[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04N 1/387

[12] 发明专利说明书

[21] ZL 专利号 97190937.7

[45] 授权公告日 2003 年 11 月 19 日

[11] 授权公告号 CN 1128535C

[22] 申请日 1997.2.13 [21] 申请号 97190937.7
[30] 优先权
[32] 1996.6.20 [33] JP [31] 159330/1996
[86] 国际申请 PCT/JP97/00395 1997.2.13
[87] 国际公布 WO97/49235 日 1997.12.24
[85] 进入国家阶段日期 1998.3.20
[71] 专利权人 国际商业机器公司
地址 美国纽约
[72] 发明人 沼尾雅之 清水周一 森本典繁 小林明
审查员 金 源

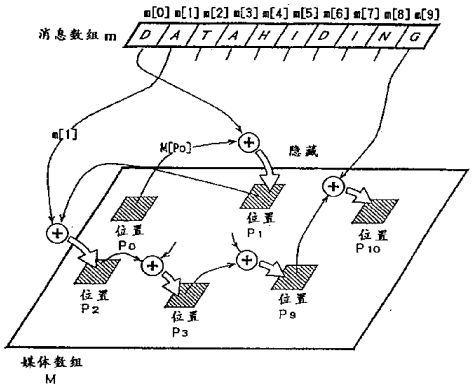
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 王以平

权利要求书 5 页 说明书 28 页 附图 17 页

[54] 发明名称 数据隐藏和抽取方法以及向网络传送和接受数据的系统

[57] 摘要

在消息数据中隐藏媒体数据的方法，和抽取隐藏数据的数据抽取方法，用媒体数组表示媒体数据，而用消息数组表示消息数据，从而可以根据状态值指示媒体数组的特定数组元素的状态值，将消息数组的数组元素分散隐藏到消息数组中。隐藏方法包括以下步骤：(a)确定第 j(j≥0)个状态值 S_j；(b)根据第 j 个状态值 S_j及其指示的媒体数组的数组元素以及消息数组的数组元素，确定第(j+1)个状态值 S_{j+1}，和(c)相对于状态值 S_{j+1}指示的媒体数组的数组元素，隐藏数据。



ISSN1008-4274

1.一种数据隐藏方法，其中用媒体数组表示媒体数据，而用消息数组表示消息数据，该方法根据确定所述媒体数组的特定数组元素的状态值，将所述消息数组的元素分散隐藏到所述媒体数组中，该方法包括以下步骤：

(a)确定第 j 个状态值，其中 $j \geq 0$;

(b)根据所述第 j 个状态值、第 j 个状态值指示的所述媒体数组的数组元素以及所述消息数组的数组元素，确定第 j+1 个状态值；和

(c)相对于所述第 j+1 个状态值指示的所述媒体数组的数组元素，隐藏数据。

2. 根据权利要求 1 的一种数据隐藏方法，其中进一步包括如下步骤：

(d)重复执行步骤(a)到步骤(c)，隐藏所述消息数组的 J 个元素。

3.根据权利要求 1 的一种数据隐藏方法，其中如果在所述步骤(a)中 $j = 0$，则根据所述消息数组的数组元素内的数据，确定初始状态值。

4.根据权利要求 1 的一种数据隐藏方法，其中如果在所述步骤(a)中 $j = 0$，就把所述消息数组的所有数组元素内的数据的异或作为输入，输入到所述初始函数，所述初始函数的输出作为所述初始状态值。

5.根据权利要求 1 的一种数据隐藏方法，其中在所述步骤(b)中，根据第 j 个状态值、第 j 个状态值指示的媒体数组的数组元素内的数据以及所述消息数组的数组元素内的数据的异或，确定第 j+1 个状态值。

6.根据权利要求 1 的一种数据隐藏方法，其中在所述步骤(b)中，把所述第 j 个状态值、第 j 个状态值指示的所述媒体数组的数组元素内的数据、以及所述消息数组的数组元素内的数据的异或作为输入，输入到所述位置转换函数，所述位置转换函数的输出作为所述第 j+1 个状态值。

7.根据权利要求 6 的一种数据隐藏方法，其中所述隐藏位置转换函数是一加密函数，该函数使用公开密钥方法中使用的密钥作为参数。

8.根据权利要求 1 的一种数据隐藏方法，其中在所述步骤(c)中，所述隐藏数据为：第 j 个状态值指示的所述媒体数组的数组元素与所述消

息数组的数组元素的异或。

9.根据权利要求 1 的一种数据隐藏方法，其中在所述步骤(c)中，把对应于所述第 j+1 个状态值指示的所述媒体数组的数组元素的第一象素块和第二象素块进行配对，并根据转换规则处理这两个象素块的特征值，以便隐藏该隐藏数据。

10.根据权利要求 9 的一种数据隐藏方法，其中所述第二象素块与所述第一象素块相邻，第一象素块与第二象素块构成一对。

11.根据权利要求 9 的一种数据隐藏方法，其中所述转换规则定义一条用于根据有关配对象素块之间的特征值的差值处理所述特征值的规则。

12.根据权利要求 11 的一种数据隐藏方法，其中所述特征值为所述象素块的亮度值。

13.根据权利要求 11 的一种数据隐藏方法，其中所述特征值为所述象素块的方差。

14.根据权利要求 2 的一种数据隐藏方法，该方法还包括在步骤(d)中抽取隐藏有所述隐藏数据的所述媒体数组以及最终状态值。

15.一种数据抽取方法，其中用消息数组表示消息数据，用隐藏数组表示包含有所述消息数据的隐藏数据，而用媒体数组表示分散隐藏有所述隐藏数据的媒体数据，该方法根据指示所述媒体数组的特定数组元素的状态值从所述媒体数组中抽取所述消息数组，该方法包括以下步骤:

(a)确定第 j 个状态值，其中 $j \geq 0$;

(b)从所述第 j 个状态值指示的所述媒体数组的数组元素中抽取所述隐藏数组的一个数组元素;

(c)根据第 j 个状态值和该隐藏数组的所述抽取数组元素，确定第 j–1 个状态值; 和

(d)根据所述第 j–1 个状态值指示的所述媒体数组的数组元素和所述隐藏数组的抽取数组元素，抽取所述消息数组的一个数组元素。

16. 根据权利要求 15 的一种数据抽取方法，其中进一步包括如下步骤: (e)递归执行步骤(a)到步骤(c)，直至满足抽取结束条件。

17.根据权利要求 15 的一种数据抽取方法，其中在所述步骤(a)中，把用于启动抽取操作的第一状态值作为抽取操作的所需信息，提供给抽取程序。

18.根据权利要求 17 的一种数据抽取方法，其中用于启动抽取操作的第一状态值为隐藏所述消息数组期间产生的最终状态值。

19.根据权利要求 15 的一种数据抽取方法，其中在所述步骤(c)中，根据所述第 j 个状态值和所述隐藏数组的数组元素内的从第 j 个状态值指示的所述媒体数组的数组元素中抽取的数据的异或，确定第 j–1 个状态值。

20.根据权利要求 15 的一种数据抽取方法，其中提供一个抽取位置转换函数，并且在所述步骤(c)中，所述第 j 个状态值、和从所述第 j 个状态值指示的所述媒体元素的数组元素中抽取的所述隐藏数组的数组元素内的数据、以及所述位置转换函数的输出的异或，作为第 j–1 个状态值。

21.根据权利要求 20 的一种数据抽取方法，其中所述抽取位置转换函数为一解密函数，该函数使用公开密钥方法中使用的公开密钥作为参数。

22.根据权利要求 15 的一种数据抽取方法，其中在所述步骤(b)中，所述隐藏数组的数组元素为第 j–1 个状态值指示的所述媒体数组的数组元素和所述消息数组的数组元素的异或。

23.根据权利要求 15 的一种数据抽取方法，其中在所述步骤(b)中，把对应于所述第 j 个状态值指示的所述媒体数组的数组元素的第一象素块和第二象素块进行配对，并根据转换规则，按照所述配对象素块特征值之间的关系，抽取隐藏数据。

24.根据权利要求 23 的一种数据抽取方法，其中所述第二象素块与所述第一象素块相邻，第一象素块与第二象素块构成一对。

25.根据权利要求 23 的一种数据抽取方法，其中所述抽取规则是基于所述配对象素块之间的特征值的差值的，并且与定义隐藏操作期间所述特征值处理的转换规则相对应。

26.根据权利要求 25 的一种数据抽取方法，其中所述特征值为所述象素块的亮度值。

27.根据权利要求 25 的一种数据抽取方法，其中所述特征值为所述象素块的方差。

28.根据权利要求 16 的一种数据抽取方法，其中利用初始函数隐藏数据，以便根据所述消息数组的数组元素内的数据，确定初始状态值，该方法还包括以下步骤：

(f)在所述步骤(d)中，一旦抽取了所述消息数组的一个元素，就利用所述消息数组的所有数组元素内的数据作为输入，以便确定所述抽取结束条件，抽取结束条件为：所述初始函数的输出等于所述第 j–1 个状态值。

29.根据权利要求 28 的一种数据抽取方法，其中所述消息数组的所有抽取数组元素内的数据的异或作为所述初始函数的输入。

30.一个向网络传送数据的系统，该系统包括：

一个存储装置，该装置存储媒体数据；

一个编码器，该编码器用于在所述媒体数据中隐藏消息数据；和

一个服务器，该服务器控制编码器，以便在所述媒体数据中隐藏所述消息数据，其中媒体数据是从所述存储装置中读取的，同时，该服务器把所述编码器的输出数据传送到网络，其中：

媒体数据是用媒体数组表示的，而消息数据是用消息数组表示的，编码器根据确定所述媒体数组的特定数组元素的状态值，将所述消息数组的元素分散隐藏到所述媒体数组中，该编码器包括如下装置：

用于确定第 j 个状态值的装置，其中 $j \geq 0$；

根据所述第 j 个状态值、第 j 个状态值指示的所述媒体数组的数组元素以及所述消息数组的数组元素，确定第 j+1 个状态值的装置；和

相对于所述第 j+1 个状态值指示的所述媒体数组的数组元素，隐藏数据的装置。

31. 根据权利要求 30 所述的系统，其中所述媒体数据是商业广告节目图象，所述消息数据是用于计算所述商业广告节目图象的广播次数的信息。

32.一个从网络接收数据的系统，该系统包括:

一个接收装置，该装置从网络上接收其中隐藏有消息数据的媒体数据；和

一个译码器，该译码器用于从所述媒体数据中抽取所述消息数据；其中:

消息数据是用消息数组表示的，包含有所述消息数据的隐藏数据是用隐藏数组表示的，而分散隐藏有所述隐藏数据的媒体数据是用媒体数组表示的，该译码器根据指示所述媒体数组的特定数组元素的状态值从所述媒体数组中抽取所述消息数组，该译码器包括如下装置:

确定第 j 个状态值的装置，其中 $j \geq 0$;

从所述第 j 个状态值指示的所述媒体数组的数组元素中抽取所述隐藏数组的一个数组元素的装置;

根据第 j 个状态值和该隐藏数组的所述抽取数组元素，确定第 j–1 个状态值的装置；和

根据所述第 j–1 个状态值指示的所述媒体数组的数组元素和所述隐藏数组的抽取数组元素，抽取所述消息数组的一个数组元素。

33. 根据权利要求 32 所述的系统，其中所述媒体数据是商业广告节目图象，所述消息数据是用于计算所述商业广告节目图象的广播次数的信息。

数据隐藏和抽取方法以及向网络传送和接受数据的系统

本发明涉及在媒体数据中隐藏消息数据的数据隐藏方法，以及抽取隐藏数据的数据抽取方法。

由于面向多媒体社会的发展，因此，在 Internet 或诸如 CD-ROM、DVD-ROM(或 DVD-RAM)、DVC 等记录介质上分布有大量数字化的图象和声音信息。由于任何人都可以轻易地全面复制以上数字化信息(该信息不易降质)，所以其不正当使用是个问题。为了防止他人不正当地复制媒体数据(如图象或声音数据)，隐藏技术正在受到关注，该技术在原始媒体数据中隐藏诸如作者标志一类的信息。如果数字化的图象数据被非法复制，通过检查副本中隐藏的标志就可以确定其来源，从而确定其是否被非法复制。该种技术被称为“数据隐藏”。

图 1 是一个半色调图象，该图象包括显示器上显示的数字化数据。如图 1(b)所示，将诸如“看护人”、“河”、“幼儿园学生”以及“鸟”这一类的照片说明(消息)隐藏在媒体数据(即图 1(a)中的数字化图象)中。通过将照片中的图象划分为小点，并确定各点的亮度值和颜色值，就可以得到媒体数据。此时，故意改变图象的原始数值。数值的细小变化不会显著地扭曲图象，用户也不会注意到。可以利用以上特性在原始图象中隐藏完全不同的信息(消息数据)。隐藏在图象中的消息数据可以包括任意信息，例如，可以为网格模式、尺状图形或图象的制作人标志。利用特定程序进行处理，就可以抽取媒体数据中隐藏的消息数据。因此，根据抽取的消息数据，就可以确定是否修改了原始媒体数据。

将图 1(b)所示的消息隐藏在该图象上一个有意义的区域附近。例如，将消息“鸟”隐藏在该鸟在该图象中出现的区域附近，并作为标题。为了在图象中隐藏诸如所有者信息一类的消息，最好将该消息散布在该图象上。这是由于当局部隐藏的消息较大时，可能降低该区域的质量。此外，如果剪去部分图象，如果消息是散布在整个图象上的，仍然可以抽取该消息。因此，如何确定在何处隐藏消息是很重要的。根据状态序列 S 确定其

位置。即，状态序列中的各元素与各消息有关，并且将该消息隐藏在根据该元素确定的相应位置。

根据常规数据隐藏方法，利用随机数序列确定状态序列 S。图 2 利用示意图说明根据常规方法散布在图象上的消息数据的布局。将图 1(a)所示的图象划分为 I 个图象区域，分别用 0 到 9 进行编号。随后，将消息数据表示为消息数组(m)，一个数组元素被描述为一个数组值 m[n]（ 0≤n≤9 ）。各数组值与分划消息数据有关。将各消息隐藏在图象中的某个位置，其中该位置是根据状态序列 S 中的元素确定的。以下等式确定位置 p_0，在位置 p_0 隐藏第零个消息 m[0]。

[等式 1]

状态值 S_0 = 初始值（常量）

位置 $p_0 = S_0 \bmod I$

以上等式表示，在给定常量作为状态值 S_0 的初值之后，状态值 S_0 对 I（图象的区域数目）的余数就是 p_0。位置 p_0 的值为 0 到（ I - 1 ）之间的任意整数。把整数值和图象区域的顺序联系起来，将消息 m[0]隐藏到第 i 个图象区域。根据以下等式确定第一消息和后继消息 m[n]的位置 p_n。

[等式 2]

$S_n = Rnd\ (S_{n-1})$

$p_n = S_n \bmod I$

以上等式表示利用前一状态值 S_{n-1} 作为随机数启动源产生伪随机数数组，利用该值作为下一状态值 S_n。状态值 S_n 对 I 的余数就是位置 p_n。将消息 m[n]隐藏到与该值相对应的图象区域。

只有知道状态值 S_0（初值）的用户，才能读取隐藏消息。若抽取了该消息，就根据初值计算状态 S_0 之后的所有状态值（ $S_1, \cdots, S_9$ ）。从而可以确定与状态值相对应的位置，并抽取隐藏在这些位置的消息。

