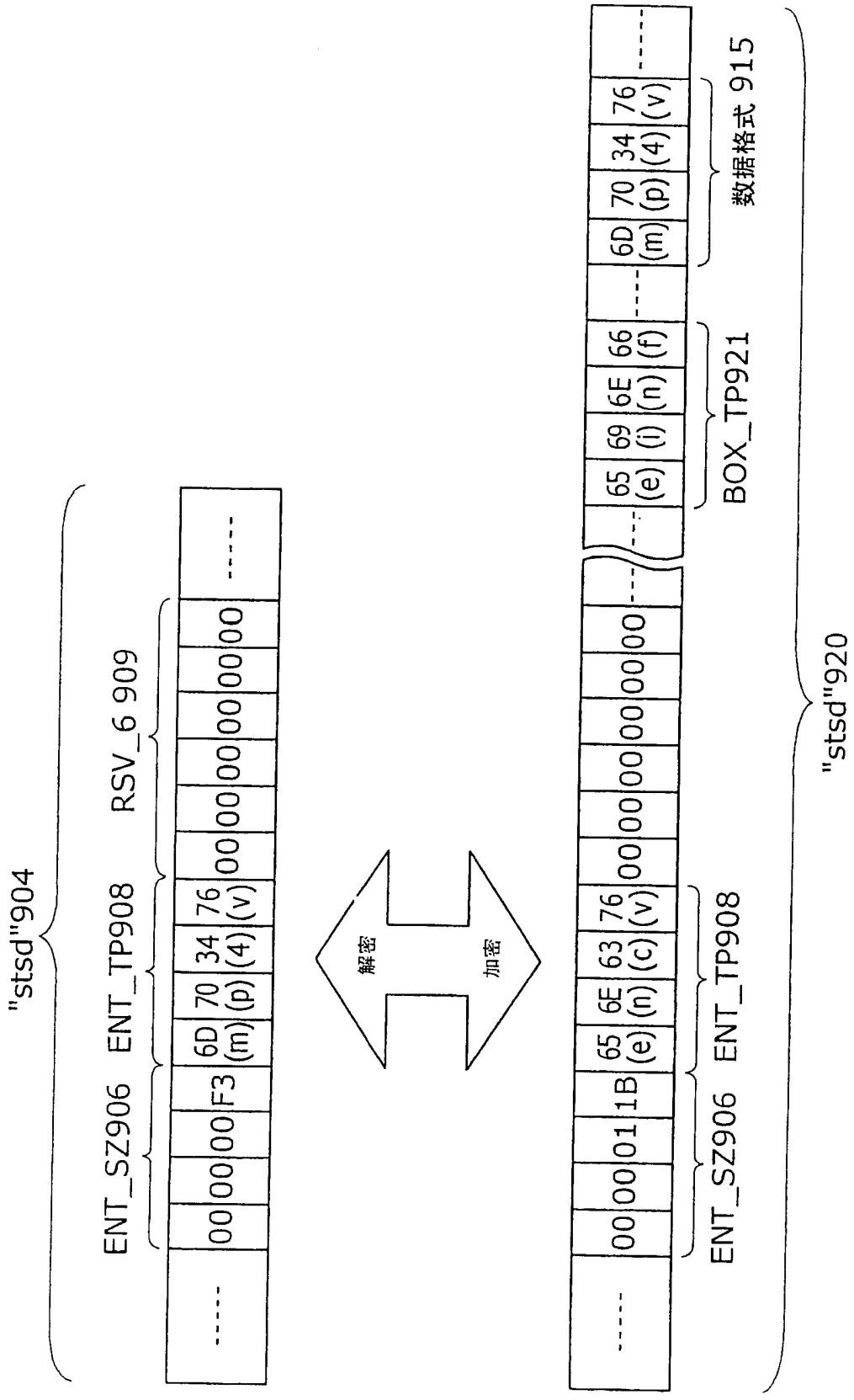

"stsd"904
ENT_SZ906
ENT_TP908
RSV_6 909
00 00 00 F3 6D(m) 70(p) 34(4) 76(v) 00 00 00 00 00 -----
解密
加密
"stsd"920
ENT_SZ906
ENT_TP908
BOX_TP921
数据格式 915
00 00 01 1B 65(e) 6E(n) 63(c) 76(v) 00 00 00 00 00 00 ---- 65(e) 69(i) 6E(n) 66(f) ---- 6D(m) 70(p) 34(4) 76(v) -----

