



[12] 发明专利申请公开说明书

[21] 申请号 03813955.3

[43] 公开日 2005 年 8 月 31 日

[11] 公开号 CN 1663231A

[22] 申请日 2003.6.11 [21] 申请号 03813955.3

[30] 优先权

[32] 2002.6.17 [33] EP [31] 02077459.2

[86] 国际申请 PCT/IB2003/002569 2003.6.11

[87] 国际公布 WO2003/107653 英 2003.12.24

[85] 进入国家阶段日期 2004.12.16

[71] 申请人 皇家飞利浦电子股份有限公司

地址 荷兰艾恩德霍芬

[72] 发明人 A·A·C·M·卡克

F·M·J·威廉斯

[74] 专利代理机构 中国专利代理(香港)有限公司

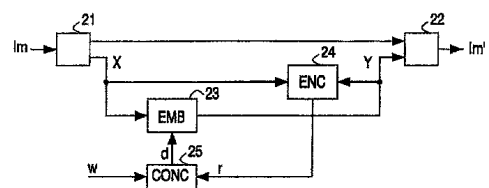
代理人 李亚非 刘杰

权利要求书 2 页 说明书 11 页 附图 4 页

[54] 发明名称 无损数据嵌入

[57] 摘要

水印或数据隐藏方案有一个不期望的副作用，那就是宿主信号失真。本发明公开了一种可逆或无损数据隐藏方案，它允许(在没有附加信令的情况下)完整并隐蔽地重建宿主信号(X)。在给出了复合信号的情况下，这可以通过在带有水印的嵌入数据(d)中提供识别宿主信号的恢复数据(r)来实现，也就是说，所述恢复数据识别(24)在嵌入(23)过程中宿主信号受到何种修改。所述恢复数据是在常规嵌入器(23)的一部分嵌入容量中接纳的。而剩余容量则被用于嵌入净荷(w)。



1. 一种在宿主信号中嵌入辅助数据的方法，该方法包括以下步骤：
骤：

5 使用一个具有给定嵌入比率和失真的预定数据嵌入方法来产生一个复合信号；

使用所述嵌入比率的一部分来接纳恢复数据，其中所述恢复数据识别那些取决于所述复合信号的宿主信号；以及
使用剩余嵌入比率来嵌入所述辅助数据。

10 2. 如权利要求 1 所述的方法，还包括以下步骤：
将宿主信号分成连续分段；

将预定的数据嵌入方法应用于所述分段；

在一个分段中接纳用于先前分段的恢复数据。

3. 如权利要求 2 所述的方法，其中，每一个分段都包含了用于所述先前分段的恢复数据以及辅助数据。

15 4. 如权利要求 2 所述的方法，还包括以下步骤：

(a) 在一个给定长度的分段中只提供辅助数据；

(b) 在后续分段中接纳仅仅用于先前分段的恢复数据；

(c) 使所述后续分段的长度适于其中嵌入的恢复数据量；

(d) 将步骤 (b) 和 (c) 重复预定的次数。

20 5. 如权利要求 4 所述的方法，其中，所述步骤 (d) 包括重复步骤 (b) 和 (c)，直到后续分段长度小于一个预定阈值为止。

6. 一种用于在宿主信号 (X) 中嵌入辅助数据 (w) 的设备，所述设备包括：

25 预定数据嵌入器 (23)，它具有给定的嵌入比率和失真，以便产生一个带有嵌入数据 (d) 的复合信号 (Y)；

用于生成对取决于复合信号 (Y) 的宿主信号 (X) 进行识别的恢复数据 (r) 的装置 (24, 25)；以及

用于在所述嵌入数据 (d) 的一部分中接纳所述恢复数据 (r) 以及在所述嵌入数据的剩余部分中提供所述辅助数据 (w) 的装置 (26)。

30 7. 一种从复合信号中重建宿主信号的方法，其中所述复合信号表示的是其中嵌入了数据的所述宿主信号的失真版本，所述方法包括以下步骤：

从复合信号中重现嵌入数据；
将嵌入数据分离成恢复数据和辅助数据；
在给出了复合信号的情况下，通过使用重建数据来重建宿主信号。

5 8. 如权利要求 7 所述的方法，还包括以下步骤：

将复合信号分成连续的分段；
使用分段中接纳的恢复数据来重建宿主信号的先前分段。

9. 如权利要求 8 所述的方法，其中，复合信号的每个分段都包含了宿主信号的所述先前分段的恢复数据以及辅助数据。

10 10. 一种用于从复合信号 (Y) 中重建宿主信号 (X) 的设备，其中所述复合信号 (Y) 表示的是其中嵌入了数据 (d) 的所述宿主信号的失真版本，所述设备包括：