正如在图 2 所示，由于状态值 S_n（该值用于确定第 n 个消息 m[n]在图象上的位置）仅依赖于状态值 S_{n-1}，因此，当确定了状态值 S_{n-1} 之后，就可以确定状态值 S_n。同样，状态值 S_{n-1} 仅依赖于状态值 S_{n-2}。通过递归重复以上过程，就能确定状态序列 S 中的所有元素（ S_0， S_1， S_2，…， S_9 ）。因此，状态序列 S 中的所有元素仅依赖于最初给定的作为初值的常量。所以，

一旦确定了初值，就能确定状态序列 S ，以便确定散布在图象上的消息位置，抽取其隐藏内容。

尽管努力保密其初值，如果公开了初值，或者他人知道了该初值，他人就可以利用该值轻易确定消息位置，删除该消息数据或者在第一数据上写入不同的消息数据。常规方法很难有效阻止他人为了使原始材料不被发现而删除原始标志，或者为了将他或她作为作者而在原始标志上写入不同标志。

因此，本发明的目的在于提出一种新方法，该方法用于在媒体数据中散布并隐藏消息数据。本发明的另一目的在于提供一种数据隐藏方法，该方法能够阻止他人修改消息数据。

第一发明涉及一种数据隐藏方法以实现以上目的，该方法根据状态值S（该值确定媒体数组内的特定数组元素），将消息数组的数组元素分散隐藏到媒体数组中，其中假设用媒体数组表示媒体数据，而用消息数组表示消息数据。具体而言，第一发明包括以下步骤:

⑷确定第 j （ j ≥ 0 ）个状态值 S_j;

⑹根据第 j 个状态值 S_j、由第 j 个状态值指示的媒体数组的数组元素以及消息数组的数组元素，确定第（ j+1 ）个状态值 S_{j+1}，和

⑹相对于由第（ j+1 ）个状态值 S_{j+1} 指示的媒体数组的数组元素，隐藏数据。

如果消息数组具有 J 个数组元素，则递归重复上述步骤（ a ）到步骤（ c ），直至隐藏了 J 个数组元素。如果 j= 0，则根据消息数组的数组元素内的数据，确定初始状态值 S_0。具体而言，提供一个初始函数确定初始状态值 S_0，并将一个基于消息数组的所有元素内的数据的值（例如，所有数据的异或），输入到以上初始函数。

在步骤（ b ），根据第 j 个状态值 S_j、该状态值指示的媒体数组的数组元素内的数据以及消息数组的数组元素内的数据的异或，确定第（ j+1 ）个状态值 S_{j+1}。具体而言，提供一个隐藏位置转换函数，并将以上异或输入该函数，从而得到第（ j+1 ）个状态值 S_{j+1} 作为输出。例如，隐藏位置转换函数可以为公共密钥密码学中用作参数或用作密钥的函数。隐藏数据可以为: 第 j 个状态值 S_j 指示的媒体数组的数组元素与消息数组的数组元素的

异或。

此外，第二发明涉及一种数据抽取方法，该方法根据状态值（该状态值确定媒体数组内的特定数组元素）从媒体数组中抽取消息数组，其中假设采用消息数组表示消息数据，采用隐藏数组表示包含消息数据的隐藏数据，而采用媒体数组表示分散隐藏有隐藏数据的媒体数据。第二发明包括以下步骤:

⑷确定第 j （ j ≥ 1 ）个状态值 S_j;

⑹从第 j 个状态值 S_j 指示的媒体数组的数组元素中，抽取隐藏数组的数组元素;

⑹根据第 j 个状态值 S_j 和已抽取的隐藏数组的数组元素，确定第（ j-1 ）个状态值 S_{j-1}；和

⑹根据第（ j-1 ）个状态值 S_{j-1} 指示的媒体数组的数组元素和已抽取的隐藏数组的数组元素，抽取消息数组的数组元素。

递归重复步骤（ a ）到（ c ），直至满足抽取结束条件。在步骤（ a ）中，事先向抽取程序提供状态值 S_j，作为抽取步骤所需信息，状态值 S_j 用于启动抽取步骤。例如，状态值 S_j 可以是隐藏消息数组时产生的最后状态。在步骤（ c ）中，根据第 j 个状态值 S_j 与隐藏数组的数组元素内数据的异或，确定第（ j-1 ）个状态值 S_{j-1}。从第 j 个状态值 S_j 指示的媒体数组的数组元素中，抽取隐藏数组的数组元素。此外，事先提供抽取位置转换函数，同时，在步骤（ c ）中，将第 j 个状态值 S_j 与隐藏数组的数组元素内数据的异或输入该函数，得到第（ j-1 ）个状态值 S_{j-1} 作为输出。例如，抽取位置转换函数可以为加密密钥方法中用作参数或用作密钥的解密函数。在步骤（ b ）中，隐藏数组的数组元素为：第（ j-1 ）个状态值 S_{j-1} 指示的媒体数组的数组元素、媒体数组的数组元素以及消息数组的数组元素的异或。

此外，第三发明提供一种在媒体数据中隐藏消息数据的数据隐藏方法，该方法包括以下步骤：（ a ）标识将要在其中隐藏消息数据的媒体数据内的一块（即图象数据内的一象素块），（ b ）确定标识块的特征值（例如，象素、亮度或方差值），和（ c ）处理该块的特征值，以便引用转换规则隐藏消息数据，该转换规则把将要隐藏的数据内容同特征值的参考值与该块的特征值之间的差值联系起来。

以上参考值可以为媒体数据内存在的其他块的特征值。如果标识了媒体数据内的第一块和第二块，就把这两块进行配对，并确定各对的特征值。对以上得到的特征值进行比较，并根据转换规则进行处理（例如，交换特征值），以便隐藏消息数据。如果消息数据包括许多位，就重复步骤（a）到步骤（c）。

第四发明提供一种数据抽取方法，该方法从隐藏有消息数据的媒体数据中抽取消息数据，该方法包括以下步骤：（a）标识媒体数据（其中隐藏有消息数据）内的一块，（b）确定标识块的特征值，和（c）根据该块的特征值，引用转换规则抽取隐藏的消息数据，该转换规则把将要抽取的数据内容同特征值的参考值与该块的特征值之间的差值联系起来。

以上参考值可以为媒体数据内存在的其他块的特征值。如果标识了媒体数据内的第一块和第二块，就把这两块进行配对，并确定各对的特征值。然后，根据各块的特征值，引用转换规则抽取隐藏的消息数据，该转换规则把将要抽取的数据内容同所有块的特征值之间的差值联系起来。如果第一块的特征值大于第二块的特征值，以上转换规则就抽取其中的一位，否则，抽取另一位。

第五发明涉及一种实现以上数据抽取方法的系统。即，第五发明提供一种数据抽取系统，该系统用于从隐藏有消息数据的媒体数据中抽取消息数据，该系统包括：转换装置，该装置将隐藏有消息的媒体数据转换为数字信号，其中以模拟信号方式传送媒体数据；标识装置，该装置用于标识媒体数据（隐藏有消息数据）内的一块，其中以转换装置的输出的方式传送媒体数据；特征值计算装置，该装置用于确定由标识装置标识的数据块的特征值；存储装置，该装置用于存储转换规则，其中该转换规则把将要抽取的数据内容同特征值的参考值与该块的特征值之间的差值联系起来；和抽取装置，该装置根据该块的特征值，抽取隐藏的消息数据。

另外，第六发明涉及在单片集成电路上设置以上数据抽取系统功能的半导体集成电路。即，第六发明提供一种半导体集成电路，该电路用于从隐藏有消息数据的媒体数据中抽取消息数据，该电路包括：用于确定某数据块（认为该数据块隐藏有消息数据）的特征值的装置；和抽取装置，该装置根据以上数据块的特征值，利用转换规则抽取隐藏的消息数据，其中转

换规则把将要抽取的数据内容同特征值的参考值与该数据块的特征值之间的差值联系起来。

图 1 是一半色调图象，该图象包括显示器上显示的数字化的数据；

图 2 利用示意图说明根据常规方法散布在图象上的消息数据的布局；

图 3 说明一媒体数组和一消息数组；

图 4 利用示意图说明隐藏处理中采用的媒体数组值之间的关系；

图 5 是一示意图，说明将要隐藏的对象；

图 6 是一流程图，说明在媒体数据中隐藏消息数据的过程；

图 7 说明隐藏中状态值 S_{j-1} 和 S_j 之间的关系；

图 8 是一流程图，说明从隐藏数据中抽取消息数据的过程；

图 9 说明抽取中状态值 S_j 和状态值 S_{j-1} 之间的关系；

图 10 说明确定生成的消息数组值是否是消息的开始；

图 11 是一概念图，说明由于修改而生成的错误状态序列 S 的状态；

图 12 说明采用 PBC 的数据隐藏和抽取方法；

图 13 说明采用单一象素作为象素块，采用 PBC 的隐藏方法；

图 14 说明在原始图象中隐藏消息和位置信息的方法；

图 15 说明采用同心圆弧作为位置信息的情况；

图 16 说明在采用同心圆弧作为位置信息的情况下，参考位置 B 的标识；

图 17 说明采用同心圆弧作为位置信息的隐藏和抽取方法；

图 18 是一广播系统框图；

图 19 是一框图，说明 Internet 中的一发送器和一接收机；

图 20 是一框图，说明一服务器和一客户；

图 21 是指纹和水印系统的框图；

图 22 是一数据抽取系统的框图；和

图 23 是在单片电路上设置数据抽取系统的半导体集成电路的框图。

A.数据定义

首先，定义以下数组和序列。

⑴媒体数组： M

⑵消息数组： m

⑶状态序列： S

(4)位置序列：p

(2)媒体数组：M

媒体数据包括图象和声音数据。利用媒体数组M定义媒体数据（其中嵌有消息数据），并且一个媒体数组元素 M[i]为以下表示的媒体数组的一个数组元素。

[等式3]

M：$\{M_0,M_1,\cdots,M_i,\cdots,M_{I-1}\}$或 M[i] $0 \le i \le I-1$ I：媒体数据的长度

例如，如果媒体数据为图1(a)所示的图象，则如图3所示，将该图象划分为I个图象区域，第一个区域具有第零个媒体数组值M[0]。第i个图象区域具有媒体数组值M[i]，最后一个图象区域具有媒体数组值M[I-1]。各媒体数组值中的数据为其相应图象区域的图象信息。对于单色屏幕而言，图象信息为密度，而对于彩色屏幕而言，该信息为亮度。如果图象区域的数目等于象素数目，则媒体数组值M[i]为第i个象素的象素值。如果图象区域包括多个象素（例如，3×3个象素），则图象信息为相应象素值。如果媒体数据为声音，则可以将媒体数组值M[i]定义为在时刻（i）的振幅值。假设可以将各数组值M[i]中的数据表示为一个BM字节的整数。

(2)消息数组（m）

例如，嵌入到媒体数据中的消息数据包括：有关图象制作人的信息，有关产品号、日期和地点的管理信息以及有关的复制许可信息。利用消息数组（m）定义消息数据，并且一个消息数组值 m[j]为如下表示的消息数组的一个数组元素：

[等式4]

m：$\{m_0,m_1,\cdots,m_i,\cdots,m_{J-1}\}$或 m[j] $0 \le i \le J-1$ J：消息数据的长度

例如，如果消息数据为图 3(b)所示的包含 10 个字母数字字符“DATAHIDING”的消息数据，则第j个字符与消息数组值m[j-1]有关，因此，消息数组值 m[j-1]中具有标识相应字符的数据。假设用 B_m 字节（1字节用于字母数字字符）的整数来表示各数组值m[j]中的数据。此时，消息数据的长度J为10。

(3)状态序列S

定义状态序列 S，以便确定经过隐藏处理的位置（媒体数组值），一个状态值 S_j 为如下表示的序列的一个元素。

[等式 5]

S: $\{S_0,S_1,\cdots,S_J\}$或 S_j $0 \le j \le J$ J: 消息数据的长度

用于产生状态序列 S 的算法是本实施方式的重要因素之一。应该注意到：状态序列 S 的元素数目 J 为（J+1），该值比消息数组（m）的元素数目 J 大 1。

(4)位置序列（p）

借助以下等式，利用位置序列（p）确定经过隐藏处理的位置。一个位置 p_j 为如下表示的位置序列（p）的一个元素。

[等式 6]

p: $\{p_0,p_1,\ldots,p_J\}$或 p_j $0 \le j \le J$ J: 消息数据的长度

$p_j = S_j \bmod I$

与状态序列 S 一样，位置序列（p）具有（J+1）元素。位置序列的元素的位置 p_j 是如下定义的：具有相同下标值（j）的状态值（即 S_j）对 I 的余数。因此，位置 p_j 的值为 0 到（I–1）之间的整数，与该值对应的图象区域经受隐藏处理。由于（I）为一常数，即图象区域数，所以一旦建立了状态值 S_j，就可以唯一确定位置 p_j 的值。因此，经受隐藏处理的位置事实上是由状态序列 S 确定的。

C.隐藏算法

根据本发明的数据隐藏算法是与抽取隐藏数据的算法紧密联系的。即，如果企图抽取隐藏数据的第三方具有特定信息，则他或她就可以检查以上消息。此时，重要的是能够有效阻止他人在抽取消息期间修改消息。鉴于以上考虑，本发明根据以下三特征隐藏数据。

(4)根据消息特征确定状态值 S_0

(5)根据消息和图象数据确定状态序列 S

(6)需要隐藏的数据

(1)根据消息特征确定状态值 S_0

状态序列的第一元素的状态值S_0为：初始函数f_{INI}对消息数组所有元素（m[0]，m[1]，，m[9]）的异或的输出。根据该值利用以下等式确定状态值S_0和位置p_0。

[等式7]

$$S_0 = f_{INI}(m[0] \text{ XOR } m[1] \text{ XOR } m[2] \text{ XOR } \cdots \text{ XOR } M[n-1])$$

$$p_0 = S_0 \bmod I$$

常规方法将初始状态值S_0作为一个特定常量，而并不考虑嵌入的消息内容。然而，根据以上实施方式，该元素是根据消息内容（即，所有的消息数组值）确定的。图4利用示意图说明了消息数据在图象上的分布。如该图所示，根据初始状态值S_0确定初始位置确定p_0。

根据消息数组（m）的特征确定初始状态值S_0是本算法的特征之一。这不仅使得初始状态值的确定更加复杂，而且能够有效阻止他人在消息上非法写入数据。同时，将初始函数f_{INI}用作抽取操作期间确定消息结束的函数。这样阻止了他人写入除原始消息之外的不同消息。

(2)根据消息和图象数据确定状态序列S

根据状态值S_0确定下一状态值S_1。状态值S_1由以下等式表示。

[等式8]

$$S_1 = SK(S_0 \text{ XOR } m[0] \text{ XOR } M[p_0])$$

即，下一状态值S_1为函数SK对以下输入的输出：当前状态值S_0、由状态值S_0指示的媒体数组值$M[p_0]$以及消息数组值m[0]的异或。媒体数组值$M[p_0]$是根据状态值S_0计算的位置p_0处的图象区域。以上结论，对状态值S_2和后继状态值同样正确，可以利用以下等式概括表示以上关系。

[等式9]

$$S_{j+1} = SK(S_j \text{ XOR } m[j] \text{ XOR } M[p_j])$$

函数SK为一个用于确定下一状态值的位置转换函数，接收以下输入：当前状态值、消息数组值和媒体数组值的异或。因此，通过递归执行以上等式，顺序确定状态值。由于必须确定（J+1）个状态值，所以最后一个状态值为S_J。如果消息数组具有图3(b)所示的10个元素，则产生11个状态值。通过利用以上方法确定状态序列S，就可以标识经过隐藏处理的所有图象区域。图4说明经过隐藏处理的媒体数组值之间的关系。