图3

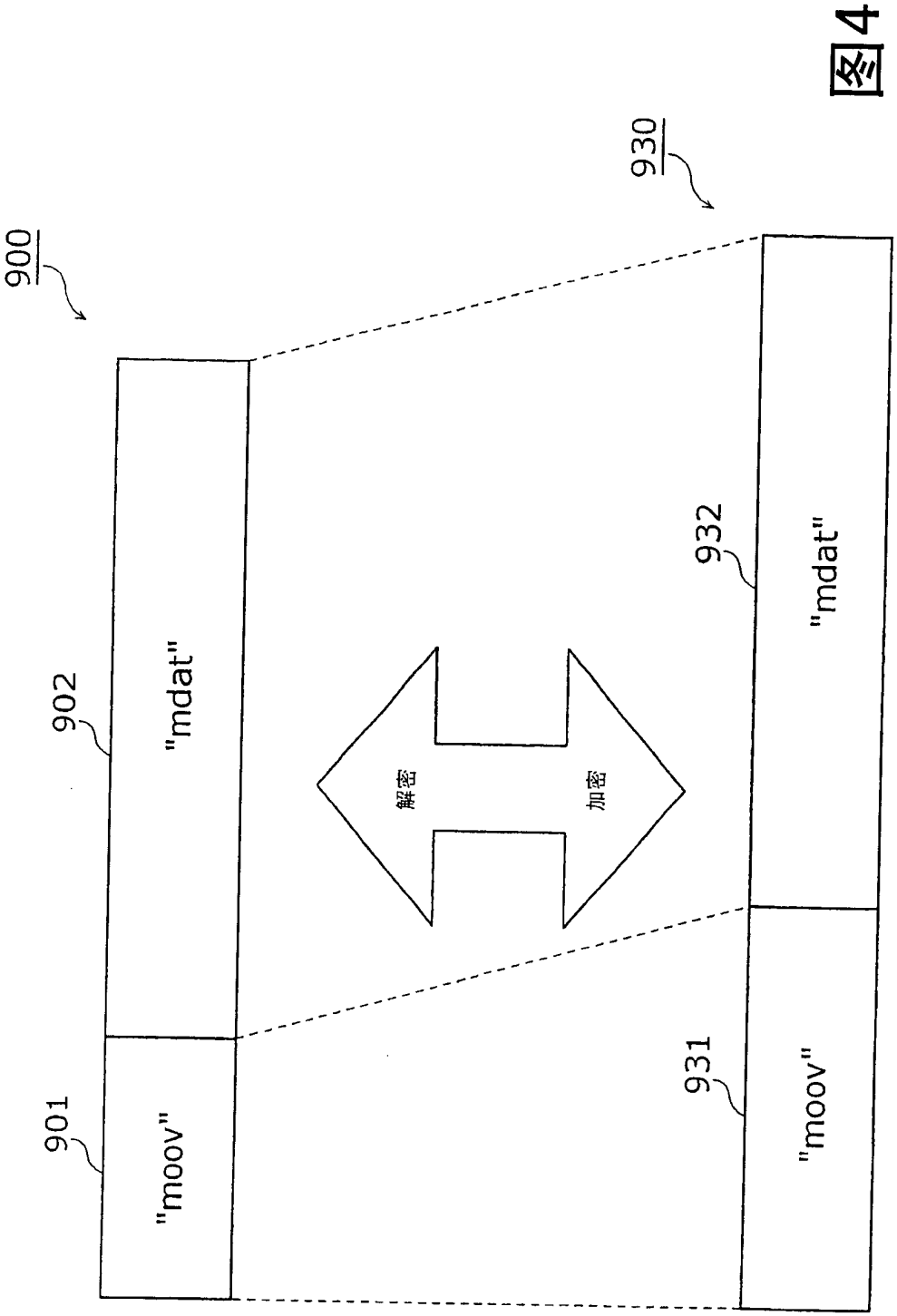


图4

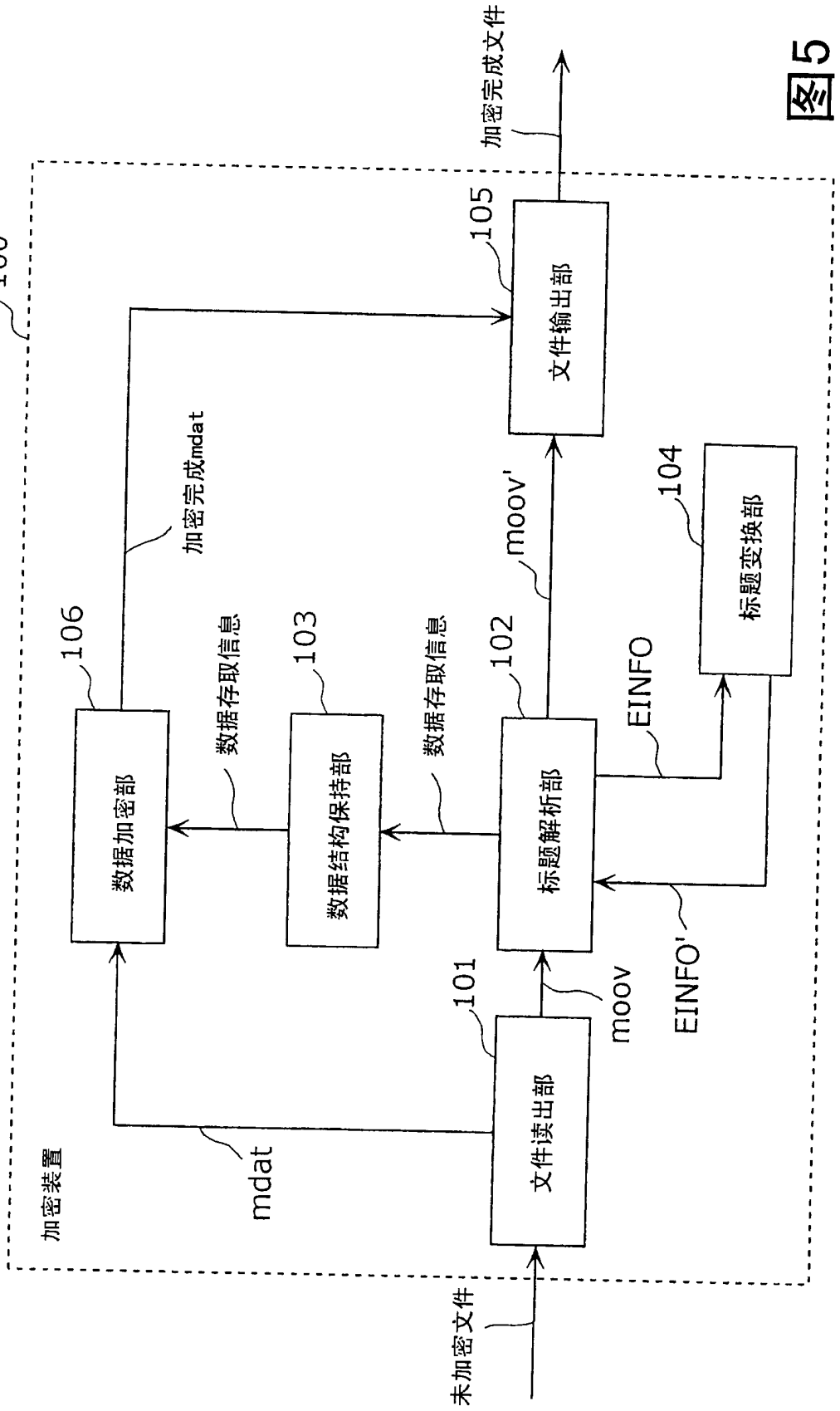

加密完成文件
100
105
文件输出部
加密完成mdat
106
数据加密部
数据存取信息
103
数据结构保持部
数据存取信息
102
moov'
104
标题变换部
EINFO
标题解析部
加密装置
mdat
101
文件读出部
moov
EINFO'
未加密文件