用于从复合信号 (Y) 中重现嵌入数据 (d) 的装置 (43)；

15 用于将嵌入数据 (d) 分离为恢复数据 (r) 和辅助数据 (w) 的分离装置 (44)；

在给出复合信号 (Y) 的情况下，使用重建数据 (r) 来重建宿主信号 (X) 的重建装置 (46)。

20 11. 一种具有嵌入数据 (d) 的复合信息信号 (Y)，其中所述嵌入数据包含恢复数据 (r) 和辅助数据 (w)，所述恢复数据识别取决于所述复合信号的宿主信号 (X) 的失真。

无损数据嵌入

发明领域

- 5 本发明涉及一种无损地将数据嵌入宿主信号的方法和设备。此外，本发明还涉及那些用于重现数据以及重建宿主信号的方法和设备。

发明背景

- 10 很多水印和数据隐藏方案都有一个不好的副作用，即嵌入了辅助数据的复合信号（例如图像、视频、音频）将会出现失真。因此，寻找嵌入数据量与所引发失真之间的最优平衡点就成了一个非常活跃的研究领域。而在理解水印及数据隐藏方案的容量-失真的基本限制的过程中也已经取得了相当大的进展。

- 15 有时，人们不仅希望得到只有少量失真的嵌入数据，而且还希望能够彻底地消除所述失真。提供这种能力的嵌入方案则称为无损或可逆数据隐藏或嵌入方案。如果不允许初始宿主信号降级，那么无损数据隐藏方案将是非常重要的。举例来说，这种情况对于医学成像和贵重原著的多媒体存档而言都是成立的。

- 20 在下面这篇文章中公开了一种已知的无损数据隐藏方法：Jessica Fridrich、Miroslav Goljan 和 Rui Du, “Lossless Data Embedding for all Image Formats”, Proceedings of SPIE, Security and Watermarking of Multimedia Contents, San Jose, California, 2002。在这种已知的方法中，信号 X 的一个特征或子集 B（例如位图
- 25 图像的最低有效位平面，或是 JPEG 图像的特定 DCT 系数的最低有效位）是从信号 X 中提取出来的并且经历了无损压缩。经过压缩的子集 B 与辅助数据（净荷）级联并且被插入到信号 X 中，以便取代初始子集。该方法基于这样一种假设，那就是在保持信号 X 的感观质量的同时，可以对子集 B (i) 无损压缩以及 (ii) 随机化。

- 30 在接收机一端则可以通过使用常规设备来再现这种失真的复合信号。为了完全去除该失真，将会提取并解压缩那些包含压缩子集的级联比特流。随后则将初始子集 B 重新插入到信号 X 中。

Fridrich 等人的论文虽然公开了无损数据隐藏的实际实例，但是根本没有注意到无损嵌入方案的理论极限。

发明目的和概述

5 本发明的一个目的是提供那些在比率-失真方面更为有效的无损数据嵌入方案。

为此目的，本发明提供了一种用于将辅助数据嵌入宿主信号的方法和设备，所述方法包括如下步骤：使用一个具有给定嵌入比率和失真的预定数据嵌入方法来产生一个复合信号；使用一部分所述嵌入比率来接纳恢复数据，其中所述恢复数据识别的是那些取决于复合信号的宿主信号；以及使用剩余的嵌入比率来嵌入辅助数据。

本发明利用的是这样一种见解，那就是在给出了接收到的复合信号的情况下，接收机有能力消除初始宿主信号的不确定性。消除不确定性所需要的数据量要小于对初始宿主信号本身进行编码所需要的数据量。此外，发明人还用公式表示了无损数据嵌入容量的理论极限。