根据常规技术的位置序列仅仅依赖于初值，然而根据本算法的位置序列是通过一并考虑消息数组值和媒体数组值确定的。如果他人企图在原始消息上写入不同消息，则由于会产生不同的状态序列，所以重写是非常困难的。同样，如果他人企图修改图象数据，也是非常困难的。

(3)需要隐藏的数据

图5是一示意图，说明将要隐藏的对象。假设已经标识了需要隐藏的位置序列（p）。首先，数据被隐藏在位置p_1及其后继位置，而在位置p_0并不隐藏任何数据。具体而言，必须隐藏媒体数组值和消息数组值的异或结果。

首先，直接从位置p_0取出媒体数组值M[0]。然后，确定消息数组值m[0]与得到的媒体数组值M[0]的异或，并将其结果隐藏在位置p_1。该隐藏操作改变了媒体数组值M[p_1]的内容。此外，随着在位置p_2进行的处理，确定由先前处理改变的内容，即消息数组值m[1]与媒体数组值M[1]的异或，并将其结果隐藏在位置p_2。

重复以上隐藏处理直至位置p_{10}，就完成了数据隐藏。将先前处理改变的内容，即消息数组值m[9]与媒体数组值M[9]的异或，隐藏在位置p_{10}。由于并未在位置p_0隐藏数据，所以状态序列S和位置序列（p）中的元素数目都大于消息数组中的元素数目。

根据本算法，如果要抽取隐藏消息，就要以相反次序（从最后一个消息数组值m[9]开始），递归执行抽取操作。根据本算法，消息数组和媒体数组的异或结果的隐藏是与消息抽取过程密切相关的。在“消息数据抽取”部分说明其细节。此外，实际上可以采用不同的算法隐藏数据。在第二实施方式中，说明了采用PBC（象素块编码）作为隐藏数据算法的示例。

C.第一实施方式

结合图6所示的过程，具体说明第一实施方式。图6是一流程图，说明在媒体数据中隐藏消息数据的过程。在以下说明中，请参看图4或图5中的相应部分。

计算初始状态值（步骤100）

为了隐藏数据，必须确定位置序列（p）。为了确定位置序列，必须首

先确定初始位置 p[0]。利用初始函数 f_{INI}（该函数使用初始状态值 S_0 作为输入）的输出确定初始位置 p[0]，并且利用以下等式确定变量 S_0。

[等式 10]

$$S_0 = f_{INI}(m[0], m[1], m[2], \cdots, M[J-1])$$
$$= H1(m[0]//m[1]//m[2]//\cdots//M[J-1])$$

在以上等式中，H1 为散列函数。此外，算符“//”表示将消息数组的所有元素连接起来。例如，具体运算可以为数组元素内数据的异或。然而，如果采用异或，则计算结果不能反映所有消息数组值的次序。即，图 3(b)所示的消息“DATAHIDING”与消息“TADAHIDING”具有相同值。因此，采用称为 CRC（循环冗余校验法）的方法，以便反映次序关系。以上算法是计算校验和的算法之一，其产生的结果依赖于数据数组的内容和次序。

对于字节长度为 B_m 字节（数组值 m[i]）的输入，散列函数 H1 产生具有不同字节长度 K（散列值）的输出。由于该函数为单向函数，因此，当 H(x) = y 时，实际上不可能从(y)推算出(x)。

利用 K 字节散列值作为数据隐藏的初始状态值 S_0。由于该散列值被直接用作数据隐藏的初值，所以必须保证不同的输出是由不同的输入产生的。因此，散列值没有其他特殊意义。重要的是，其运算结果为标识该数组特征的输出值，即，根据所有的数组元素内容唯一确定散列值，该值依赖于所有数组的内容。

如果消息数据为图 3(b)所示的“DATAHIDING”，则根据标识所有字母数字字符数据（数组值 m[i]中的数据）的异或，散列函数 H1 的输出就是状态值 S_0。状态值 S_0 对 I（图象区域数目）的余数就是位置 p_0。这样，就能得到状态值 S_0 和位置 p_0 作为初始状态值。

象素值抽取（步骤 200）

确定在步骤 100 得到的位置值 p_0 所对应的图象区域内的图象信息。例如，如果 $p_0 = i$，则该信息为媒体数组值 M[i]。采用 B_M 字节的整数表示该数据。

下一状态计算（步骤 300）

除在步骤 100 确定的状态值 S_0 之外，根据媒体数组值 $M[p_0]$ 和状态值 S_0 标识的消息数组值 m[0]，确定下一状态值 S_1。可以利用以下等式确定状态

值S_1。

[等式11]

$S_1 = SK\ (\ S_0\ XOR\ m[0]\ XOR\ M[p_0]\ )$

（XOR为异或运算）

即，确定状态值S_0、消息数组值m[0]以及媒体数组值$M[p_0]$的异或，并将其结果输入到函数SK。然后，函数SK的输出就是状态值S_1。该函数SK被称为位置转换函数，并且将在媒体数据中隐藏消息数据的位置转换函数SK特别称为隐藏位置转换函数。由于位置转换函数SK与抽取隐藏数据的抽取位置转换函数PK紧密联系，所以在以下抽取位置转换函数的说明中也详细说明位置转换函数SK。

通过执行相似过程，确定状态值S_2及其后继状态值。概括地说，可以采用以下等式表示第j个状态值S_j和位置p_j。

[等式12]

$S_j = SK\ (\ S_{j-1}\ XOR\ m[j-1]\ XOR\ M[p_{j-1}]\ )$

$p_j = S_j\ mod\ I$

（SK：隐藏位置转换函数）

应该再次注意到：位置p_j依赖于消息数据和媒体数据的内容，也依赖于先前状态值S_{j-1}。

作为隐藏位置转换函数SK的输入的状态值S_{j-1}、消息数组值m[j-1]以及媒体数组值$M[p_{j-1}]$分别具有不同的字节长度：K、B_m和B_M。当然可以计算具有不同字节长度的所有输入的异或，但是，最好在将所有输入转换为相同字节长度之后，再计算其异或。以下两个散列函数H2和H3用于转换所有的输入，以便使所有输入的字节长度均为状态值的K字节长度。

H2：根据B_m字节的整数，产生K字节散列值的散列函数

H3：根据B_M字节的整数，产生B_m字节散列值的散列函数

即，对消息数组值m[j-1]而言，利用散列函数H2，根据数组值内的B_m字节的整数，产生一个K字节的散列值。此外，对于媒体数组值$M[p_{j-1}]$而言，利用散列函数H3将位长为B_M字节的整数，转换为B_m字节的整数。散列函数H2还用于产生一个K字节的散列值。上述等式7包括以该方式利用散列函数转换输入的情况。

消息嵌入（步骤400）

确定消息数组值m[j-1]和媒体数组值M[p_{j-1}]的异或，得到的数据就是隐藏数组值Mm[j-1]。将隐藏数组值Mm[j-1]中的数据隐藏在步骤300确定的位置p_j中。隐藏数组值Mm[j-1]为隐藏数组Mm的一个数组元素。

[等式13]

Mm：{Mm [0]，Mm [1]，…，Mm [j]，…，Mm [J-1]}

Mm [j] = m [j] XOR M[p_j]

应该理解的是：以上隐藏数据不是消息数组值m[j]，而是由消息数组值m[j]与媒体数组值M[p_j]的异或产生的隐藏数组值Mm[j]。利用函数X，将隐藏数组值Mm[j]隐藏到位置p_j。这就改变了媒体数组值M[p_j]中的数据。将其内容改变的媒体数组值M[p_j]称为M′[p_j]。即，对于函数X的特定内容，该算法在其特定位置隐藏以上隐藏数组，在第二实施方式中，以示例方式说明PBC。

确定（步骤500）

确定（j）的值是否等于J（该值比消息数组中元素的数目大1）。如果j = J，则隐藏了所有的消息数组值。如果（j）小于J，则将（j）加1，并且返回到步骤200。随后，递归执行步骤200到步骤400，直至（j）等于J。该过程使得产生分别包含（J+1）个元素的状态序列S和位置序列。

[等式14]

状态序列S：{S_0，S_1，S_2，…，S_J}

位置序列P：{p_0，p_1，p_2，…，p_J}

由于数据隐藏，所以根据以下等式改变媒体数组M的所有元素。

[等式15]

（隐藏前的媒体数组）

M：{M[0]，…，M[p_0]，…，M[p_1]，…，M[p_{I-1}]}

（隐藏后的媒体数组）

M′：{M′[0]，…，M′[p_0]，…，M′[p_1]，…，M′[p_{I-1}] = {M[0]，…，M[p_0]，…，M′[p_1]，…，M′[p_{I-1}]

M′表示隐藏后的媒体数组，M′[i]表示该媒体数组值的内容在隐藏之前

已经改变。即，媒体数组值M′表示仅仅改变了原始消息数组M（由状态序列S标识）的J个数组元素。由于与状态值S_0相应的数组元素M[p_0]无需改变数据，所以M′[p_0]等于M[p_0]。

图7说明隐藏中状态值S_{j-1}和状态值S_j之间的关系。通过计算状态值S_{j-1}和隐藏数组Mm[j-1]（M′[p_{j-1}] XOR m[j-1]）的异或，并将该结果输入到位置转换函数SK，就可以确定状态值S_j。在前一状态的隐藏期间，就已经改变了媒体数组值M′[p_{j-1}]的内容。此外，利用函数X，将隐藏数组Mm[p_{j-1}]隐藏在位置p_j。这就改变了位置M[p_j]的数据。

状态值抽取（步骤600）

通过抽取以下两条消息，就完成了消息隐藏。

（1）隐藏后的媒体数组M′

（2）最终状态值S_J

在步骤400，通过在媒体数据内隐藏数据最终得到媒体数组M′。最终状态值S_J是最后计算的第J个状态值。如下所述，当抽取消息数据时，需要以上信息。当抽取隐藏消息时，抽取人无需知道第（J-1）个状态值之前的状态值S0到SJ-1，他或她只要知道第J个状态值即可。这是由于通过反向转换最终状态值，就可以确定以上状态值。当然，抽取人必须具备下述所需信息。

（消息数据抽取）

为他人提供以下三条信息，以便抽取消息数据。

⑴隐藏后的媒体数组M′

⑵最终状态值S_J

⑶抽取位置转换函数PK

信息（1）和信息（2）是嵌入消息数据期间最终产生的。以下结合隐藏位置转换函数，说明信息（3）中的抽取位置转换函数PK。

a.隐藏位置转换函数SK，抽取位置转换函数PK

如同在隐藏消息中定义产生下一状态值的隐藏位置转换函数SK一样，在抽取消息中定义产生前一状态值的抽取位置转换函数PK。如以下等式所示，隐藏位置转换函数SK和抽取位置转换函数PK互为逆函数。

[等式16]

$PK(SK(x)) = x$

$SK(PK(x)) = x$

因此，通过利用隐藏位置转换函数SK转换消息数组（m），随后利用其逆函数PK进一步转换该结果，就可以抽取原始消息数组（m）。

满足以上等式的各种函数都是可能的。事实上，为了防止他人利用已配备的抽取位置转换函数PK来复制隐藏位置转换函数SK，最好采用公开加密法中的加密函数和解密函数。根据公开密钥法，存在多种算法，可以选择任一种算法。例如，以下说明的典型RSA方法。RSA方法的算法如下所述。

1.选择两个大素数p和q，计算$n = p \times q$。

2.计算$r = lcm(p-1, q-1)$并选择(d)，使得$gcd(d, r) = 1$。

3.确定(e)，其中(e)满足$e \times d = 1 \pmod{r}$和$0<e<r$。

4.公开(e)作为公开密钥，同时公开(n)。保密(d)作为秘密密钥。

5.为了加密消息(m)，计算(c)，使得$m^e = c \pmod{n}$。该(c)成为加密消息。

6.为了解密加密消息，计算(m)，使得$c^d = m \pmod{n}$。该(m)成为解密消息。

通过将以上算法应用到本实施方式，就得到以下隐藏函数SK和抽取函数PK。

[等式17]

$SK(m) = x^d \pmod{n}$

$PK(m) = x^e \pmod{n}$

即，制作图象的制作人具有密钥(d)，并利用该密钥得到隐藏函数SK。为了嵌入消息数据，利用函数SK产生位置状态序列S，函数SK将数据嵌入到媒体数据中。具有以上分布数据的第三人，利用公开密钥(e)得到抽取函数PK。为了读取该消息，第三人利用函数PK产生位置状态序列S。在公开密钥方法中，向他人公开公开密钥，但是只有制作图象的作者才具有秘密密钥，从而他人不能知道图象的内容。因此，他们不能知道隐藏位置转换函数的内容。由于从公开密钥中计算出秘密密钥需要大量计算，因此他人几乎不可能知道隐藏位置转换函数SK。以上方法能够有效阻止他人修

改原始数据。

以下简要说明异或的重要性质，该性质用于解释消息抽取过程。异或运算具有以下性质。如果确定了A与B的异或，随后又确定了该结果与B的异或，就能再现A。

[等式18]

$$(A\ XOR\ B)\ XOR\ B = A$$

（抽取算法）

图8是一个流程图，说明抽取嵌入消息数据的过程。

初始状态值计算（步骤110）

首先，根据以下等式，从最终状态值S_J（已提供给了抽取人）中确定位置p_J，其中在位置p_J隐藏有消息数组值m[J-1]。

[等式19]

$$p_J = S_J \bmod I$$

隐藏值抽取（步骤120）

媒体数组$M'[p_J]$具有隐藏数组值Mm[J-1]，该值被隐藏在位置p_J的原始图象信息中。数组Mm[J-1]为媒体数组值$M'[p_{J-1}]$和消息数组值m[J-1]的异或。随后定义函数X′，以便从媒体数组值$M'[p_J]$中抽取隐藏数组值Mm[J-1]。在第二实施方式中，说明以下等式中函数X′特定内容的示例。

[等式20]

$$Mm[J-1] = 函数X'(M'[p_J])$$

前一状态计算（步骤130）

接着，通过计算状态值S_J和隐藏数组值Mm[J-1]（由函数X′确定）的异或，确定前一状态值S_{J-1}。应该注意到：此时利用了以上异或运算的数学性质。

[等式21]

$$PK\ (S_J)\ XOR\ X'(M'[p_J])$$
$$= (S_{J-1}\ XOR\ Mm[J-1])\ XOR\ Mm[J-1]$$
$$= S_{J-1}$$

即，由于抽取位置转换函数PK是隐藏位置转换函数SK的逆函数，所以可以使用该函数从状态值S_J、状态值S_{J-1}与隐藏数组值Mm[J-1]的异或结果

中进行再现。确定了以上结果与隐藏数组值Mm[J-1]（在步骤120确定该值）的异或，就能确定前一状态值S_{J-1}。

消息计算（步骤140）

一旦确定了状态S_{J-1}，就可以标识相应的媒体数组值$M'[p_{J-1}]$。随后，可以利用以下等式抽取消息数组值m[J-1]。如果隐藏了图3(b)所示的消息，该步骤就可以抽取尾部字母“G”。

[等式22]

$$M'[p_{J-1}] \text{ XOR } Mm[J-1]$$
$$= M'[p_{J-1}] \text{ XOR } (M'[p_{J-1}] \text{ XOR } m[J-1])$$
$$= m[J-1]$$

利用下标值(j) ($1 \le j \le J$)，可以将状态值的抽取或消息数组值的抽取概括为以下等式。

[等式23]