图5

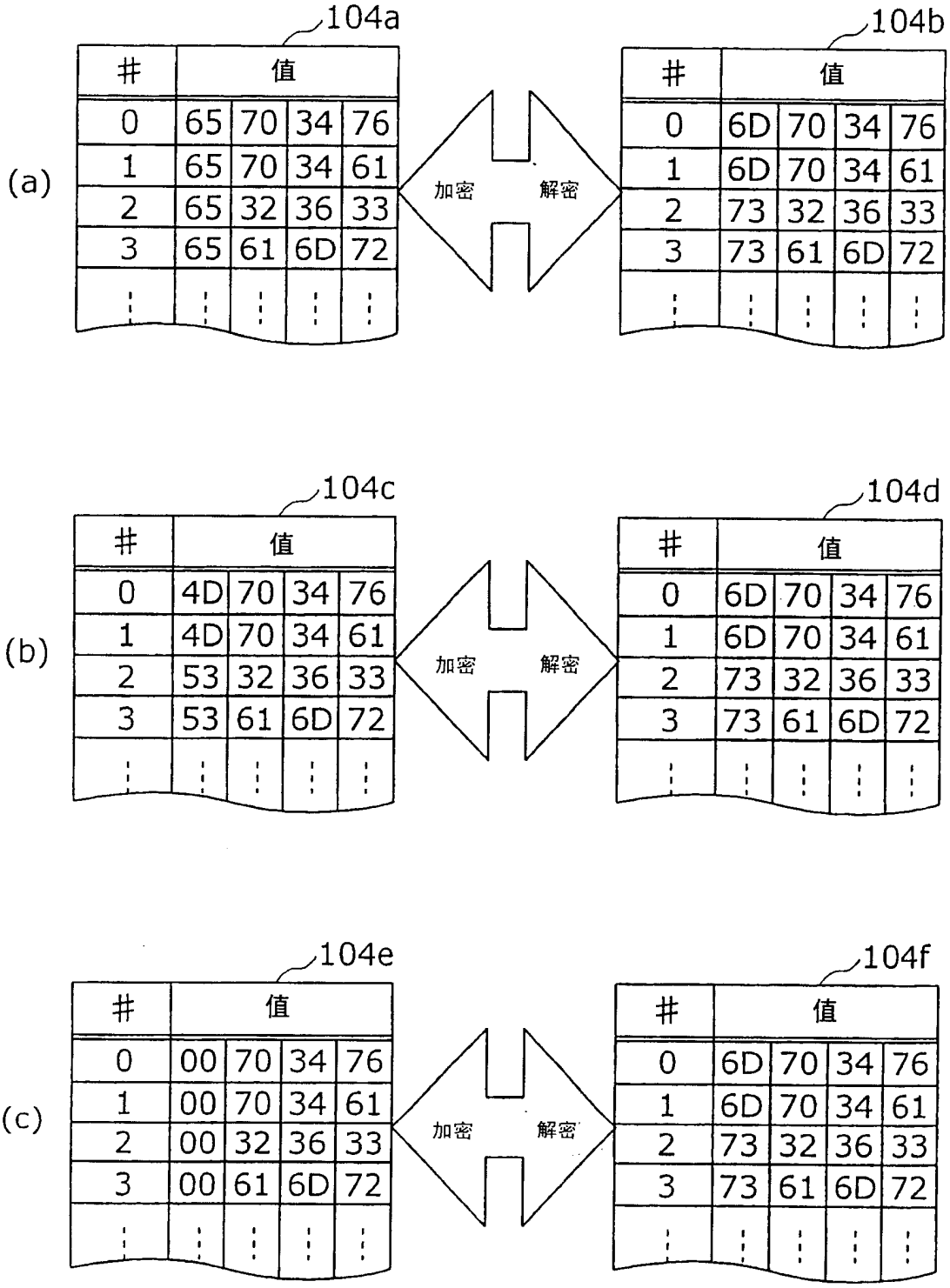

(a)
104a
#
值
0 65 70 34 76
1 65 70 34 61
2 65 32 36 33
3 65 61 6D 72
加密
解密
104b
#
值
0 6D 70 34 76
1 6D 70 34 61
2 73 32 36 33
3 73 61 6D 72
(b)
104c
#
值
0 4D 70 34 76
1 4D 70 34 61
2 53 32 36 33
3 53 61 6D 72
加密
解密
104d
#
值
0 6D 70 34 76
1 6D 70 34 61
2 73 32 36 33
3 73 61 6D 72
(c)
104e
#
值
0 00 70 34 76
1 00 70 34 61
2 00 32 36 33
3 00 61 6D 72
加密
解密
104f
#
值
0 6D 70 34 76
1 6D 70 34 61
2 73 32 36 33
3 73 61 6D 72

图6

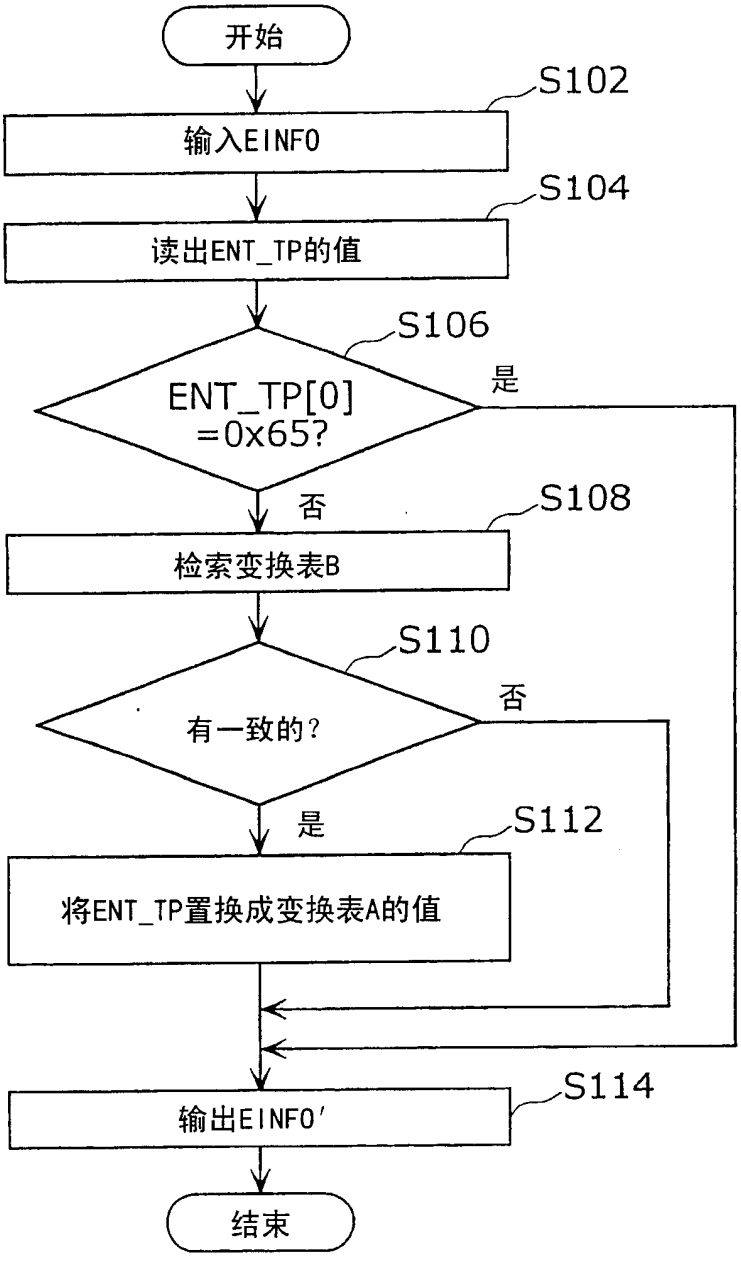

开始
S102
输入EINFO
S104
读出ENT_TP的值
S106
ENT_TP[0]
=0x65?
是
否
S108
检索变换表B
S110
有一致的?
否
是
S112
将ENT_TP置换成变换表A的值
S114
输出EINFO'
结束