附图简述

图 1 显示了一个表示无损数据嵌入方案的极限的图示。

20 图 2 示意性显示了根据本发明而在宿主信号中无损嵌入辅助数据的设备的图示。

图 3 显示了一个对依照本发明的无损数据嵌入设备的实施例的性能进行描述的图示。

25 图 4 显示的是一个根据本发明来重建宿主信号的设备的示意图。

图 5 和 6 描述的是根据本发明而在宿主信号中接纳恢复数据的实施例。

图 7 和 8 显示的是描述对称与非对称信道之间差别的图示。

30 优选实施例的描述

这里首先对现有技术的压缩和比特替换方案进行更一般的论述。Fridrich 等人的信号源产生一个信号采样序列，例如图像像素。

所压缩信号的子集 B (位平面, 特定 DCT 系数的最低有效比特位) 构成了一个二进制符号源 $x_1 \dots x_N$ 。假设概率 $p_0 = \Pr\{x=0\}$ 与 $p_1 = \Pr\{x=1\}$ 并不相等, 也就是说, 信源熵 $H(p_0) = -p_0 \log_2(p_0) - p_1 \log_2(p_1)$ 小于 1。在这种情况下, 信息论中的教导是可以将 N 个符号的序列压缩成一个具有 $K = N \times H(p_0)$ 个符号的更短序列 $y_1 \dots y_K$ 。现在, 通过将 $N \times (1 - H(p_0))$ 个辅助数据符号附加于序列 $y_1 \dots y_K$, 可以获取一种可逆的数据隐藏方案。举例来说, 如果 $p_0 = 0.9$ 并且 $p_1 = 0.1$, 那么信源熵将是 $H(p_0) \approx 0.47$, 由此 (对很大的 N 来说) 只需要 $0.47 \times N$ 个比特就能表示初始宿主符号。相应地, 在这里也可以将 $0.53 \times N$ 个辅助数据符号作为净荷嵌入序列 $y_1 \dots y_N$ 的剩余部分。在解码器一端, 初始序列 $x_1 \dots x_N$ 是通过解压缩 $y_1 \dots y_K$ 而得到恢复的。序列的剩余部分 $y_{K+1} \dots y_N$ 则解译成了辅助数据。

对 Fridrich 等人的嵌入方案来说, 其数据比率是 $R = 1 - H(p_0)$ 比特/采样。由于压缩序列 $y_1 \dots y_K$ 的各位与 $x_1 \dots x_N$ 的各位不相关并且辅助数据是随机选择的, 因此很容易看出: $x_1 \dots x_N$ 与 $y_1 \dots y_N$ 之间的失真 $D = 0.5$ 。只要对 $x_1 \dots x_N$ 中的一小部分 α 的符号进行构造, 就可以减少 Fridrich 等人的方案中的失真。这种处理称为时间共享技术。然后, 数据比率和失真都会下降因数 α 。这种“简单”的时间共享嵌入方案的最终数据比率和失真分别是 $R = \alpha(1 - H(p_0))$ 以及 $D = \alpha/2$, 或者

$$R_{\text{simple}}(D) = 2D(1 - H(p_0)) \quad (1)$$

在图 1 中, $p_0 = 0.9$ 的线性比率失真函数显示为点划线 11。

发明人已经发现: 线性等式 (1) 并不是最优的。他们已经发现了无损数据嵌入容量的理论极限。更为特别的是, 对用于无记忆二进制信源的可逆嵌入方案和 $p_0 \geq 0.5$ 的情况而言, 可以实现的数据比率 R_{rev} 是:

$$R_{\text{rev}} = H(\max(p_0 - D, 0.5)) - H(p_0) \quad (2)$$

其中 $0 \leq D \leq 0.5$

就 $p_0 = 0.9$ 的情况而言, 这个比率失真函数是作为实线 12 而在图 1 中显示的。等式 (2) 一般适用的是非对称信道 (发明人将“信道”这一概念用于数据嵌入器)。而对那些对称信道而言, 所述比率为:

$$R_{\text{sym}} = H(p_0 + (1 - 2p_0)D) - H(p_0) \quad (3)$$

就 $p_0 = 0.9$ 的情况而言, 这个比率失真函数是作为虚线 13 而在图

1 中显示的。对称信道的嵌入比率始终介于最佳嵌入比率与时间共享嵌入比率之间。稍后将会给出关于对称和非对称信道的实用范例。在图 1 中，线条 11、12 和 13 涉及的是 $p_0=0.9$ （以及 $p_1=0.1$ ）。出于示例目的，在这里还显示了 $p_0=0.8$ 的相似线条 14、15 和 16。

5 图 2 显示的是依照本发明的无损数据嵌入设备的概括性示意图。该设备接收图像 I_m 这类感知宿主信号的数字表示。提取级 21 从中提取一个将要嵌入辅助数据的宿主符号序列 $X=\{x_1 \dots x_N\}$ 。与 Fridrich 等人的嵌入方案相类似的是，所述宿主信号可以通过从图像中提取位平面或特定 DCT 系数的最低有效位来获取。