S_{j-1}:

$$PK(S_j) \text{ XOR } X'(M'[p_j])$$
$$= (S_{j-1} \text{ XOR } Mm[j-1]) \text{ XOR } Mm[j-1]$$
$$= S_{j-1}$$

m[j-1]:

$$M'[p_{j-1}] \text{ XOR } Mm[j-1]$$
$$= M'[p_{j-1}] \text{ XOR } (M'[p_{j-1}] \text{ XOR } m[j-1])$$
$$= m[j-1]$$

图9表示以上等式标识的数据关系。该图表示了抽取中状态值S_j和状态值S_{j-1}之间的关系。将该图与图7相比，显示出抽取过程是隐藏过程的逆过程。

确定（步骤150）

每当产生消息数组值m[j]时，就确定该值是否为消息数组的开始。如果是这样的话，就抽取了消息数组(m)的所有元素。由于以相反次序（即从最后元素开始）抽取了该消息数组(m)，所以对于图3(b)的示例而言，以次序“GNIDIHATAD”抽取该消息。在步骤160，颠倒以上消息次序，以便产生完整消息。如果消息数组值m[j]并不是消息数组的开始，就递归执行步

骤120到步骤140，直至步骤140的确定结果变为肯定。

确定消息数组(m)的某个元素是否为该消息数组的开始等价于，确定产生的状态值S_j是否满足散列函数H1的输出。将已经产生的消息数组(m)的所有元素的异或输入到散列函数H1。如果以相反次序产生的状态值S_j与散列函数H1的输出满足以下等式所示的关系，则j的值为0(参见等式10)。

[等式24]

$$S_j = f(m[J-1] \text{ XOR } m[J-2] \text{ XOR } \cdots \text{ XOR } m[j] = S_0$$

仅当j = 0时，以上等式才成立，而对于其他情况($j \neq 0$)，以上等式并不成立。每当以相反次序产生最终状态值S_j时，就把该值与基于所有抽取消息数组值的散列函数的输出进行比较。图10说明了确定生成的消息数组值是否为该消息的开始。首先，确定最终状态值S_J的前一状态值S_{J-1}，以及消息数组值m_{J-1}。输入消息数组值m_{J-1}时，得到的初始函数(f)的输出F与状态值S_{J-1}不匹配。如果确定了状态值S_0，则该值与初始函数的输出匹配，并能够确定该消息数组值就是消息的开始。因此，由于以下性质，本算法在防止他人修改消息方面是非常有用的。

(1)防止重写不同信息

根据常规技术，所产生的位置序列S仅仅依赖于初始提供的常量值，而并不考虑该消息的内容。仅仅知道该常量，他人就可以删除该消息或者在原始消息上重写不同消息。然而，根据本算法，状态序列的产生还依赖于消息的内容，不同的消息产生不同的位置序列。由于隐藏位置是基于该位置序列的，所以不可能将具有不同内容的不同消息隐藏在存在原始消息的位置。这对媒体数据也是同样正确的。

(2)防止隐藏不同信息

本算法检查等式24所示的条件，以便确定结束抽取。仅当某个抽取消息的内容与原始消息的内容相同，并且该抽取消息的长度与消息数据(J)的长度相同时，才满足该条件。不满足该要求，就没有完成抽取。因此，如果企图根据最终状态值S_J，以相反次序隐藏除原始消息之外的数据，则永远不会满足等式24的要求，并且计算将会永久进行下去。因此，由于没有完成该计算，所以企图在原始消息出现位置之外的位置隐藏消息是不可能的。

如图 10 和图 11 所示，如果他人修改了消息数组值，则根据修改消息将产生不同的状态数组 S′。这样就能防止他人删除或重写位于状态状态序列 S′标识的位置以外位置的原始消息。图 11 所示的通过修改产生的状态序列 S′永远不能确定已经完成了抽取。事实上，由于可以防止写入不同消息，所以能够有效防止他人修改消息。

D. 第二实施方式

本节说明象素块编码（以下称为“ PBC ”），象素块编码是在媒体数据中嵌入需要隐藏的数据和抽取隐藏数据的一种方法。借助 PBC，根据以下说明的转换规则，就可以进行数据隐藏和数据抽取。

（基本算法）

通常，两个相邻象素的象素值的主要特征为较高的相关性。因此，即使在相邻象素之间交换象素值，该图象也不会明显降质。考虑到这一性质，本算法将至少具有一个象素的图象区域定义为一个象素块，并根据特定的转换规则，通过有意交换相邻象素块的特征值来隐藏一比特数据。即，通过交换相邻象素块的特征值来表示数据。此外，根据以上转换规则确定的抽取规则，抽取数据。

根据以下转换规则，通过交换两个相邻象素块的特征值（例如，亮度）来表示位信息。

位接通 <1>: 象素块（ PB_1 ）特征值大于另一象素块（ PB_2 ）的特征值

位断开 <0>: 象素块（ PB_1 ）特征值小于另一象素块（ PB_2 ）的特征值

此外，根据以下抽取规则，通过比较两个相邻象素块的特征值（例如，亮度）来抽取位信息。

象素块（ PB_1 ）特征值大于另一象素块（ PB_2 ）的特征值: 位接通 <1>

象素块（ PB_1 ）特征值小于另一象素块（ PB_2 ）的特征值: 位断开 <0>

图 12 说明了利用 PBC 进行数据隐藏和数据抽取。可以将象素块 PB_1 和象素块 PB_2 定义为多个象素（例如， 3×3 象素）的集合，或者将一个象素定义为一个象素块。由于相邻的象素块具有较高的相关性，所以交换其位置不会使该图象明显降质（图 12a ）。

假设原始图象中的象素块的位置为图 12 (b) 所示的位置。同时假设两个象素块的特征值的比较结果为: PB_1 的特征值大于 PB_2 的特征值。如果在原

始图象中隐藏有数据“1”，则象素块的特征值就满足转换规则中数据“1”的条件，因此，无需交换象素块的特征值。当抽取数据时，抽取数据“1”(这是由于抽取规则确定如果PB_1的特征值较大就抽取数据“1”)。

另一方面，如果在原始图象中隐藏有数据“0”，就交换原始图象中象素块的特征值(这是由于这些特征值之间的关系并不满足数据“0”的条件)。然而，并不能明显辨别以上交换。在抽取期间，根据这些象素块的特征值之间的关系，抽取数据“0”。

这样，PBC从图象中选择足够的象素块，以便隐藏需要隐藏的信息。随后，将某个所选象素块和相邻象素块配对，以便产生一个配对数组。从该数组的开始着手，顺序隐藏以上配对。

可以把该数组和第一实施方式中的状态序列S联系起来。例如，把一个象素块和第一实施方式中媒体数组M的数组元素(m)联系起来。将隐藏期间顺序产生的每个数组元素(状态值S_j)和相邻媒体数组值进行配对。随后，对得到的配对进行以上处理。同样可以根据特定随机数启动源产生的伪随机数序列进行确定。

在抽取期间，扫描与隐藏块数组相同的块数组。根据抽取规则(通过确定各对是表示“位接通”还是表示“位断开”)，通过1比特接1比特收集，就能抽取全部图象。如果配对象素块的特征值相同，就跳过该配对(如同隐藏操作一样)。通过保密以上块数组或数组产生方法，就可以对他人隐藏以上隐藏信息。

在PBC中，最好根据图象质量和抽取精度确定嵌入位置。即，如果配对象素块之间的特征值差别较大，则交换操作将会降低图象质量。为了遏止图象质量的下降，最好提供第一阈值(一上限值)，这样，如果特征值之差大于等于该阈值，就不在该配对中嵌入任何比特(位)。

此外，如果特征值之差足够小，则交换操作基本上不会降低图象的质量。然而，此时，噪声可能颠倒特征值的幅度，因此，不能抽取嵌入位。因此，为了遏止抽取精度下降，最好提供第二阈值(一下限值)，这样，如果特征值之差小于等于该阈值，就不在该配对中嵌入任何比特。

跳过与以上情况对应的配对，而不进行任何处理。随后将需要隐藏的位信息传送到下一配对。

（块特征值）

象素块的主要特征值和次要特征值被用作特征值。主要特征值是直接象素值参数，如象素块的亮度和色度。次要特征值为表示统计特性的值，如以上参数的平均值和方差，并且通过分析主要特征值得到。另外，该特征值可以为某一数组（该主组包含多个象素值）与一特定数组（掩码）或一特定元素值（通过频率转换得到）的运算结果。两个相邻象素块之间的主要特征值具有较高的相关性。然而，两个互不相邻的独立的象素块之间的次要特征值具有较高的相关性。因此，应该注意到：无需限制进行PBC处理的象素块为相邻象素块。以下把亮度值（即主要特征值）和方差值（即次要特征值）称作象素块特征值的示例。

首先，说明采用亮度值作为象素块的特征值。如果一个单象素与一象素块有关，就可以直接使用该象素的亮度值作为该块的特征值。在自然图象中，相邻象素通常具有较高的相关性，因此，即使交换象素，图象质量也不会明显下降。图13说明当象素块仅包含单象素时，执行PBC后的隐藏处理。

接着，说明采用方差值作为象素块的特征值。当象素块包含n×m个象素时，如果在象素块之间交换象素的亮度值，就会明显降低图象的质量，例如，图象中会出现条纹图。因此，最好不要直接把象素值作为象素块的特征值。从而，想到利用象素亮度的方差值作为特征值。

众所周知，当把象素块的亮度值特性划分为平均值(h)和方差值(d)时，如果交换相邻象素块的方差值(d)而保留其平均值(h)，并不会明显降低图象的质量。因此，根据以上性质，采用方差值(d)作为象素块的特征值，并且根据转换规则交换相邻象素块的特征值，就可以隐藏数据。

如图12(c)所示，假设象素块PB_1的平均值为h_1，方差值为d_1，而象素块PB_2的平均值为h_2，方差值为d_2。如果位“1”被隐藏，由于$d_1<d_2$，所以并不满足该位的条件。因此，仅仅交换两个象素块的方差值(d)。这等价于在两个象素块之间交换分布的峰值，而保持其平均值(h)。

（可以隐藏的信息量）

在PBC中，利用图象的尺寸和象素块的尺寸，可以隐藏的信息量的上限定义如下。

（图象尺寸）/（象素块尺寸）/2 [比特]

例如，如果把1×1的象素块应用于384×256的图象，则可以隐藏的信息量的上限为6 KB。然而，由于并非所有象素块都可用于隐藏（例如，在相邻象素块具有相同特征值的情况下），所以实际上限要小一些。此外，尽管存在隐藏的可能性，由于为了防止降低图象的质量往往要取消交换处理，所以该值还会进一步减少。

（图象保存和降质）

众所周知，图象上的两个相邻象素（其中该图象的边缘部分在该象素之间延伸）具有大不相同的亮度值。因此，交换这样两个象素将断开以上边缘，导致图象质量的明显下降。因此，为了防止图象质量下降，为需要交换的亮度值设置某一阈值。事实上，如果超过了该阈值，就跳过该配对而并不交换其特征值。可以根据从该图象数据计算出的方差值或该象素块周围的局部方差值，确定以上阈值。

如果把某个象素块的方差值（该方差值接近0）与另一个象素块的方差值（该方差值远大于0）进行互换，就会明显改变小象素块，导致图象质量的明显下降。因此，将较小的方差值与以上阈值进行比较，如果该方差值小于阈值，就取消交换操作。

（PBC的强度）

由于比较了相邻象素块的特征值，并且隐藏了与特征值交换有关的数据，所以只要保留象素块之间的相对关系，就能够正确检索隐藏信息。因此，根据特征值之差，即使进行色度调整或色度校正，也应该能够保留隐藏信息。此外，在上述方差值交换方法中，如果象素块的尺寸为8×8，即使经过JPEG压缩处理，也能够正确抽取隐藏信息。实验证明：即使执行“有损压缩”以便将文件尺寸降至5%，也能够保留90%的信息。即使经过D/A和A/D转换（如打印/扫描操作），以上方差值交换方法也能有效保留隐藏信息。

（PBC的扩充）

应该注意到：以上PBC方法仅仅是示意性的，还可以想到许多其他方法。正如在上述实施方式中明显看到的那样，在数据嵌入和数据抽取中，根据有关特征值之差的规则处理象素块的特征值是非常重要的。从这个意

义上讲，除了按上述方式交换特征值之外，可以对某一特征值增加一特定值或者从另一特征值中减去该特定值（或者同时执行两种处理）。此时，该特定值可以为一常量，也可以根据需要处理的象素块的条件进行改变。此外，作为 PBC 的扩充，可以定义一条用于联系特征值符号和二进制信息的规则，以便根据该规则嵌入或抽取数据。

本发明的实质在于：根据一条有意义的规则，利用某个参考值（例如，图象数据中的一个相邻象素块）来处理另一象素块。即，通过引用转换规则处理相邻象素块之一的特征值实现数据隐藏，其中该转换规则把隐藏数据的内容和特征值的参考值与该象素块的特征值之间的差值联系起来。从这种意义上讲，根据本发明，只要该参考值明确并且能够处理特征值即可，而并不要求该参考值为图象数据中的一个特定区域（一个象素块）。因此，可以从除图象数据之外的数据中获得该参考值。例如，将具有特定值（参考值）的固定掩码模式用作特征值处理的参考值，其中固定掩码模式的尺寸与象素块的尺寸相同。此时，在隐藏操作期间，以掩码模式中的参考值为基准，处理特定象素块的特征值，而在抽取操作期间，根据与参考值的差值，抽取数据。

E.第三实施方式

本节说明在参考位置隐藏信息的方法。以上数据隐藏技术选择原始图象中的象素块进行处理，并从经过处理的象素块中抽取消息。因此，对于抽取消息而言，有关象素块的位置信息是必不可少的。利用图象中的某个区域（在第一实施方式中，原始图象的左上角）作为基准，相对确定象素块的位置。然而，如果他人修改该图象（例如，剪切部分图象），就不能够确定该图象的参考位置，从而不能抽取消息。再次参照图 3(a)，如果剪切了部分原始图象（该图中虚线所围区域），就不能根据剩余的屏幕图象确定原始参考位置（消息数组中第 0 个数组元素的位置 M[0]）。

数据隐藏的重要要求为：他人不能够轻易删除隐藏信息、即使该数据被他人蓄意修改或者该数据经过有损图象压缩处理（如 JPEG ）也能够正确抽取隐藏信息。因此，如图 14 所示，除消息之外，最好也将用于确定参考位置的信息隐藏在原始图象中。隐藏这种位置信息使得从修改图象或压缩图象中正确抽取消息成为可能。因此，也将用于确定媒体数据参考位置的信

息隐藏在消息数据中。以上有关参考位置的信息被隐藏在整个消息数据中。如果剪切掉部分消息数据，则以上信息使得从被剪切的部分消息数据中，检测该消息数据的参考位置或者检测相对于该参考位置的任一位置成为可能。例如，如下所述，可以将围绕参考位置的同心圆弧隐藏在整个图象中。

（采用同心圆弧作为位置信息）

将图 15 所示的同心圆弧用作位置信息。该同心圆弧是以原始图象的左上角（参考位置）为基础，以特定间隔绘制的。为了从已剪切的部分图象中正确抽取参考位置，假设被剪切的部分图象至少包含有一条圆弧。因此，假设以上条件，设置同心圆弧之间的间隔。

利用圆的性质（即，如果采用另一个圆周上的一点作为圆心，以该圆周的半径作为半径绘制一个圆，则所绘制的圆周将通过第二个圆的圆心），就能够确定以上参考位置。图 16 说明在使用同心圆弧作为位置信息的情况下，参考位置 B 的确定。首先，确定被剪切的部分图象内的任意三点（a_1，a_2，a_3），其中（a_1，a_2，a_3）分别出现在三条同心圆弧（c_1，c_2，c_3）上。然后，从各点绘制具有不同半径（r_1，r_2，r_3，r_4，…）的圆。此时，圆弧相交数最大的圆弧交点就是参考位置 B。在数字图象中，由于象素是以网格形式分散排列的，因此，通过按上述方法绘制圆弧，就能够非常精确地确定参考位置。