图7

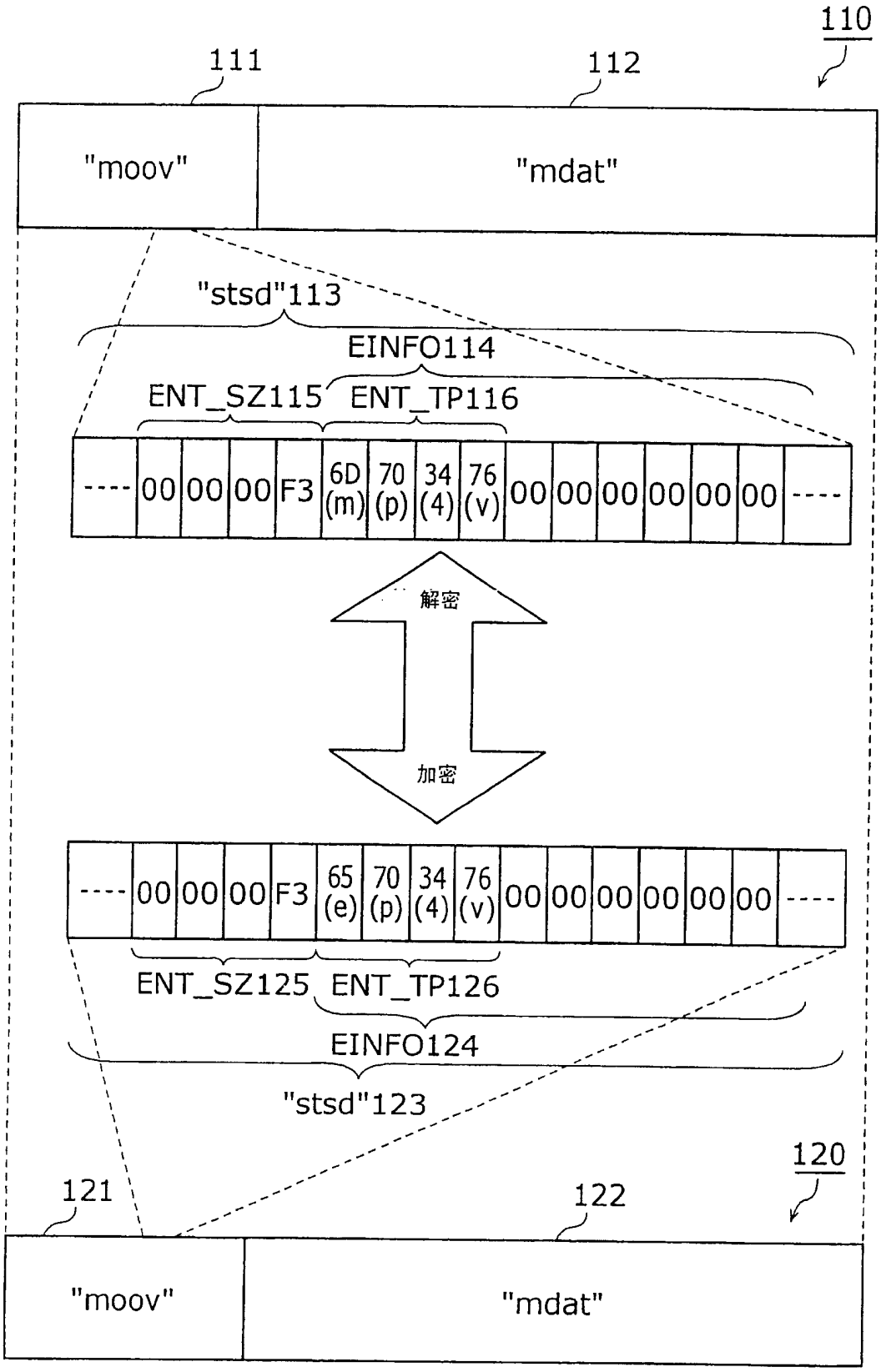

110
111
112
"moov"
"mdat"
"stsd"113
EINFO114
ENT_SZ115
ENT_TP116
---- 00 00 00 F3 6D (m) 70 (p) 34 (4) 76 (v) 00 00 00 00 00 00 ----
解密
加密
---- 00 00 00 F3 65 (e) 70 (p) 34 (4) 76 (v) 00 00 00 00 00 00 ----
ENT_SZ125
ENT_TP126
EINFO124
"stsd"123
120
121
122
"moov"
"mdat"

图8

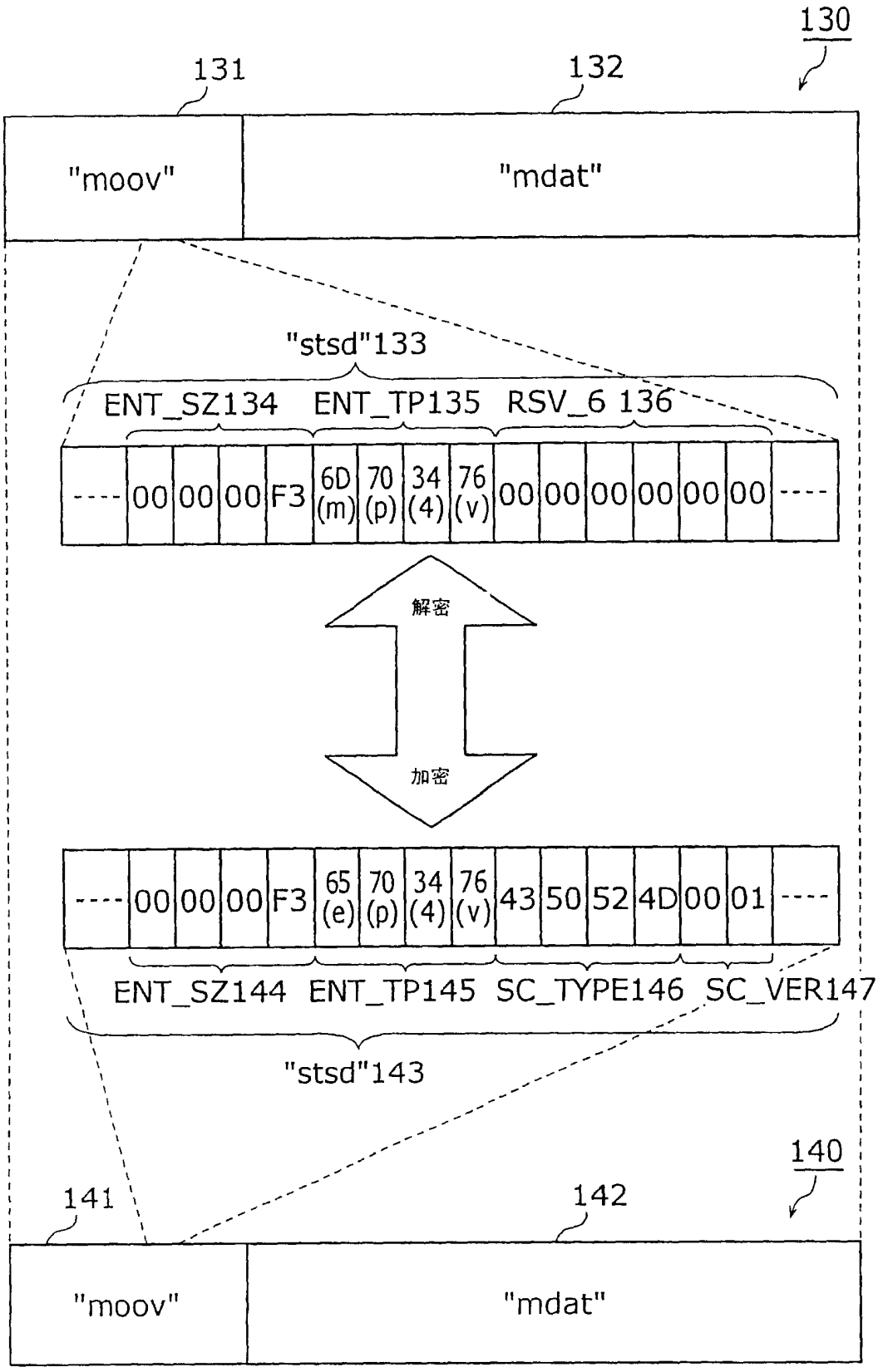

130
131
132
"moov"
"mdat"
"stsd"133
ENT_SZ134 ENT_TP135 RSV_6 136
---- 00 00 00 F3 6D (m) 70 (p) 34 (4) 76 (v) 00 00 00 00 00 00 ----
解密
加密
---- 00 00 00 F3 65 (e) 70 (p) 34 (4) 76 (v) 43 50 52 4D 00 01 ----
ENT_SZ144 ENT_TP145 SC_TYPE146 SC_VER147
"stsd"143
140
141
142
"moov"
"mdat"

图9

104g

	加密方式1	加密方式2	加密方式3	
mp4v	^A	^A'	^A"	---
samr	^B	^B'	^B"	---
mp4a	^C	^C'	^C"	---
⋮	⋮	⋮	⋮	---