10 该设备还包括一个数据嵌入器 23，从嵌入器引入宿主信号失真这个意义上讲，所述数据嵌入器是一个常规设备。此外通常是使用“均方误差(squared error)”来表示所述失真的：

$$D(x, y) = (y - x)^2$$

15 嵌入过程将会产生一个复合信号 $Y=\{y_1 \dots y_N\}$ 。一开始，假设宿主信号 X 与复合信号 Y 都是结合了字母表 $\{0, 1\}$ 的二进制信号。插入级 22 会将复合信号 Y 回插到图像中，以便获取一个印有水印的图像 I_m' 。

20 恢复编码器 24 接收宿主信号 X 和复合信号 Y 。恢复编码器保持了对哪些宿主符号进行何种修改的记录，并且将所述信息编码到恢复数据 r 中。在这里必须对关于“对哪些宿主符号进行何种修改”的表述进行概括性的解释。如果失真是 $D=0$ 或 $D=1$ （这是本实施例中的情况），那么它有能力识别哪些符号遭受到失真。而对其它类型的嵌入器 23 来说，其中还必须对失真量进行编码。应该注意的是，恢复编码器 24 表示的是本发明的一个功能性特征。同样，所述电路无需以物理方式给出。在以下介绍的关于设备的实用实施例中，关于哪些符号出现失真的信息固有地由嵌入器 23 自身所产生。

25 在这里将会显示，以比特/符号为单位的恢复数据比率要小于嵌入器 23 的嵌入比率。而剩余嵌入容量则被用于嵌入辅助数据（净荷） w 。恢复数据 r 与净荷 w 是在级联电路 25 中级联的。此外，出于嵌入目的而被应用于嵌入器 23 的是级联数据 d 。

30 在该设备的一个优选实施例中，嵌入器 23 是依照下述论文中的教导来操作的：M. van Dijk 和 F.M.J. willems, “Embedding

Information in Gray scale Images”, Proceedings of the 22nd Symposium on Information Theory in the Benelux, Enschede, The Netherlands, 2001 年 5 月 15~16 日, pp.147-154。在这篇论文中, 作者描述了具有高效的比率-失真比率的有损嵌入方案。更为特别的是, 这其中将数量为 L ($L>1$) 的宿主信号采样聚集在一起, 从而提供了一个宿主符号块或矢量。块中的宿主符号是以这样一种方式修改的, 其中所述块的校正子代表了一个或多个 (但是少于 L) 嵌入消息符号 d 。

在纠错领域中, 表述“检验子”是一个众所周知的概念。在纠错方案中, 接收数据字的检验子是通过将接收数据字与给定矩阵相乘而被确定的。如果检验子为零, 那么数据字是正确的。如果检验子不等于零, 那么所述非零值表示的是出错数据字符的位置 (或多个位置)。汉明纠错码具有大小为 3 的汉明距离。它们能够纠正 1 个出错的数据符号。诸如戈莱码之类的其他编码则允许纠正数据字的多个符号。

从数学角度来看, M. van Dijk 等人所教导的数据嵌入方法与纠错技术相类似。为了将消息符号 d 嵌入一个具有 L 个宿主符号 $x_1 \dots x_L$ 的块中, 嵌入器修改了该块的一个或多个宿主符号。输出块 $y_1 \dots y_L$ 是以数学方式计算得到的, 所述输出块具有预期的检验子, 以及从汉明码的意义上讲, 它是最接近 $x_1 \dots x_L$ 的。作为实例, 现在将对使用了块长 $L=3$ 的汉明码的数据嵌入处理进行简要概述。

为了计算 3 比特的块或矢量的检验子, 所述矢量将与以下的 3×2 奇偶校验矩阵相乘:

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

25 应该注意的是, 所有数学运算都是模 2 运算。例如, 输入矢量 (001) 的检验子是 (11), 因为

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

30 这个检验子 (11) 表示的是被嵌入的数据。很明显, 宿主矢量的检验子通常并不是所要嵌入的消息。因此必须对其中一个宿主符号进行修改。举例来说, 如果所要嵌入的是消息 (01) 而不是 (11), 那