对于远离左上角（参考位置）的圆弧（该圆弧具有较大直径）而言，以该部分图象包含两个或两个以上圆弧的方式，降低圆弧之间的间隔。随着圆弧的直径越来越大，该圆弧将包含越来越多线性元素，引起参考位置计算值中的较大差别。降低间隔就能够降低该差别，这是由于该部分图象包含许多圆弧。此外，通过在左上角和右上角设置参考位置（即，同心圆弧的圆心），就可以根据两个圆心来确定原始图象的尺寸。

（利用同心圆弧进行隐藏）

图 17 说明了采用同心圆弧作为参考位置的隐藏和抽取方法。在图 17(a)中，采用第二实施方式中说明的方法在原始图象中隐藏消息，随后在该点隐藏同心圆弧作为位置信息。例如，将位于同心圆弧上的象素的 LBP 设置为“1”。采用 LBP 是由于改变该值几乎不会在该图象中引起明显视觉变

化。此外，在图17(b)中，在原始图象中隐藏位置信息，随后在该点隐藏消息。

（利用同心圆弧进行抽取）

创建一个二维表决数组T。通过综合可能剪切的部分图象的最大尺寸确定该数组的大小。例如，如果该数组的宽度为(2m-1)，则该数组能够处理的部分图象最大为原始图象的1/m。表决数组T中的各个元素表示参考位置B内的一个候选项，该元素的值表示该候选项的表决数。两个坐标按以下方式关联：部分图象位于表决数组的中心。

扫描以上部分图象，一旦遇到LBP为“1”的点，就以该点为基准，绘制表决数组中所有已知半径的圆弧。随后，将表决数组T的各元素的表决数加1。此时，如果该点为隐藏各元素相对应点的圆周上的点，则至少一条绘制圆弧通过原始圆心。

对部分图象交替进行垂直扫描和水平扫描，并且一旦遇到LBP为“1”的点，就执行以上过程。这样，对应最大表决数元素的位置就是参考位置B。最大表决数集中在对应参考位置的表决数组的数组元素上。因此，尽管存在噪声影响，本算法也能够正确确定参考位置。

由于图17(a)所示的方法利用隐藏的消息改变图象数据，于是根据所确定的参考位置从部分图象中适当地抽取消息。因此，如果不采用能够抵抗随机噪声的数据隐藏方法，信息抽取就不会成功。然而，图17(b)所示的方法在抽取隐藏消息之前，并不改变该隐藏消息，所以该方法比图17(a)所示的方法更能抵抗噪声。因此，本算法允许采用多种数据隐藏方法。然而，应该注意到：根据本发明，可能破坏有关参考位置的部分信息。

F.特定应用

具体而言，可以在以下系统中应用采用上述算法的数据隐藏和数据抽取方法。

（电视图象CM事件计数）

对于已预定了广播的人员而言，是否将其商业广告节目广播所请求的次数是重要的。可以采用本算法来构造图18所示的系统，以便自动计算广播次数。该广播站具有一个存储装置、一个编码器和一个广播装置。存储装置存储商业广告节目图象，编码器在商业广告节目图象中隐藏用于计算广

播次数的信息。广播装置广播其中隐藏有以上信息的商业广告节目图象。该系统利用上述数据隐藏方法编码商业广告节目图象。根据计数信息中的数据（该数据被分散隐藏到商业广告节目图象中）进行编码。此外，接收站具有一个接收器、一个译码器和一个计数器。接收器接收其中隐藏有计数信息的商业广告节目图象。译码器从商业广告节目图象中抽取计数信息。根据抽取的计数信息，计数器计算广播次数。该接收系统根据上述数据抽取方法抽取计数信息。根据计数信息中的数据，通过确定计数信息在该商业广告节目图象上的排列位置，并从该位置抽取数据进行译码。

广播站广播具有隐藏计数信息的商业广告节目图象，计数信息使得接收站可以根据隐藏算法来计算广播次数。因此，通过抽取计数信息，接收站就能够计算广播次数。

（防火墙审查）

拓扑（如防火墙）内外的所有 HTTP 传输都要经过位于该拓扑上的代理服务器。可以利用以上性质来审查该代理服务器上的图象数据和声音数据。如果检测到其中隐藏有水印的媒体数据，就将其留在日志中。这样，就能够检测非法分布数据。图 19 是该系统的框图。服务器具有一个存储装置和一个编码器，存储装置存储媒体数据，而编码器用于在该媒体数据中隐藏消息数据。服务器控制编码器，以便在该媒体数据（该数据是从存储装置中读取的）中隐藏消息数据，同时，该服务器把输出数据传送到 Internet 。因此，可以根据消息数据的内容，利用上述隐藏方法在媒体数据中分散隐藏消息数据。接收站具有一个代理服务器和一个译码器，其中代理服务器从 Internet 接收媒体数据（已经在传输站对该媒体数据进行了隐藏处理），而译码器从接收数据中抽取消息数据。根据消息数据的内容，通过利用上述数据抽取方法确定分布消息数据的位置，进行抽取操作。

（应用于旅行社服务器）

WWW 服务器（由旅行社控制）上显示的旅游场所照片中隐藏有附加信息（如旅游场所的说明或地图、 URL 点信息）。通过采用 WWW 浏览器对该照片进行网络复制，随后就可以从该照片中抽取地图，以便检查说明、交通和路线。如图 20 所示，即使该客户已经与 WWW 服务器断开连接，也能够抽取附加信息。与从照片数据文件中分离附加信息文件的方法相比，利用隐

藏方法就能够保存照片数据和附加信息之间的密切关系，因此，可以轻而易举地保存数据。

（指纹和水印）

指纹是指发布给他人的媒体数据中的隐藏标记，该标记使得媒体数据的发行者能够确定他人的身份。如果有人从事了非法活动（如非法拷贝），则利用该指纹就能确定活动源。因此，如果该人正在非法发布拷贝，则他或她将对该非法拷贝负责。

另一方面，水印是指发布给他人的媒体数据中的隐藏标记，该标记使得媒体数据的发行者能够确定他或她的身份。这样，就能够确保在发布期间该数据不会被修改，即，该数据是由合法发行者发行的，并在发布期间未作修改。

为了隐藏以上标记，可以构造图 21 所示的系统。当向他人发布数据时，该数据内隐藏有一个水印。可以从他人那里得到的数据中抽取该标记，以便检查。

除以上系统之外，可以将本发明应用于采用电缆、卫星通信或 DVD-ROM（DVD-RAM）存储介质的系统。具体而言，如果采用 DVD-ROM（DVD-RAM）发布数据，则该数据中包含有关复制许可的隐藏信息，即，是允许复制还是禁止复制。终端用户用来复制数据的 DVD 播放器具有限制复制功能。因此，如果复制播放器发现从其介质中抽取的复制许可状态为禁止复制的话，就启动禁止复制。

G.数据抽取系统和实现该系统的半导体集成电路

具体而言，可以在具有以下结构的系统中实现上述数据抽取方法。此外，可以在一块芯片（如半导体集成电路）上提供以上系统的大部分功能。为了避免重复，省略了该系统和半导体集成电路特性的详细说明，但是，在数据抽取方法中说明的术语、其扩充以及其变更同样适用于这些系统。根据以上方法的详细说明，对于本领域熟练的技术人员而言，以下术语的细节是显而易见的。

具体而言，如图 22 所示，用于从媒体数据中抽取消息数据的系统具有一个转换装置、一个确定装置、一个特征值计算装置、一个存储装置和一个抽取装置。转换装置为一个 A/D 转换器，该转换器将由模拟信号构成的

媒体数据（其中隐藏有消息数据）转换为数字信号，随后转换器输出该数字信号。确定装置确定由转换装置输出的媒体数据中隐藏有消息数据的一个数据块。特征值计算装置决定由确定装置确定的数据块的特征值。存储装置存储转换规则，该规则把需要抽取的数据内容同特征值的参考值与该数据块的特征值之间的差值联系起来。抽取装置依据该数据块的特征值，参照转换规则，抽取隐藏的消息数据。

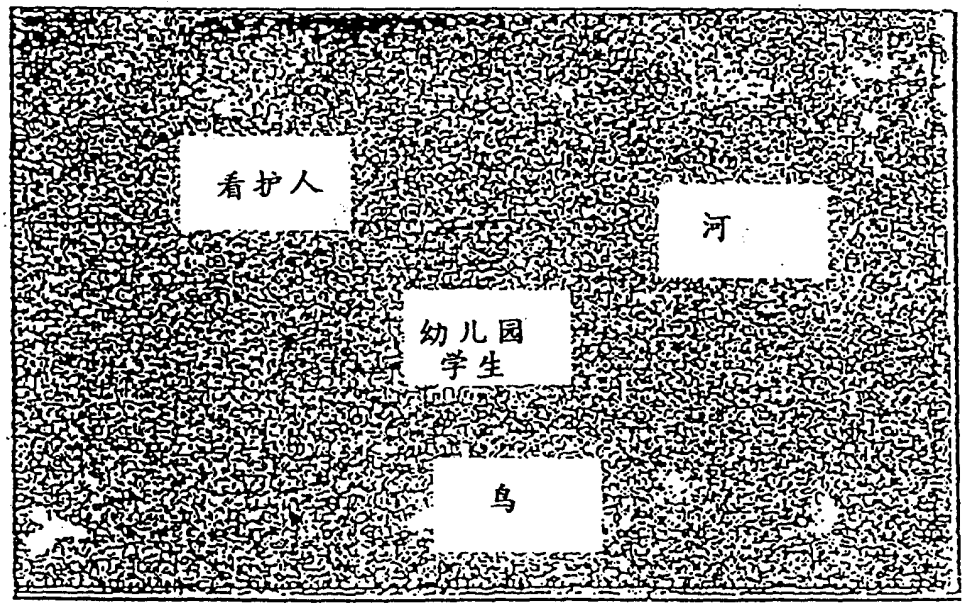
参考值为媒体数据中出现的不同于第一数据块的第二数据块的特征值。存储在存储装置内的转换规则规定：如果第一块的特征值大于第二块的特征值，则抽取该位中的一位；反之，如果第一块的特征值小于第二块的特征值，就选择另一位。

此外，如图 23 所示，由安装有上述系统的芯片构成的半导体集成电路至少具有一个计算装置和一个抽取装置。计算装置决定媒体数据（由输入信号构成）中已经被确定为隐藏有消息数据的数据块的特征值。抽取装置根据该数据块的特征值，参照转换规则，抽取隐藏消息，其中转换规则把需要抽取的数据内容同特征值的参考值与该数据块的特征值之间的差值联系起来。

如上所述，如果在媒体数据（如图象或声音）中分散隐藏消息数据，则本发明根据媒体数据和消息数据的内容确定该消息的隐藏位置。因此，本发明使得数据隐藏处理能够防止他人轻易修改消息。

图 1

(a)



(b)

图 2

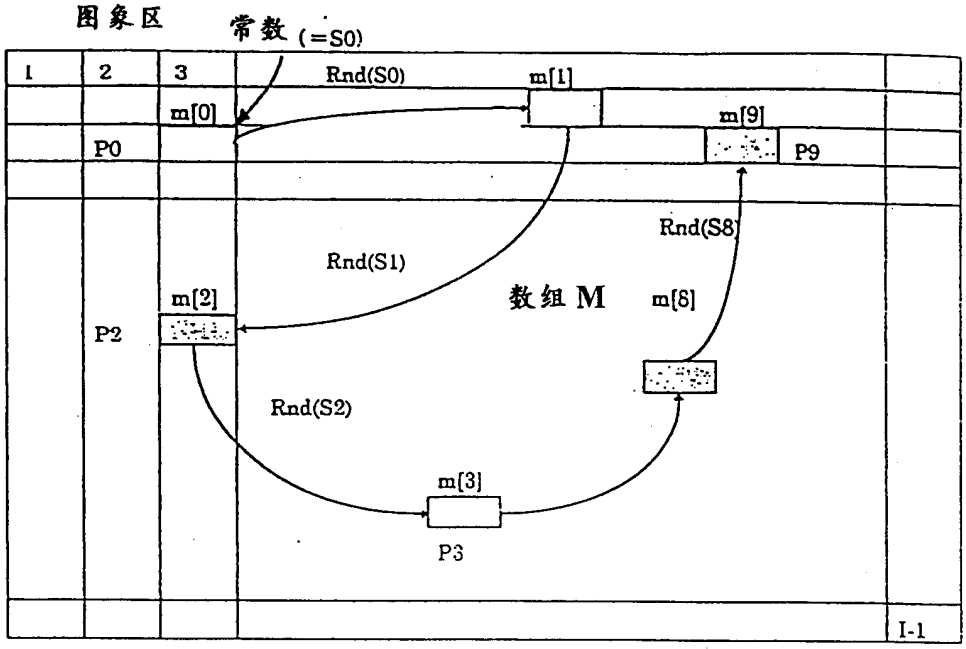

图象区
常数 (=S0)
1
2
3
Rnd(S0)
m[1]
m[0]
m[9]
P0
P9
Rnd(S8)
Rnd(S1)
m[2]
数组 M
m[8]
P2
Rnd(S2)
m[3]
P3
I-1

图 3

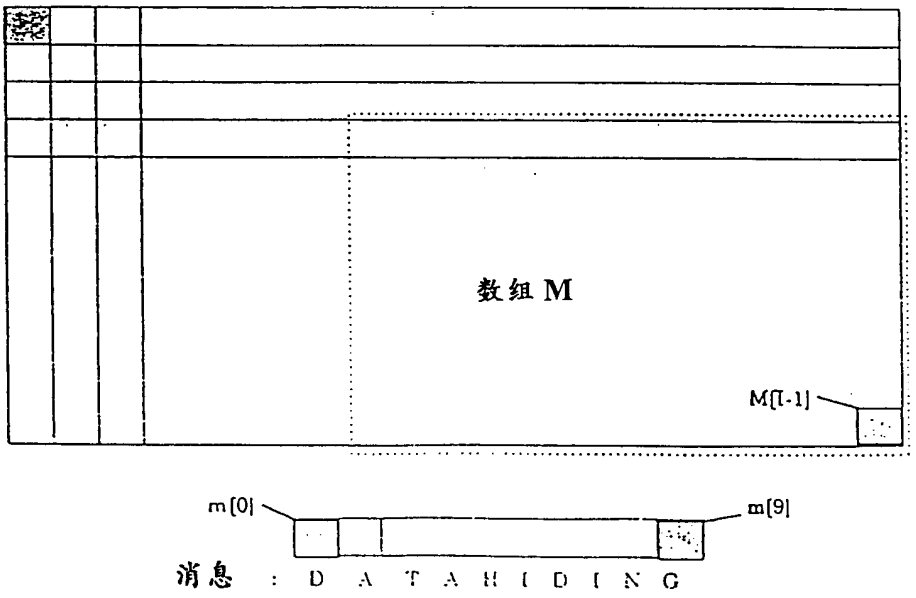

数组 M
M[I-1]
m[0]
m[9]
消息 : D A T A H I D I N G

图 4

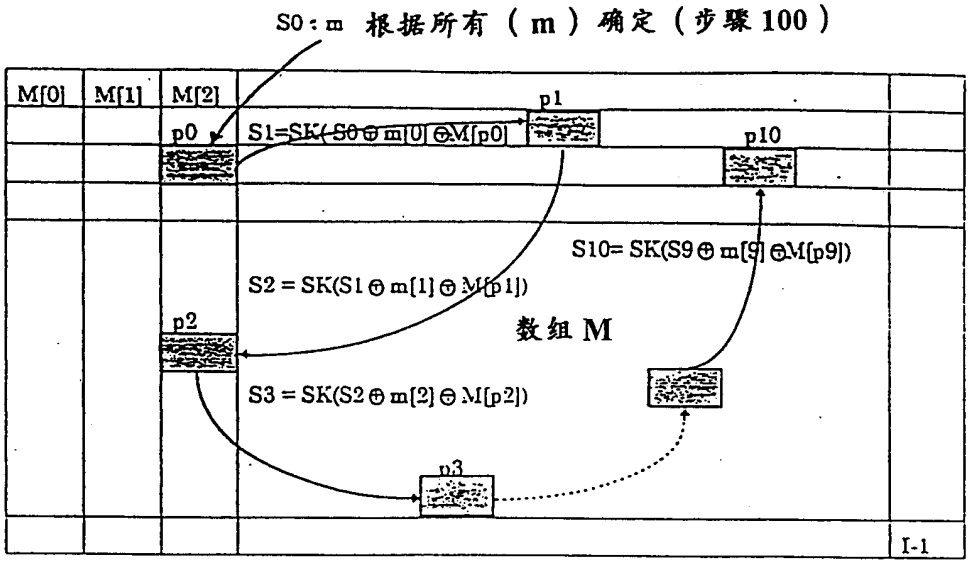

S0：m 根据所有（m）确定（步骤 100）
M[0]
M[1]
M[2]
p0
p1
p10
S1=SK(S0⊕m[0]⊕M[p0]
S10= SK(S9⊕m[9]⊕M[p9])
S2 = SK(S1⊕m[1]⊕M[p1])
p2
数组 M
S3 = SK(S2⊕m[2]⊕M[p2])
p3
I-1