图10

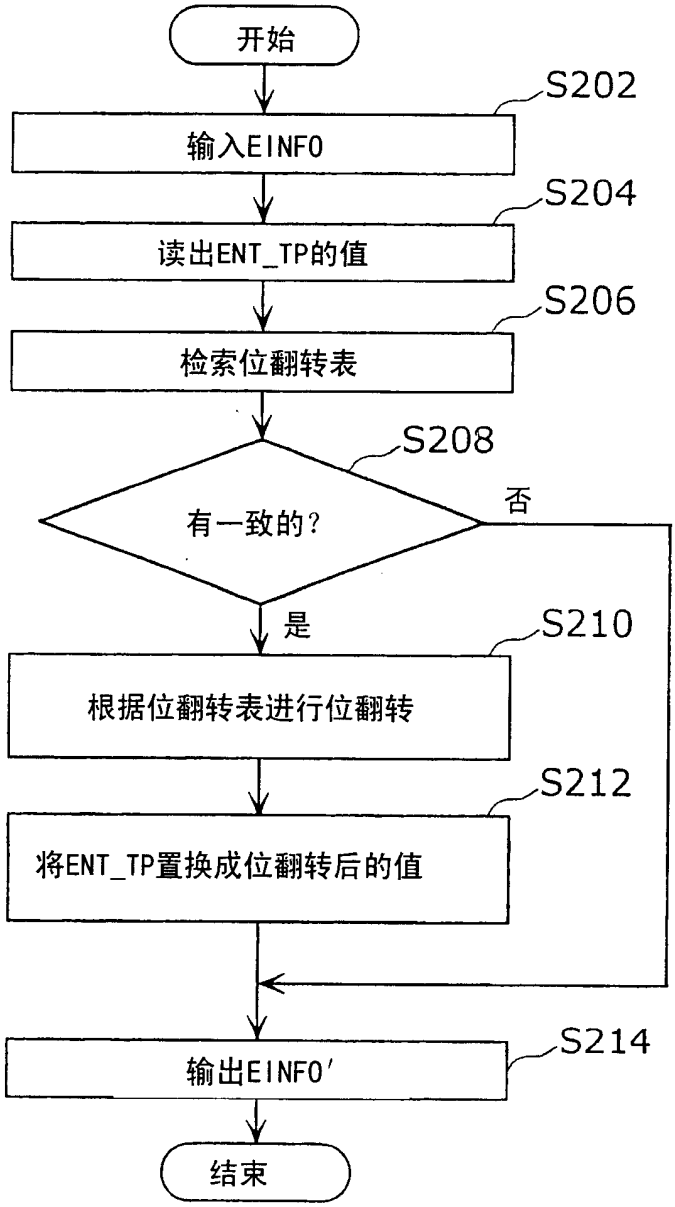
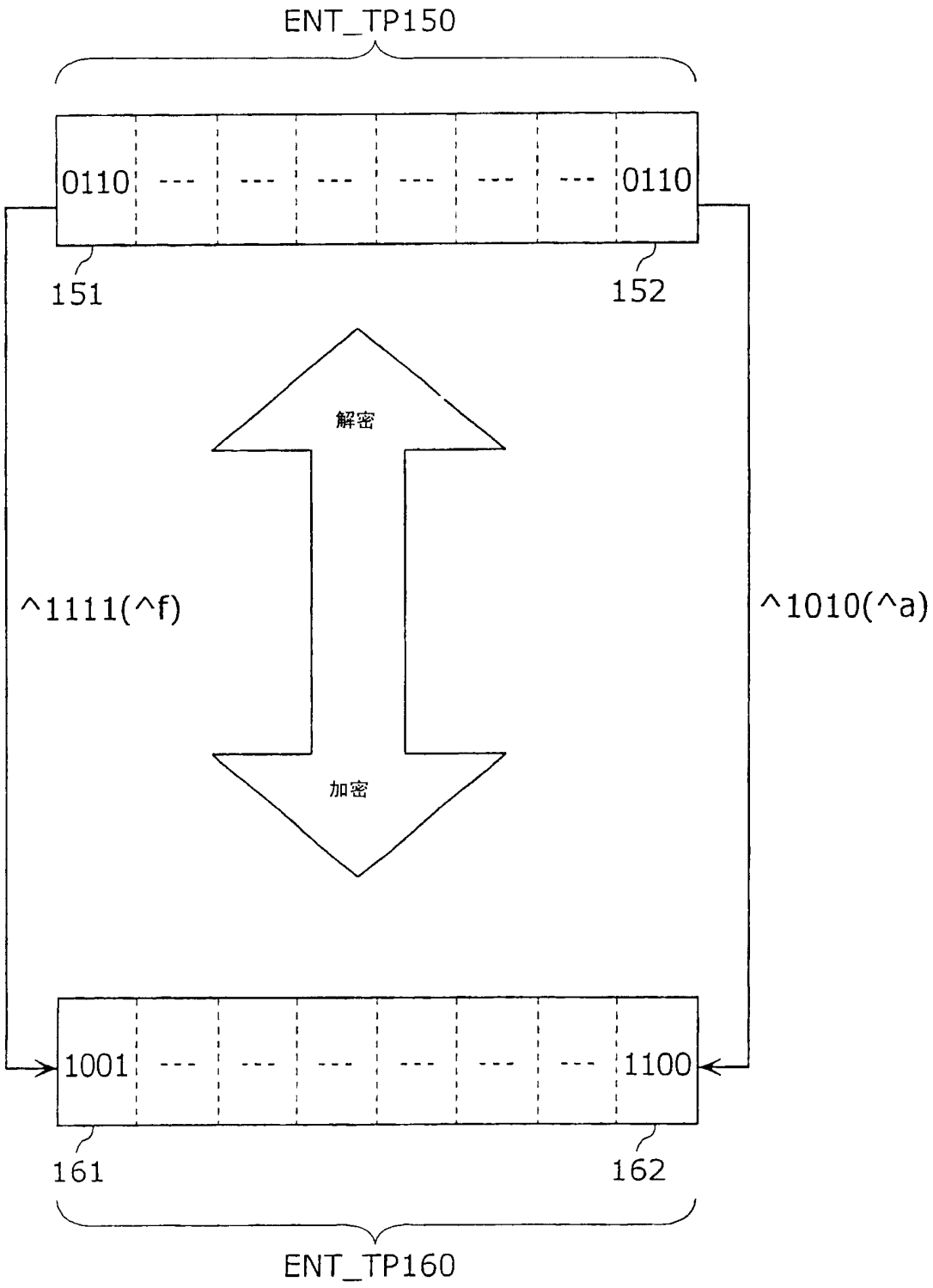

开始
S202
输入EINFO
S204
读出ENT_TP的值
S206
检索位翻转表
S208
有一致的?
否
是
S210
根据位翻转表进行位翻转
S212
将ENT_TP置换成位翻转后的值
S214
输出EINFO'
结束