么嵌入器 23 将会改变第二个宿主符号，由此将初始宿主矢量 (001) 改为 (011)：

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- 对这种依照三个符号的嵌入方案来说，其失真为 $\frac{1}{4} \cdot 0^2 + \frac{3}{4} \cdot 1^2 = \frac{3}{4}$ (宿主符号不变的概率是 1/4，其中一个符号改变了 ± 1 的概率是 3/4)，这样一来，每个符号的平均失真是 $D=1/4$ 。嵌入比率是 2 比特/块，即 $R=2/3$ 比特/符号。在图 3 中，相应 (R,D) 对是由 302 所表示的标记+来显示的。

- 在一种类似方式中，可以将 3 个数据比特嵌入一个具有 7 个信号符号的块，并且可以将 4 个比特嵌入 15 个信号符号等等。更一般来说，基于汉明码的嵌入方案允许通过修改至多一个宿主符号而在具有 $L=2^m-1$ 个宿主符号的块中嵌入 m 个消息符号。嵌入比率为：

$$R = \frac{m}{2^m - 1}$$

并且失真为：

$$D = \frac{1}{2^m}$$

- 图 3 把与 $m=2, 3, \dots, 6$ 相对应的 (有损，不可逆) 嵌入方案的相应 (R,D) 对显示为 302、303、... 306 所示的标记+。在这里将对应于 $m=1$ (这是简单的比特替换) 的 (R,D) 对显示成由 301 表示的标记+。应该注意的是，(R,D) 的值不取决于二进制信源熵 $H(p)$ 。此外，图 3 还显示了 Fridrich 等人给出的 $p_0=0.9$ 的无损嵌入方案的 (R,D) 对 300 ($R=0.53$ 比特/符号， $D=0.5$)。作为参考，在图 3 中还显示了 $p_0=0.9$ (参看图 1) 的无损嵌入方案的理论极限 11、12 和 13。

- 依照本发明，现在使用了一部分嵌入消息数据比特 d 来识别是否修改了其中一个信号采样，如果是的话，则识别所修改的是哪一个信号采样。对块长为 3 ($m=2, L=3$) 的汉明码来说，这其中存在 4 种可能性：并未修改这三个宿主符号中的任何一个符号，修改了第一个符号，修改了第二个符号或者修改了第三个符号。如果信号源的熵 $H(p)$ 等于 1，那么所有事件都具有相同概率。这种情况下则需要恢复每一个块的嵌入消息比特。然而，如果信号源的熵 $H(p)$ 不等于 1，那么这

些事件将会具有不同概率，并且只有少于 m 个恢复比特是必需的。由此为宿主符号块中的被嵌入“真实”辅助数据比特（也称为净荷）留下了空间。

- 与 Fridrich 等人所给出的实例相类似的是，在这里假设 $p_0=0.9$ 。
- 5 相应地，信源产生宿主矢量(000)的概率 $P(x=000)$ 是 $(0.9)^3 \approx 0.729$ 。信源产生宿主矢量(001)的概率 $P(x=001)$ 是 $(0.9)^2 \times (0.1) \approx 0.081$ ，等等。假设所述设备的嵌入器 23 产生了一个复合矢量 $y=000$ 。初始宿主矢量 x 有可能是(000)。在这种情况下，没有一个初始信号采样已经被修改。然而，初始宿主矢量也可以是(001)、(010)或(100)。
- 10 这种情况下将会有有一个宿主信号已经被修改。如果产生 $y=000$ ，那么宿主矢量为 $x=000$ 的概率是：

$$p(x=000|y=000) = \frac{p(x=000)}{p(x=000) + p(x=001) + p(x=010) + p(x=100)} = 0.75$$

在一种相似方式中，可以对 $y=000$ 源自宿主矢量(001)、(010)或(100)的概率进行计算。这将会产生：

15 $p(x=001|y=000) = 0.083$

$$p(x=010|y=000) = 0.083$$

$$p(x=100|y=000) = 0.083$$

- 因此，每一个合成矢量都具有一个关联条件概率集合 $p(x|y)$ 。在下表中对其进行了概括。所述表格还包含了每一个块 y 的相应条件熵 $H(x|y)$ 。所述条件熵表示的是在给出了 y 的情况下的初始矢量 x 的不确定性。此外，该表还包含了在假设消息 00、01、10 和 11 具有相同概率 $1/4$ 的情况下的各个矢量 y 的概率 $p(y)$ 。举例来说，所述概率 $P(y=000)$ 是如下计算的：
- 20

$$p(y=000) = \frac{1}{4}p(x=000) + \frac{1}{4}p(x=001) + \frac{1}{4}p(x=010) + \frac{1}{4}p(x=100) = 0.2430$$