图 10

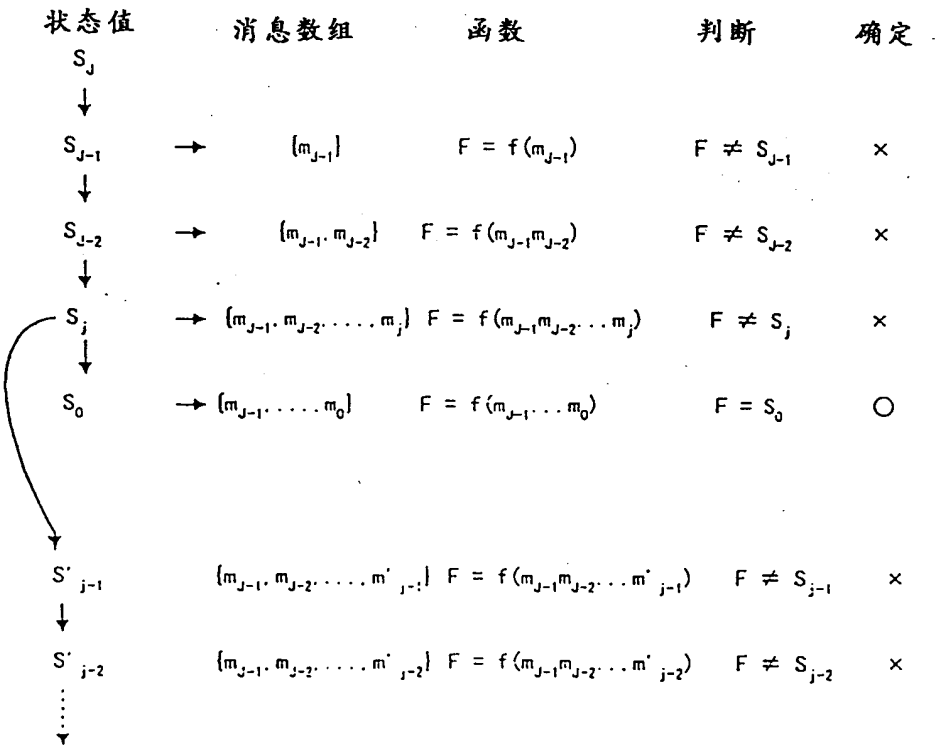

状态值
消息数组
函数
判断
确定
S_J
S_{J-1} → $\{m_{J-1}\}$ $F = f(m_{J-1})$ $F \neq S_{J-1}$ ×
S_{J-2} → $\{m_{J-1}, m_{J-2}\}$ $F = f(m_{J-1}m_{J-2})$ $F \neq S_{J-2}$ ×
S_j → $\{m_{J-1}, m_{J-2}, \ldots, m_j\}$ $F = f(m_{J-1}m_{J-2}\ldots m_j)$ $F \neq S_j$ ×
S_0 → $\{m_{J-1}, \ldots, m_0\}$ $F = f(m_{J-1}\ldots m_0)$ $F = S_0$ ○
S'_{j-1} $\{m_{J-1}, m_{J-2}, \ldots, m'_{j-1}\}$ $F = f(m_{J-1}m_{J-2}\ldots m'_{j-1})$ $F \neq S_{j-1}$ ×
S'_{j-2} $\{m_{J-1}, m_{J-2}, \ldots, m'_{j-2}\}$ $F = f(m_{J-1}m_{J-2}\ldots m'_{j-2})$ $F \neq S_{j-2}$ ×

图 5

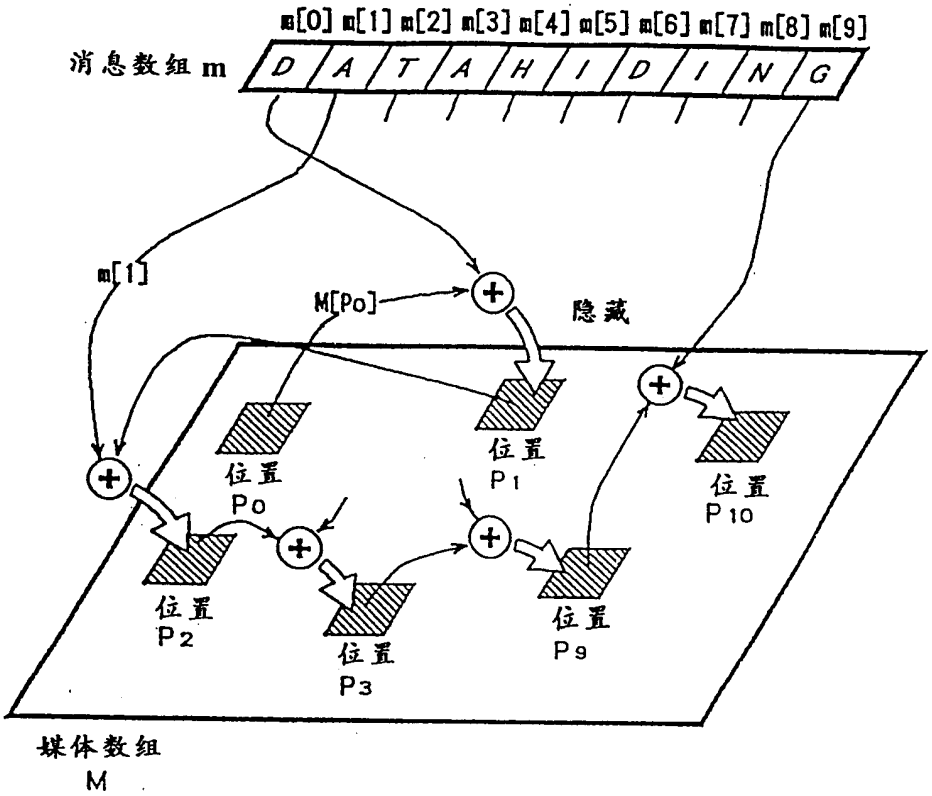

m[0] m[1] m[2] m[3] m[4] m[5] m[6] m[7] m[8] m[9]
消息数组 m
D A T A H I D I N G
m[1]
M[Po]
隐藏
位置
Po
位置
P1
位置
P10
位置
P2
位置
P3
位置
P9
媒体数组
M

图 6

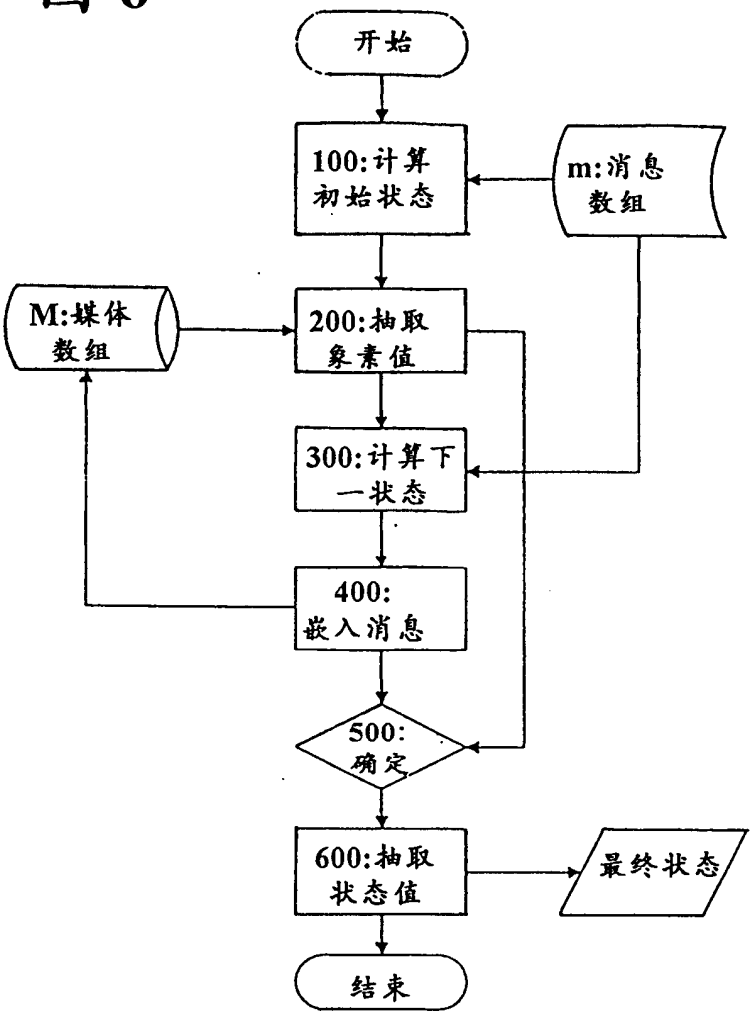

开始
100:计算初始状态
m:消息数组
M:媒体数组
200:抽取象素值
300:计算下一状态
400:嵌入消息
500:确定
600:抽取状态值
最终状态
结束

图 7

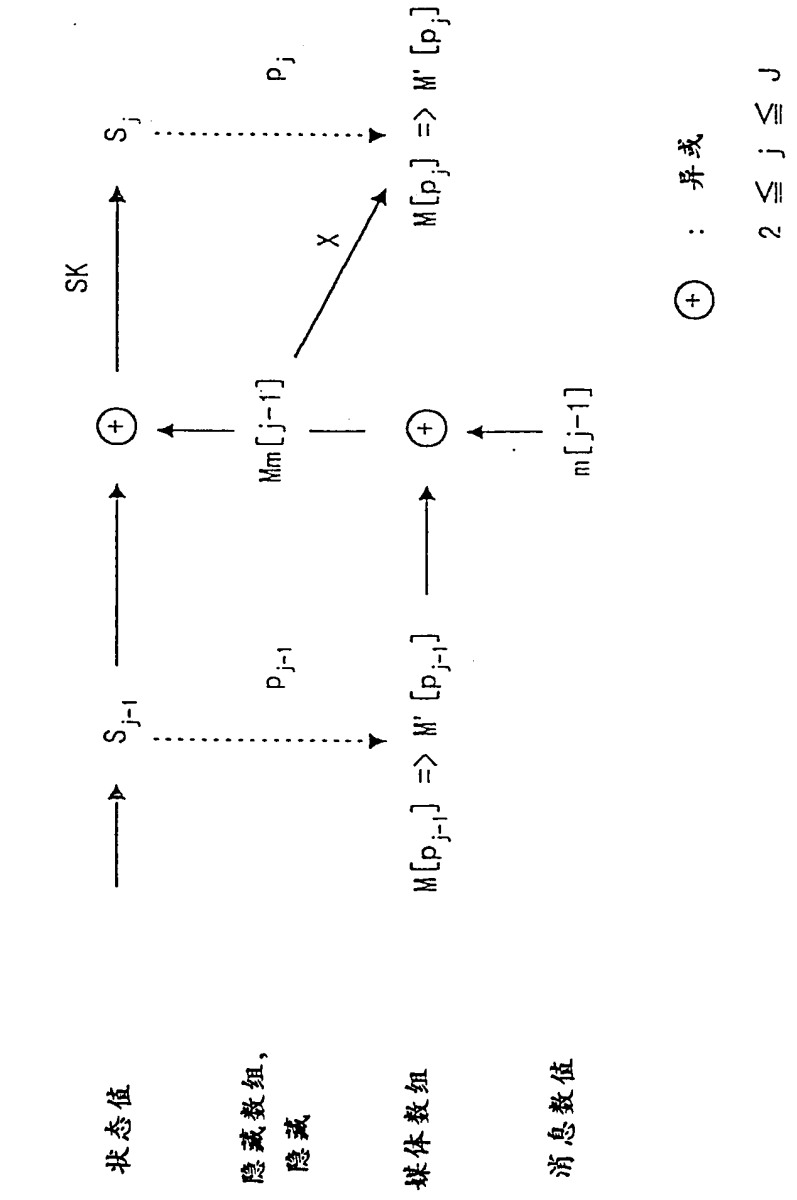

状态值
隐藏数组，
隐藏
媒体数组
消息数值
S_{j-1}
S_j
SK
p_{j-1}
p_j
Mm[j-1]
X
m[j-1]
$M[p_{j-1}] \Rightarrow M'[p_{j-1}]$
$M[p_j] \Rightarrow M'[p_j]$
⊕ : 异或
$2 \leq j \leq J$