图11


ENT_TP150
0110

0110
151
152
解密
^1111(^f)
^1010(^a)
加密
1001

1100
161
162
ENT_TP160

图12

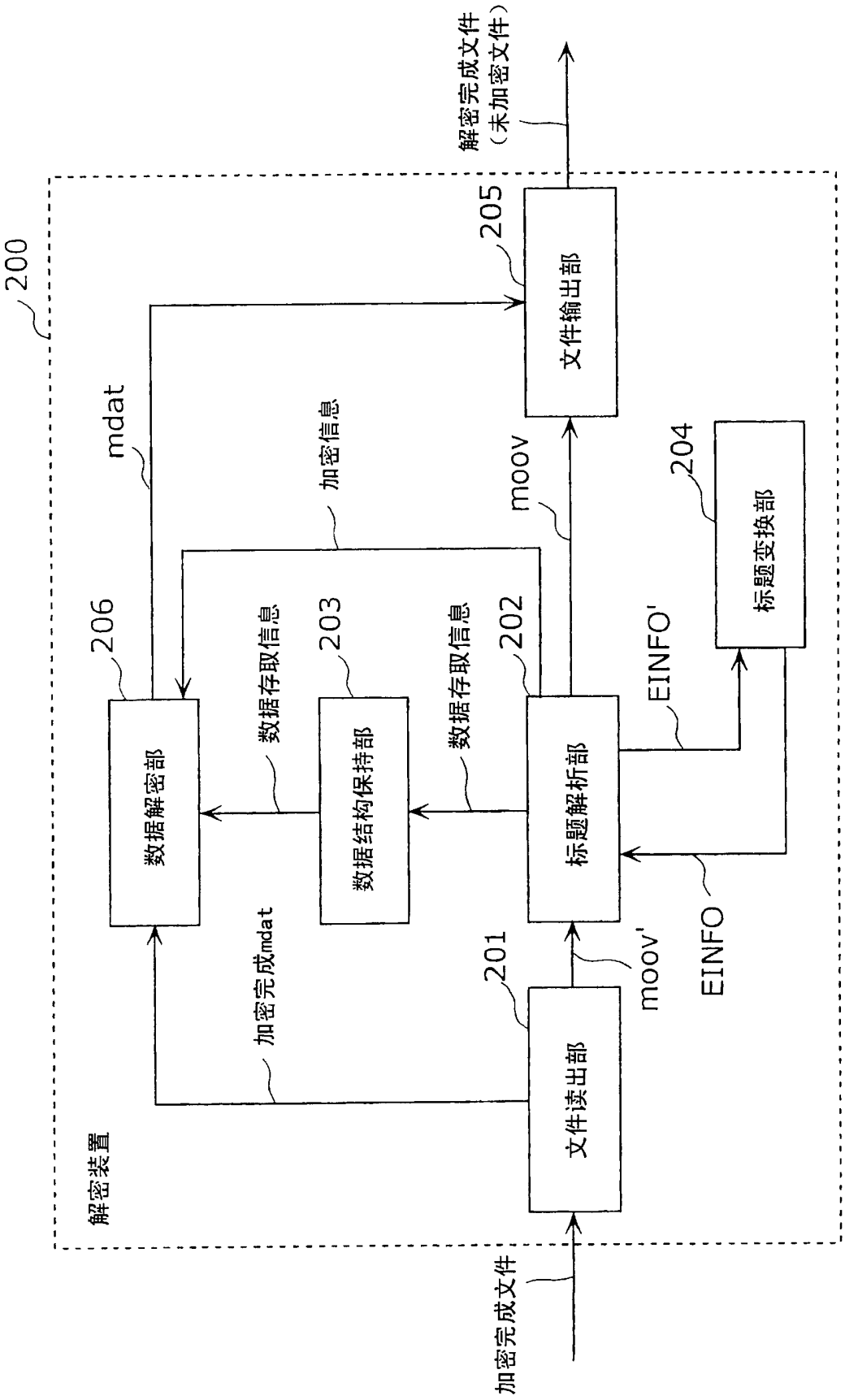

解密完成文件
（未加密文件）
200
205
文件输出部
mdat
加密信息
moov
204
标题变换部
206
数据存取信息
203
数据存取信息
202
EINFO'
数据解密部
数据结构保持部
标题解析部
加密完成mdat
201
moov'
EINFO
文件读出部
解密装置
加密完成文件

图13

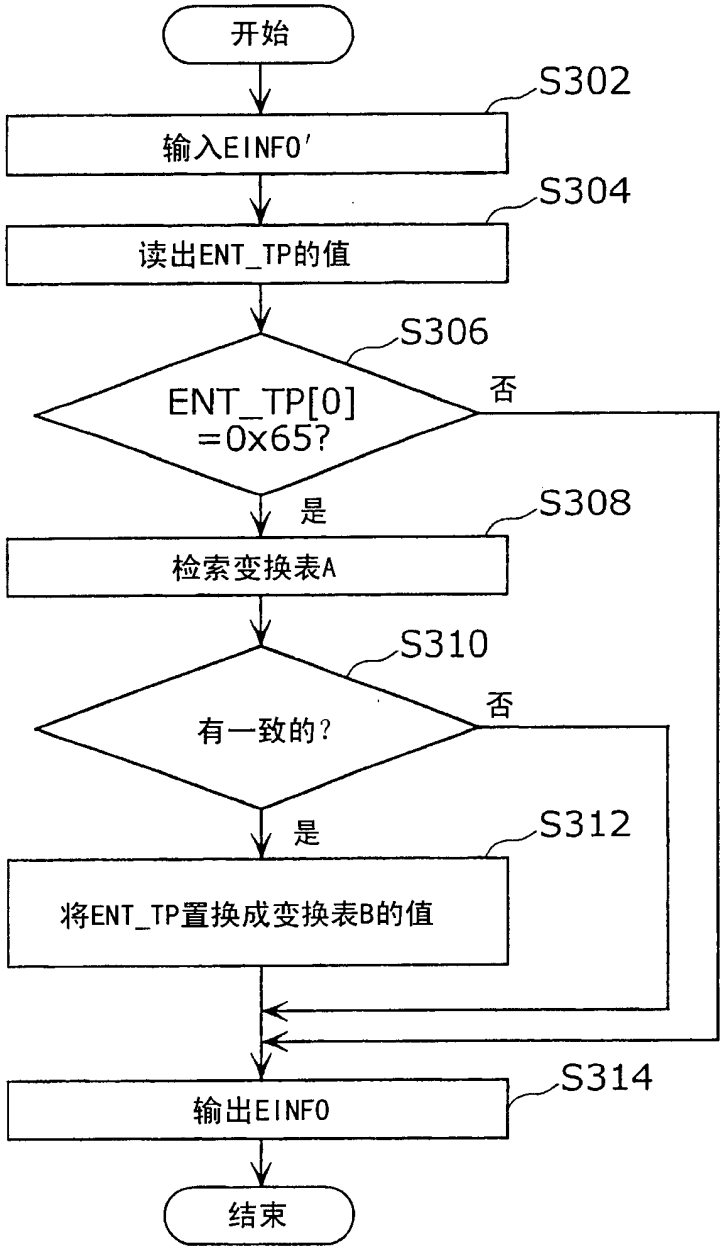

开始
S302
输入EINFO'
S304
读出ENT_TP的值
S306
ENT_TP[0]
=0x65?
否
是
S308
检索变换表A
S310
有一致的?
否
是
S312
将ENT_TP置换成变换表B的值
S314
输出EINFO
结束