25

			$p(x y)$							
x	检验子	$P(x)$	$y=000$	$y=001$	$y=010$	$y=011$	$y=100$	$y=101$	$y=110$	$y=111$
000	00	0.729	0.7500	0.8804	0.8804		0.8804			
001	11	0.081	0.0833	0.0978		0.4709		0.4709		
010	10	0.081	0.0833		0.0978	0.4709			0.4709	
011	01	0.009		0.0109	0.0109	0.0523				0.3214

100 01	0.081	0.0833			0.0978	0.4709	0.4709
101 10	0.009		0.0109		0.0109	0.0523	0.3214
110 11	0.009		0.0109		0.0109		0.0523 0.3214
111 00	0.001			0.0058		0.0058	0.0058 0.0357
H(x y)=1.2075 0.6316 0.6316 1.2891 0.6316 1.2891 1.2891 1.7506							
p(y)= 0.2430 0.2070 0.2070 0.0430 0.2070 0.0430 0.0430 0.0070							

在给出了 y 的情况下, 在所有块 y 上求平均值的信源条件熵 $H(X|Y)$ 代表了重建 x 的比特数目。在本实例中, 所述平均熵等于:

$$H(X|Y) = \sum_y p(y)H(x|y) = 0.8642 \text{ 比特/块}$$

- 5 相应地, 在这里需要每个块都具有 0.8642 个恢复比特, 以便对初始块进行识别。由此将会为嵌入净荷留下 $2-0.8642=1.1358$ 比特/块。这样一来, 数据比率 R 为:

$$R = \frac{1.1358}{3} = 0.3786 \text{ 比特/符号}$$

- 10 应该注意的是, 现在指定给嵌入数据 d 的特定意义并不影响复合信号的失真 D 。如先前所述, 这种无损嵌入方案的失真是:

$$D=1/4$$

- 在图 3 中, 相应的 (R, D) 对是由 312 所表示的标记 $\diamond$ 来显示的。应该了解的是, 与 Fridrich 等人提出的具有相同失真 (参见 333) 的无损嵌入方案相比, 这种无损嵌入方案具有高出很多的嵌入比率 R 。
15 在类似方式中也可以对长度为 7、15、31、63 等等的汉明码的比率失真对进行计算。图 3 则将 $m=3\dots 6$ 的相应 (R, D) 对显示成由 313...316 所表示的标记 $\diamond$ 。

- 图 4 显示的是用于从接收到的复合信号中重建初始宿主信号的设备示意图。该设备接收一个带有水印的图像 Im' 。接收到的图像
20 则是初始图像 Im 的略带失真的版本。并且所述图像可以直接施加给一个再现设备, 以便进行显示。所述设备还包括一个从接收到的图像中提取嵌入了数据 d 的复合信号 $Y=\{y_1\dots y_N\}$ (例如给定位平面) 的提取级 41。该提取级 41 与图 2 所示的嵌入设备的提取级 21 是相同的。

- 25 复合信号 Y 施加给一个数据重现电路 43, 其中所述电路重现那些嵌入到复合信号中的数据 d 。在通过使用长为 L 的汉明码来嵌入数

据 d 的优选实施例中，所述重现电路 43 将会确定每一个符号块 $y_1 \dots y_L$ 的检验子。所提取的数据是级联的净荷 w 和恢复比特 r 。它们是在一个分离器 44 中分离的，其中所述分离器执行的是图 2 所示的级联电路 26 的逆操作。并且由此可以重现净荷 w 。

5 重建单元 45 使用恢复比特 r 以及复合信号 Y 来重建初始宿主信号 X 。在这里安排重建单元来消除应用于初始宿主信号 $X=x_1 \dots x_n$ 的一个或多个修改。在优选实施例中，恢复数据 r 识别是否修改了块 Y 中的一个符号，如果是的话，则识别所修改的是哪一个符号。在更常见的作法中，恢复数据识别的是符号 $y_1 \dots y_N$ 的失真 D 。最终，重建的宿主信号 X 由插入级 42 回插到图像中，以便获取初始图像 I_m 。所述插入级 42 与图 2 所示的嵌入设备的插入级 21 是相同的。

在上述实施例中，假设宿主信号 X 、复合信号 Y 以及数据符号都是结合了字母表 $\{0, 1\}$ 的二进制信号。然而，本发明并不局限于二进制信号。举例来说，在这里也可以使用 van Dijk 等人的论文中所公开的三元嵌入方案。在一个三元数据嵌入器中，数据符号属于字母表 $\{0, 1, 2\}$ 。更为特别的是：