图 8

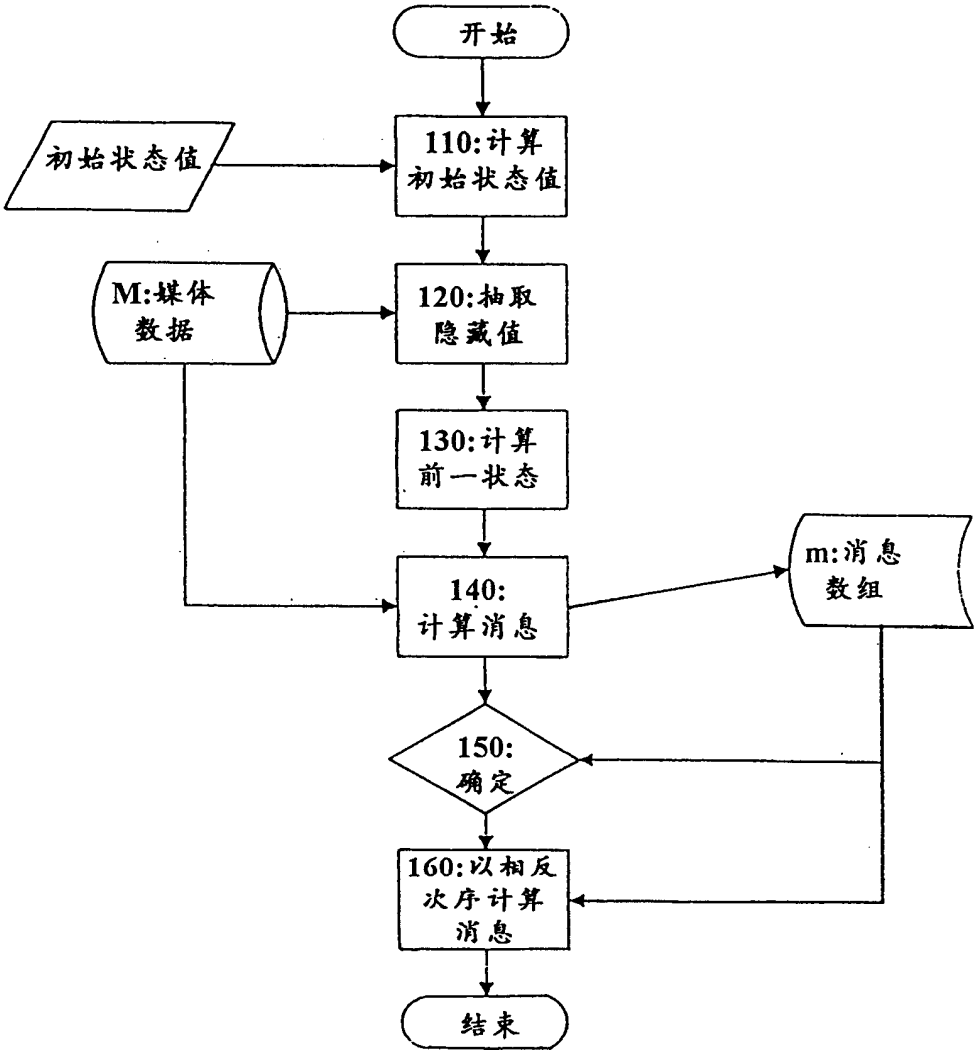

开始
初始状态值
110:计算初始状态值
M:媒体数据
120:抽取隐藏值
130:计算前一状态
m:消息数组
140:计算消息
150:确定
160:以相反次序计算消息
结束

图 9

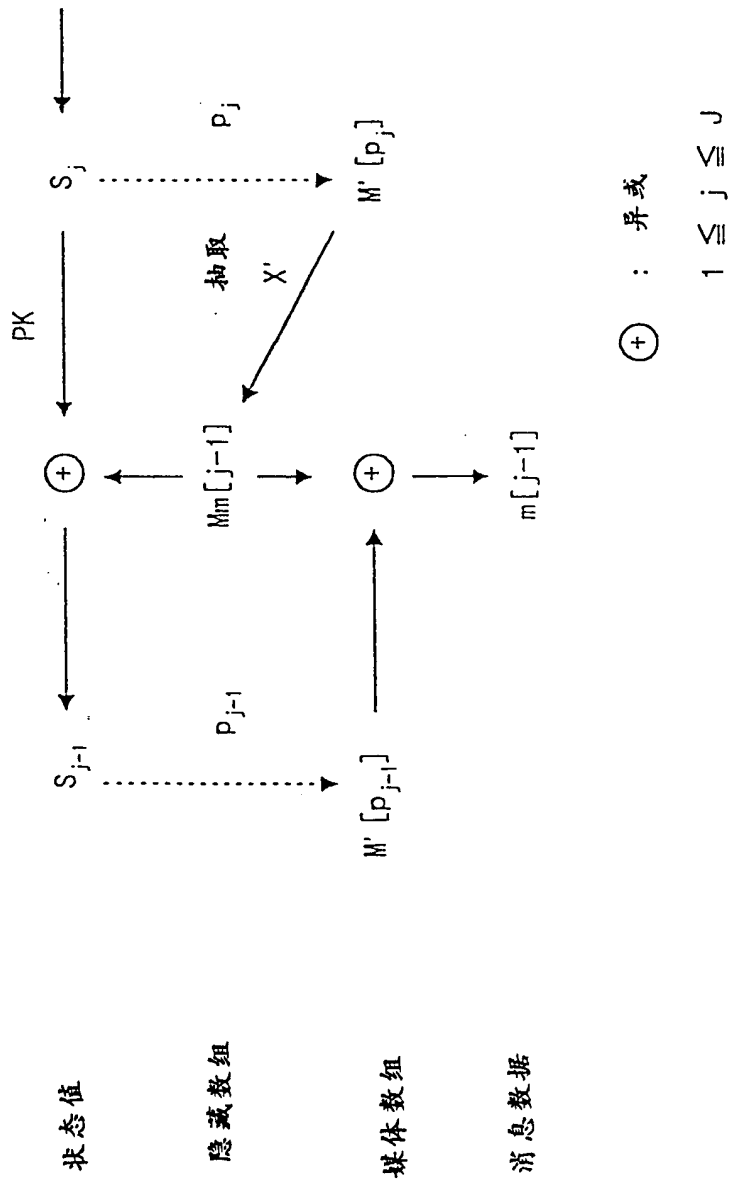


图 11

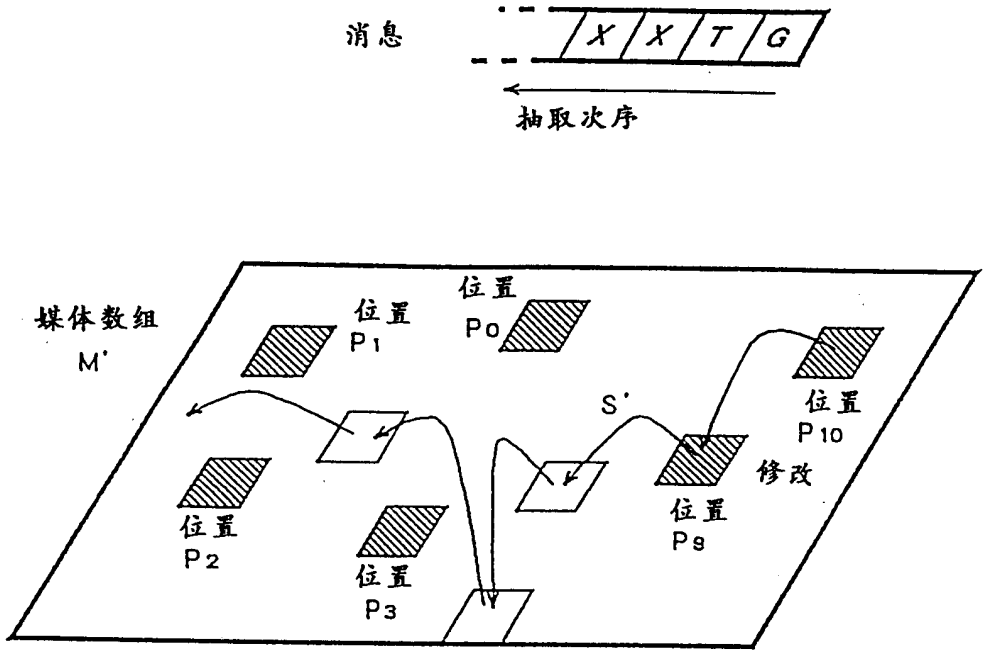


图 12

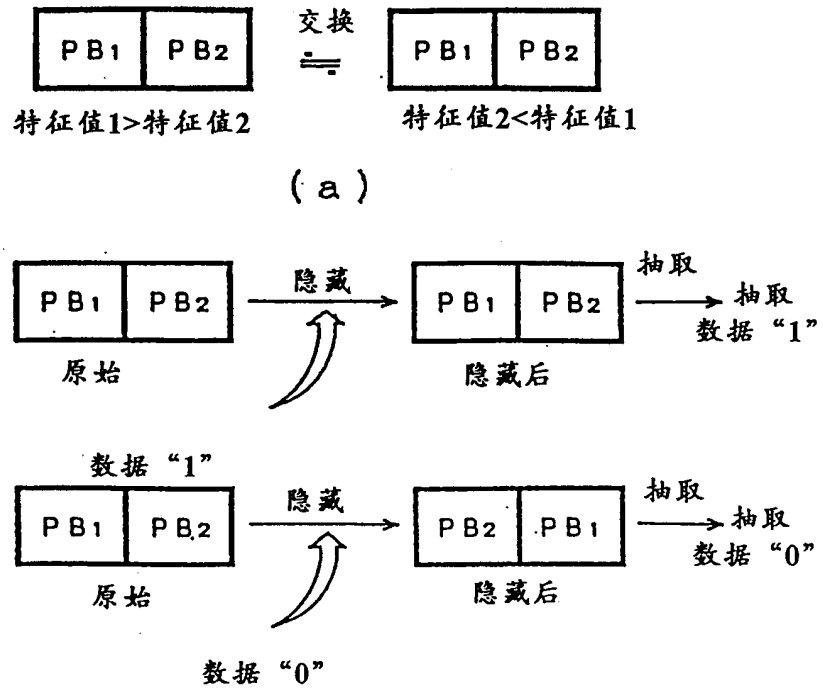

PB1
PB2
交换
特征值1>特征值2
特征值2<特征值1
(a)
隐藏
抽取
抽取
数据“1”
原始
隐藏后
数据“1”
数据“0”
(b)
h1
d1
d2
交换
h2
d2
d1
(c)

图 13

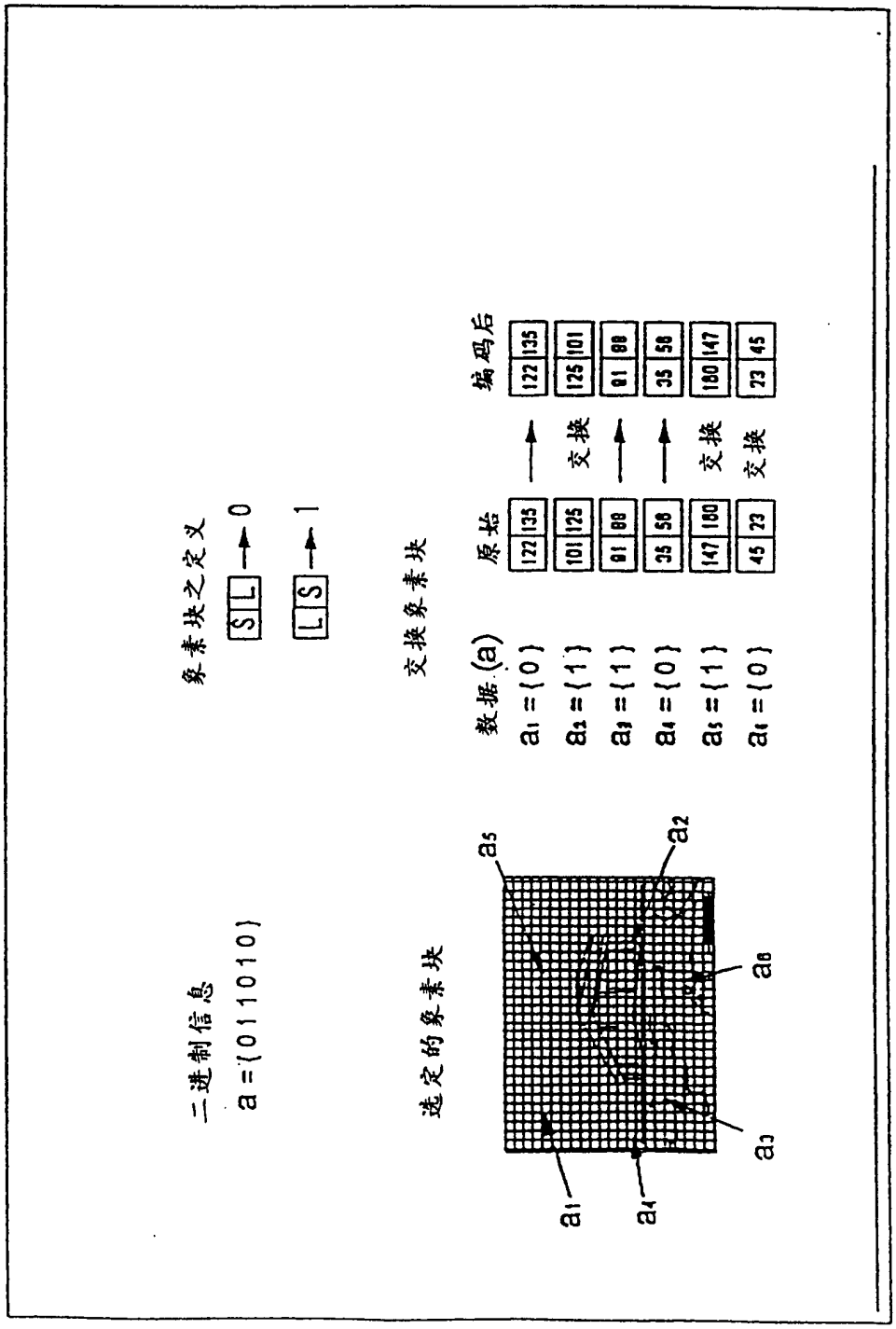

二进制信息
a={011010}
象素块之定义
SL → 0
LS → 1
交换象素块
选定的象素块
数据(a)
原始
编码后
a1={0}
a2={1}
a3={1}
a4={0}
a5={1}
a6={0}
122 135
101 125
01 88
35 58
147 180
45 23
125 101
01 88
35 58
180 147
23 45
交换
交换
交换
a1
a2
a3
a4
a5
a6