图14

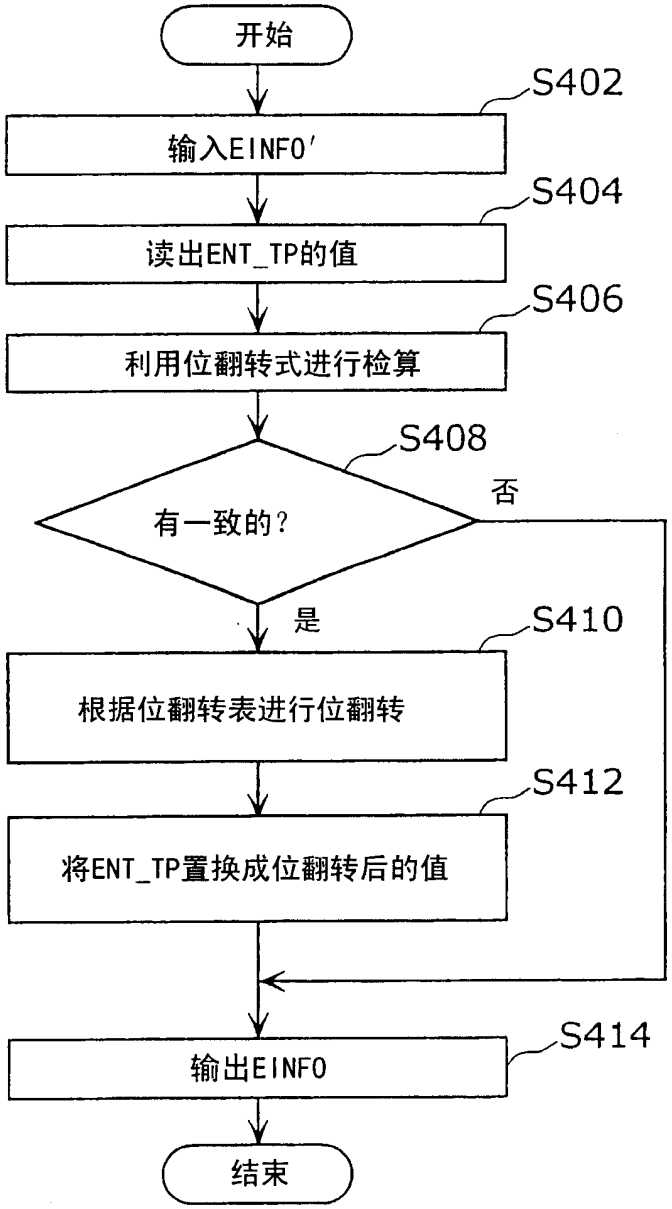

开始
S402
输入EINFO'
S404
读出ENT_TP的值
S406
利用位翻转式进行检算
S408
有一致的?
否
是
S410
根据位翻转表进行位翻转
S412
将ENT_TP置换成位翻转后的值
S414
输出EINFO
结束

图15

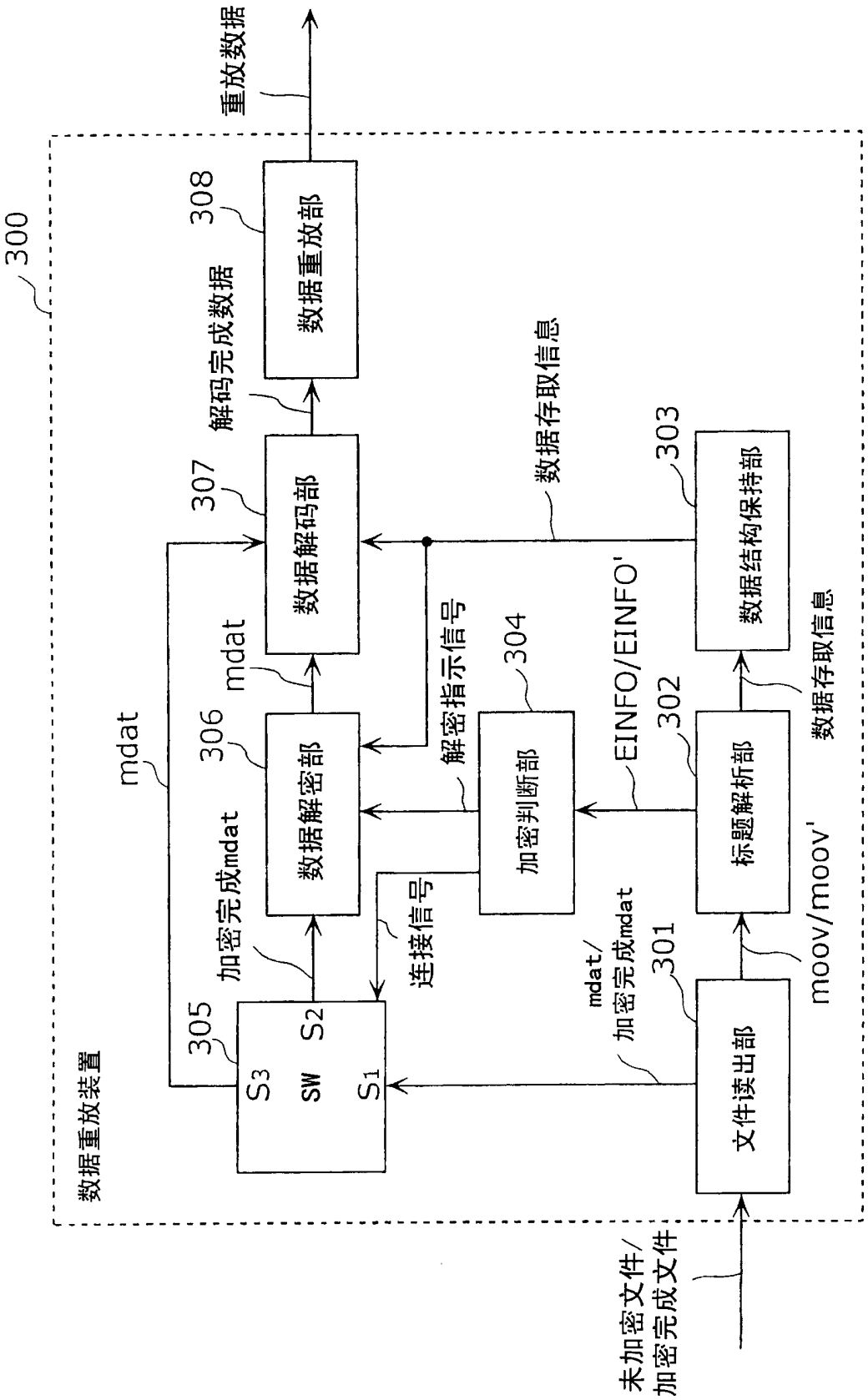

300
数据重放装置
重放数据
308
数据重放部
解码完成数据
307
数据解码部
数据存取信息
303
数据结构保持部
mdat
306
数据解密部
mdat
解密指示信号
304
加密判断部
EINFO/EINFO'
302
标题解析部
数据存取信息
加密完成mdat
305
S3
SW
S2
S1
连接信号
mdat/
加密完成mdat
301
文件读出部
moov/moov'
未加密文件/
加密完成文件