信号采样值 $y=0, 3, 6 \dots$ 表示的是消息符号 $d=y \bmod 3=0$,

信号采样值 $y=1, 4, 7 \dots$ 表示的是消息符号 $d=y \bmod 3=1$ ，以及

信号采样值 $y=2, 5, 8 \dots$ 表示的是消息符号 $d=y \bmod 3=2$ 。

20 现在，数据嵌入器 23（参见图 2）接收初始图像信号（电路 21 和 22 是多余的），并且修改信号采样 x_i 的最低有效部分，从而使嵌入在已修改采样 y_i 中的数据将会是 d 。在针对二进制嵌入所描述的相似方式中，也可以将三元符号嵌入宿主符号组。同样，在这里也可以使用（三元）汉明码或（三元）戈莱码来完成这个操作。在申请人提交的未公开的国际专利申请 IB02/01702（律师案卷号 PHNL010358）中描述了与之相关的实例。

在另一个数据嵌入方案中，消息符号 d 嵌入到信号采样对中。在这个方案中，信号采样 (x_a, x_b) 的二维符号空间是用 5 种颜色“染色”的。网格上的每个点都表示一对信号采样，并且具有与其邻居颜色不同的颜色。其中所述颜色是用 $0 \dots 4$ 来进行编号的，并且每一种颜色都代表了一个消息符号 $d \in \{0, 1, 2, 3, 4\}$ 。在这个实施例中，嵌入器 23 检查 (x_a, x_b) 是否具有将要嵌入的颜色 d 。如果不是的话，则它改变符

号对 (x_a, x_b) ，从而使经过修改的符号对具有颜色 d 。应该了解的是，二维嵌入方案可以扩展到更多的维数。例如在三维网格中，每一个点不但可以移动到同一层的四个相邻位置，而且还可以上下移动。这时可用的则是七种颜色，也就是七个消息符号。

5 现在将对那些在嵌入数据 d 中接纳恢复数据 r 的特定方法的实用实施例进行描述。在这方面应该注意的是，使用给定嵌入器 23 所获取的嵌入比率 R （例如，对使用块长为 3 的汉明码的二进制嵌入而言， $R = 0.3786$ 比特/符号）是最大的。所述嵌入比率则趋近于长的（ N 值很大）宿主信号采样序列。

10 在依照本发明的方法的第一实施例中，宿主信号划分成足够大的分段。每一个分段的恢复数据则是在后续分段中接纳。剩余的容量将被用于嵌入净荷。图 5 显示了这种处理，其中数字 51 表示初始宿主信号 I_m 。该信号分成了若干个分段 $S(n)$ ，每一个分段都包含了给定数目的信号采样（在这里是图像像素）。数字 52 表示的是与信号时间
15 对齐的嵌入数据流 d 。如所述，在这里已经将分段 $S(n)$ 的恢复比特 $r(n)$ 嵌入到分段 $S(n+1)$ 中。分段 $S(n+1)$ 的剩余部分则被用于接纳净荷 w 。应该注意的是，恢复比特的确切数目可能会随着分段而不同。此外，举例来说，较为有利的是通过给各个恢复比特序列提供恰当的结束码而在分段中识别恢复比特 r 与净荷 w 之间的边界。

20 图 5 中显示的图形只是用于说明目的。假设分段的长度是 N 个（在这里 $N = 3000$ ）信号符号。嵌入器 23（参见图 2）基于块长为 3 的汉明码。该嵌入器的嵌入比率为 R （在这里 $R = 2/3$ ）比特/符号，它允许将 $R \times N$ （在这里为 2000）个比特嵌入到各个分段中。对给定概率 p_0 （在这里是 0.9）而言，信源熵是 $H(X|Y)$ （在这里是 $0.8642/3 \approx 0.3$
25 比特/符号）。在给出了 Y 的情况下，用于消除分段 X 的不确定性的恢复比特数目是 $H(X|Y) \times N$ （在这里是 0.3 比特/符号 $\times 3000$ 符号 = 900 比特）。由此将会为净荷留下 $R \times N - H(X|Y) \times N$ （在这里是 $2000 - 900 = 1100$ ）个比特。