图 14

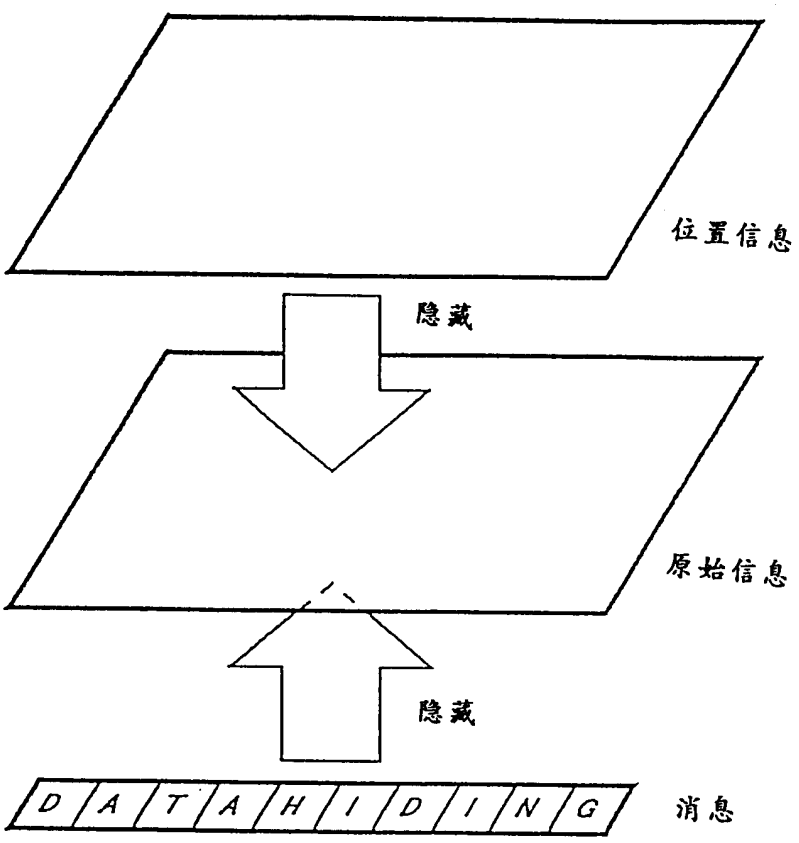


图 15

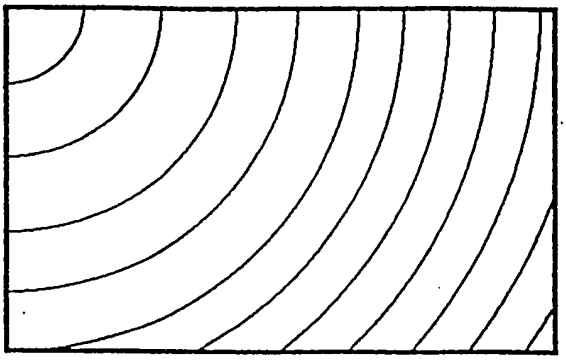


图 16

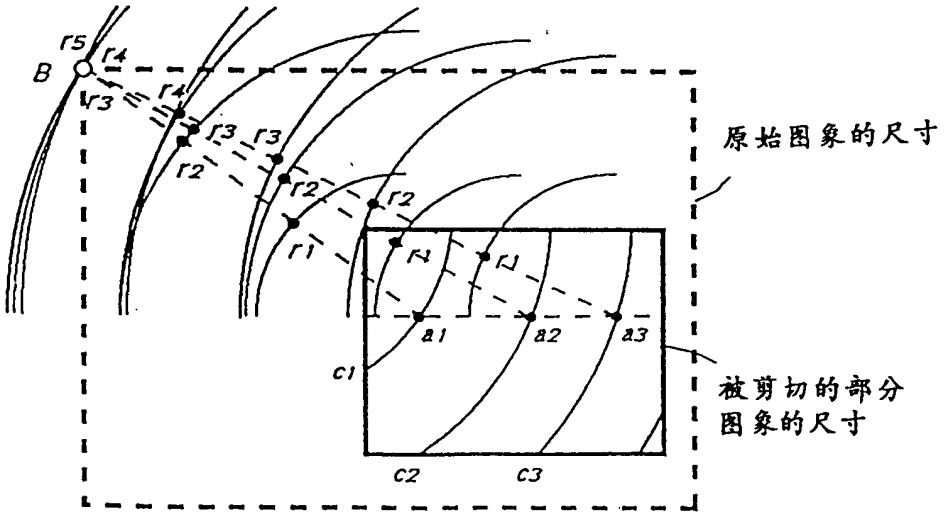


图 17

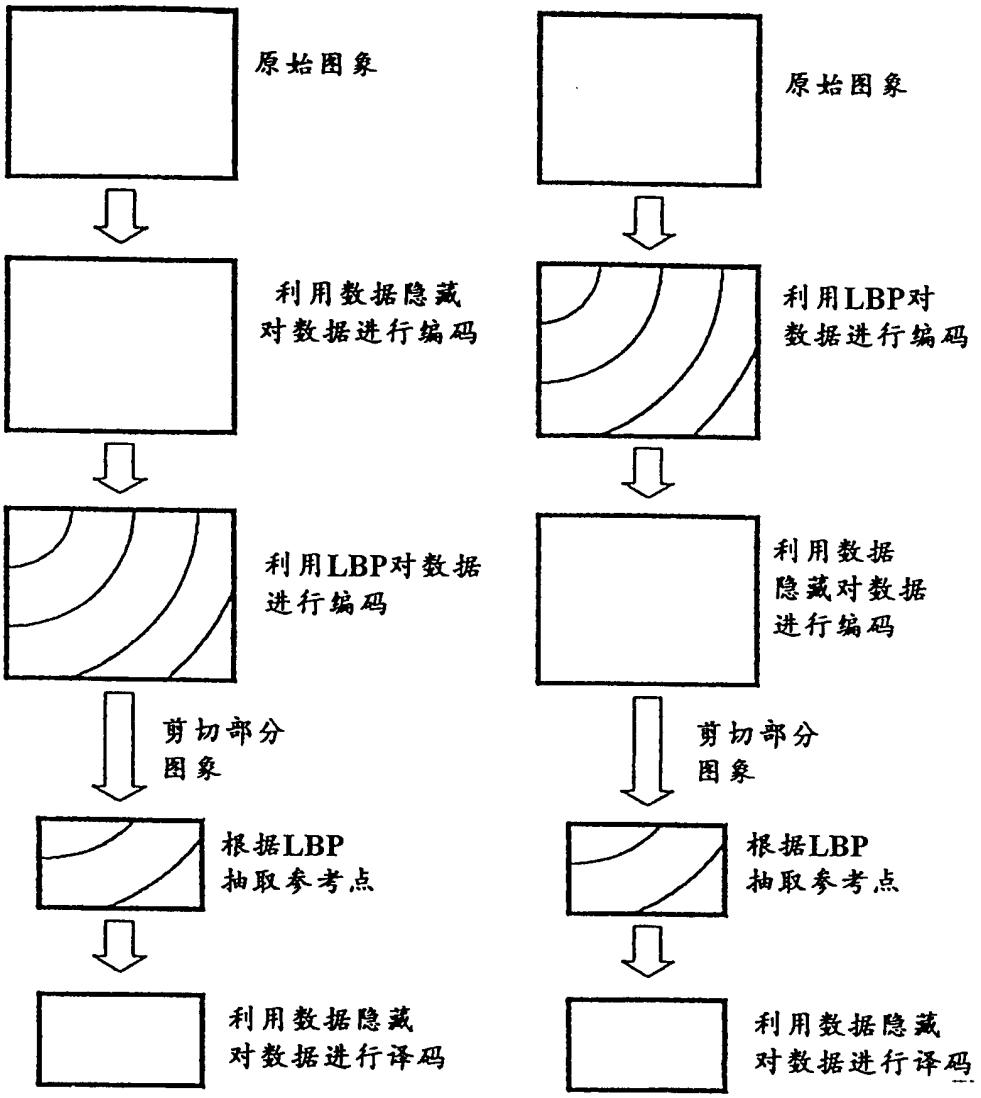

原始图象
利用数据隐藏
对数据进行编码
利用LBP对数据
进行编码
剪切部分
图象
根据LBP
抽取参考点
利用数据隐藏
对数据进行译码
(a)数据隐藏→
同心圆弧嵌入
原始图象
利用LBP对
数据进行编码
利用数据
隐藏对数据
进行编码
剪切部分
图象
根据LBP
抽取参考点
利用数据隐藏
对数据进行译码
(b) 同心圆弧嵌入
→数据隐藏

图 18

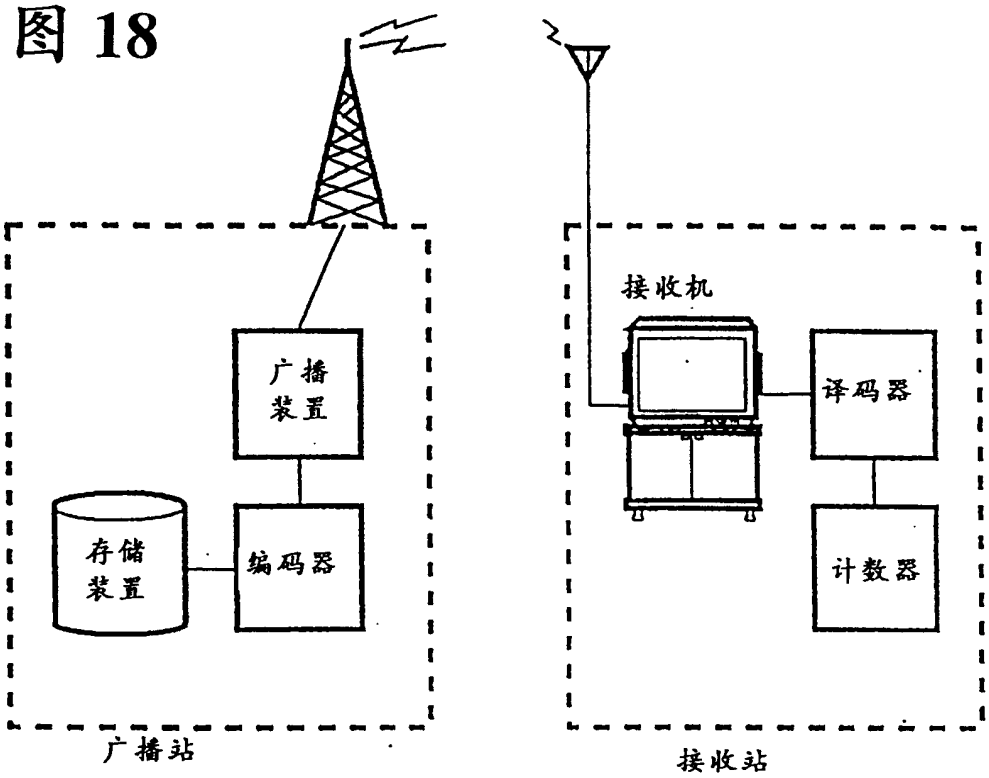

广播装置
存储装置
编码器
广播站
接收机
译码器
计数器
接收站

图 19

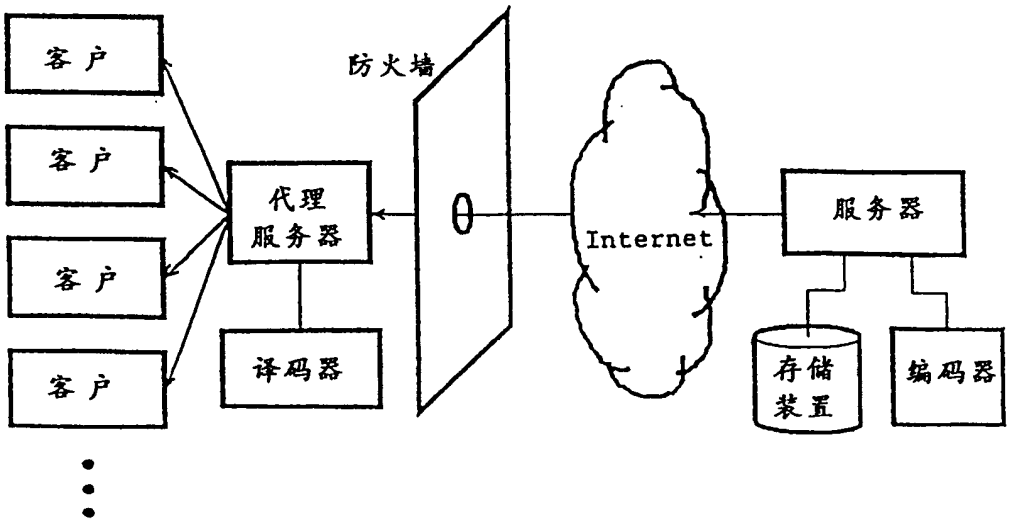

客户
客户
客户
客户
代理服务器
译码器
防火墙
Internet
服务器
存储装置
编码器

图 20

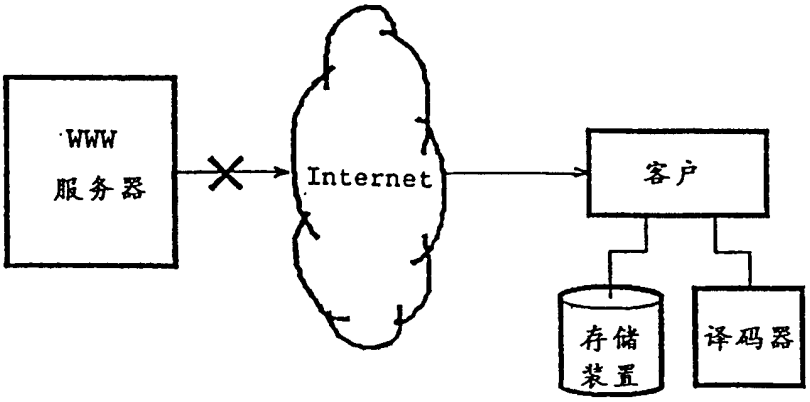


图 21

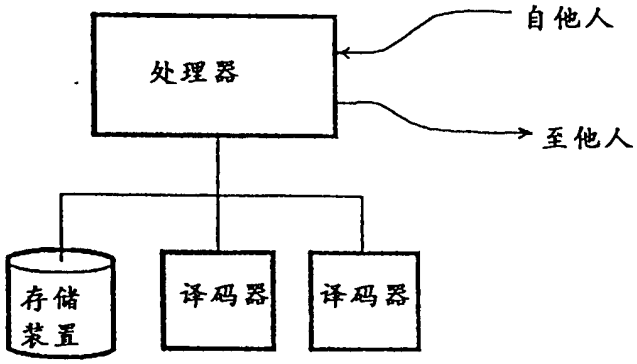


图 22

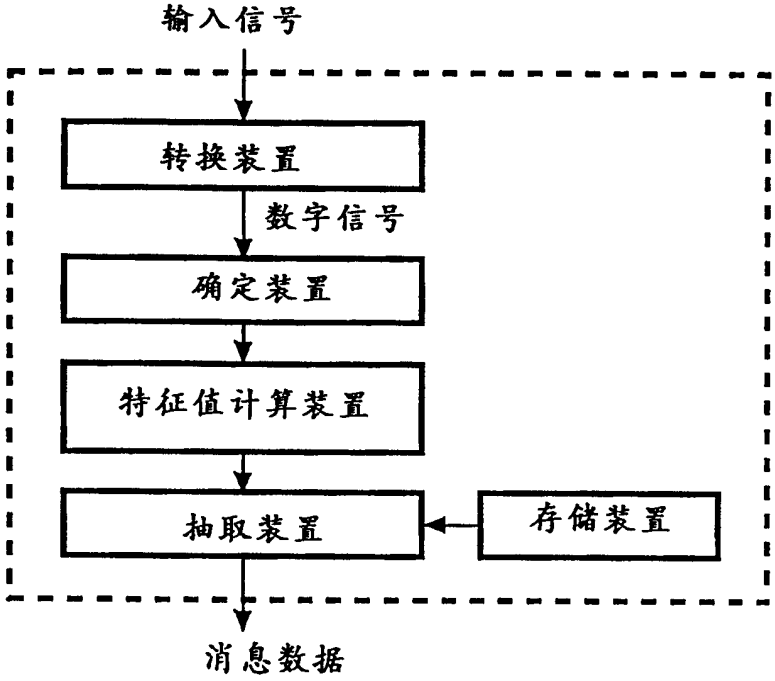
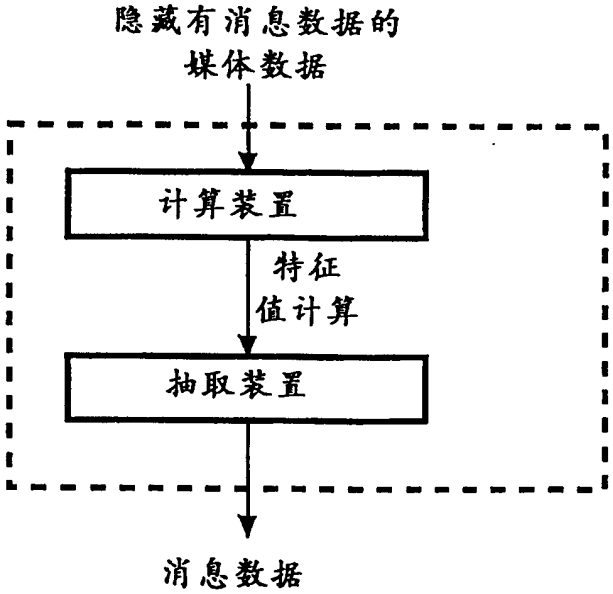

输入信号
转换装置
数字信号
确定装置
特征值计算装置
抽取装置
存储装置
消息数据

图 23


隐藏有消息数据的
媒体数据
计算装置
特征
值计算
抽取装置
消息数据