图16

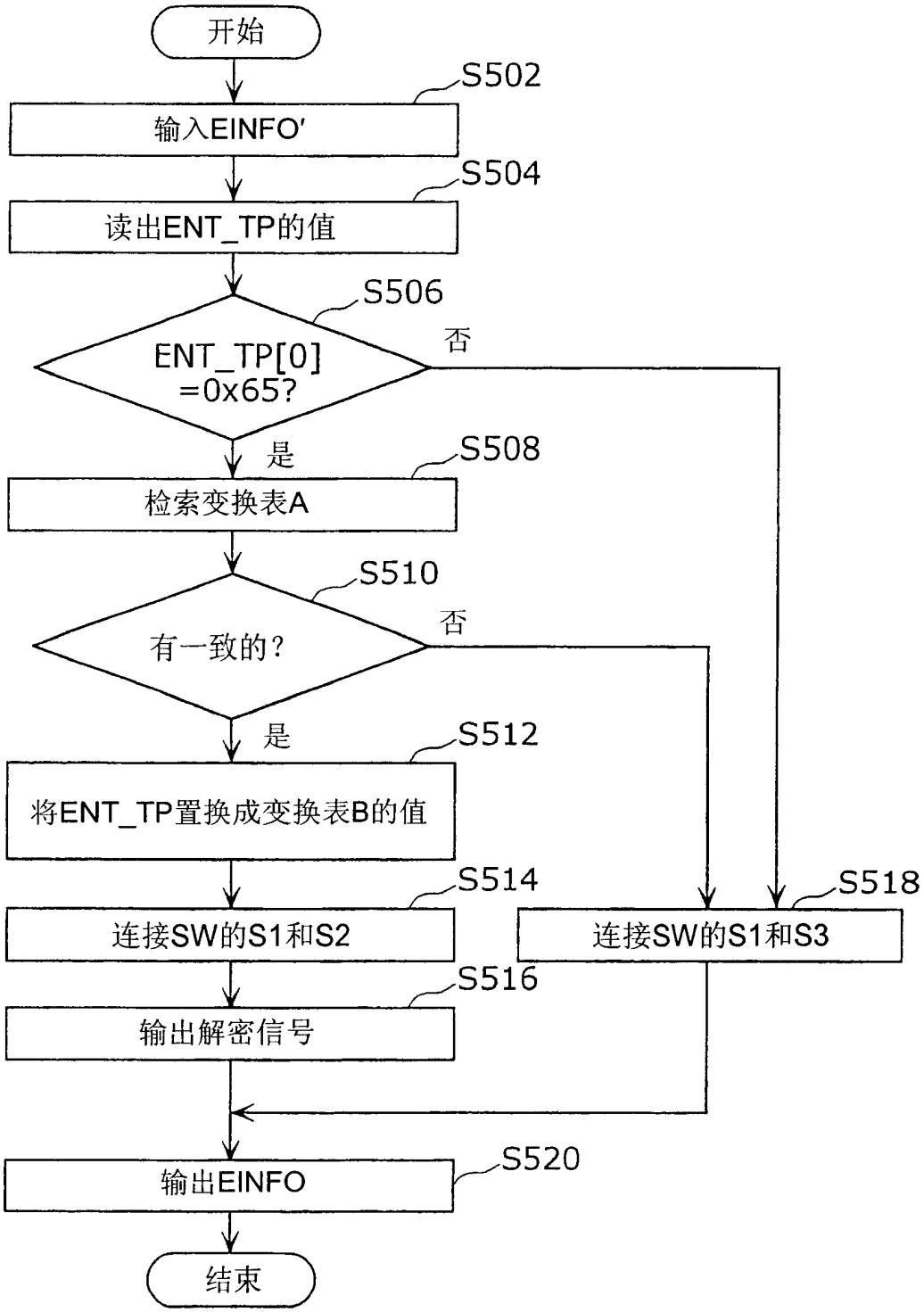

开始
S502
输入EINFO'
S504
读出ENT_TP的值
S506
ENT_TP[0]
=0x65?
否
是
S508
检索变换表A
S510
有一致的?
否
是
S512
将ENT_TP置换成变换表B的值
S514
连接SW的S1和S2
S518
连接SW的S1和S3
S516
输出解密信号
S520
输出EINFO
结束

图17

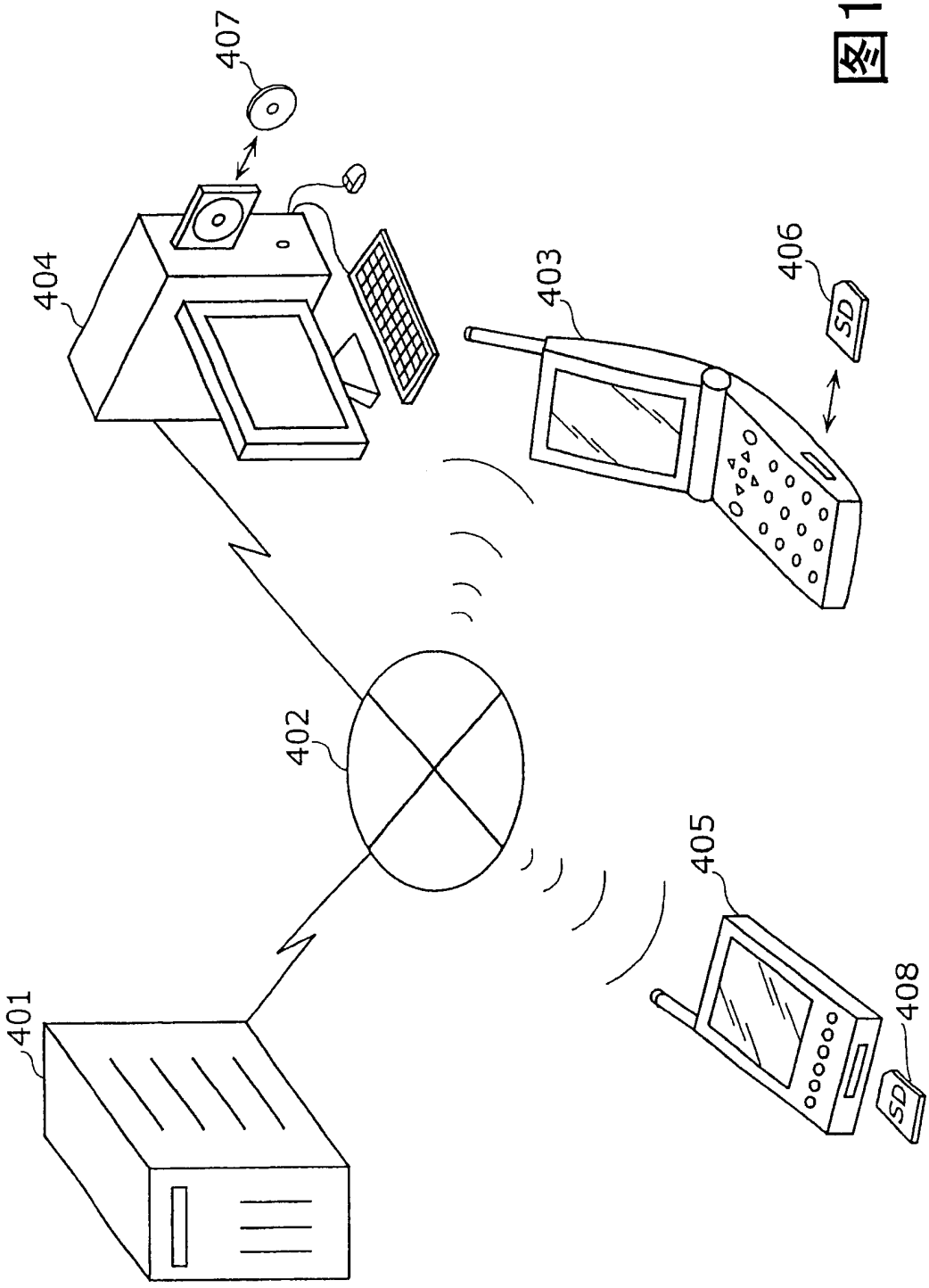


图18