30 图 6 显示的是用于接纳恢复比特的替换实施例。在这个实施例中为具有给定初始长度的分段 $S(n)$ 只提供了净荷 w 。而分段 $S(n)$ 的恢复比特 $r(n)$ 则是在后续分段 $S(n+1)$ 中接纳。现在则为后续分段 $S(n+1)$ 指定了一个接纳恢复比特 $r(n)$ 所需要的长度。分段 $S(n+1)$ 需要将新

的数目的恢复比特 $r(n+1)$ 嵌入到另一个分段 $S(n+2)$ 中，等等。并且举例来说，这个处理将会多次重复进行，直到后续分段小于某个给定阈值。然后则为给定初始长度的新分段 $S(\cdot)$ 重复执行整个处理。

将输入符号或矢量 X 变成输出符号或矢量 Y 的数据嵌入器表示的是一个“信道”。迄今描述的数据嵌入器构成了一个对称信道。这一点可以在图 7 中看出，其中图 7 是先前所述的基于块长为 3 的汉明码的数据嵌入器的图形表示。图 8 是非对称信道的图形表示。这个特定实施例是通过在嵌入 $d=00$ 时将输入矢量 (001) 、 (010) 以及 (100) 修改成 $y=(111)$ 而不是 $y=(000)$ 来完成的（优选地，1 不变为 0）。这种嵌入方案的嵌入比率是 $R=0.4335$ 比特/符号（与相应的对称信道比率 $R=0.3786$ 相比较）。由于矢量的 2 个比特而不是 1 个比特有时会发生变化，因此失真要稍大一些。在这种情况下，失真是 $D=0.2701$ （与对称信道的 $D=0.25$ 相比较）。图 3 中的参考数字 322 表示相应的 (R, D) 对。从图中可以看出，非对称信道的性能介于界线 12 与 13 之间。

本发明可以概括如下。水印或数据隐藏方案具有一个不期望的副作用，那就是导致宿主信号失真。本发明公开了一种可逆或无损数据隐藏方案，它允许（在没有附加信令的情况下）完整并隐蔽 (blind) 地重建宿主信号 (X) 。在给出了复合信号的情况下，这可以通过在带有水印信号 (Y) 的被嵌入数据 (d) 中接纳识别宿主信号的恢复数据 (r) 来实现，也就是说，恢复数据识别 (24) 在嵌入 (23) 过程中宿主信号受到何种修改。恢复数据在常规嵌入器 (23) 的一部分嵌入容量中被接纳。而剩余容量则被用于嵌入净荷 (w) 。

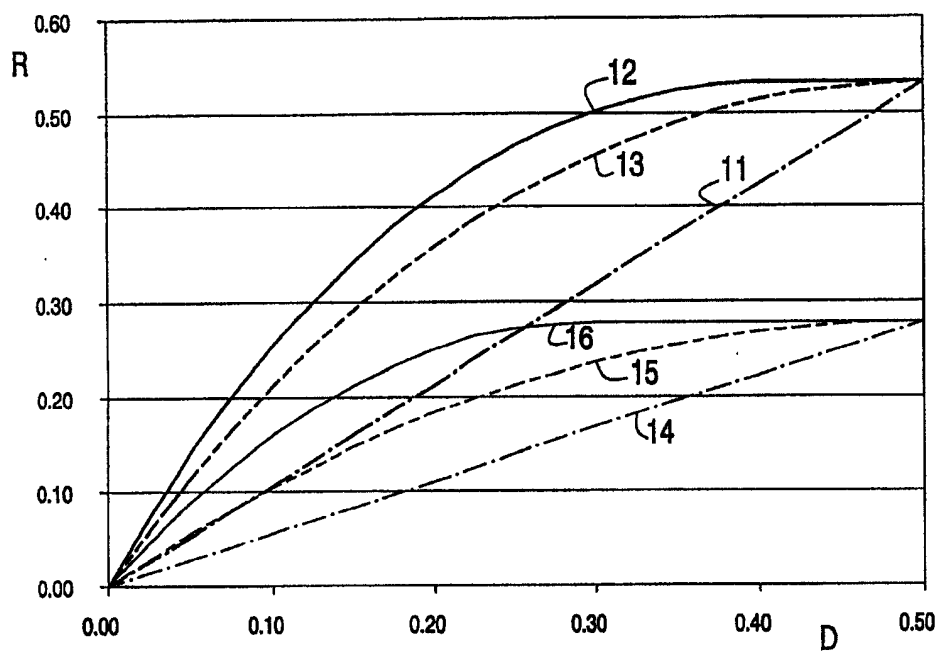


图 1

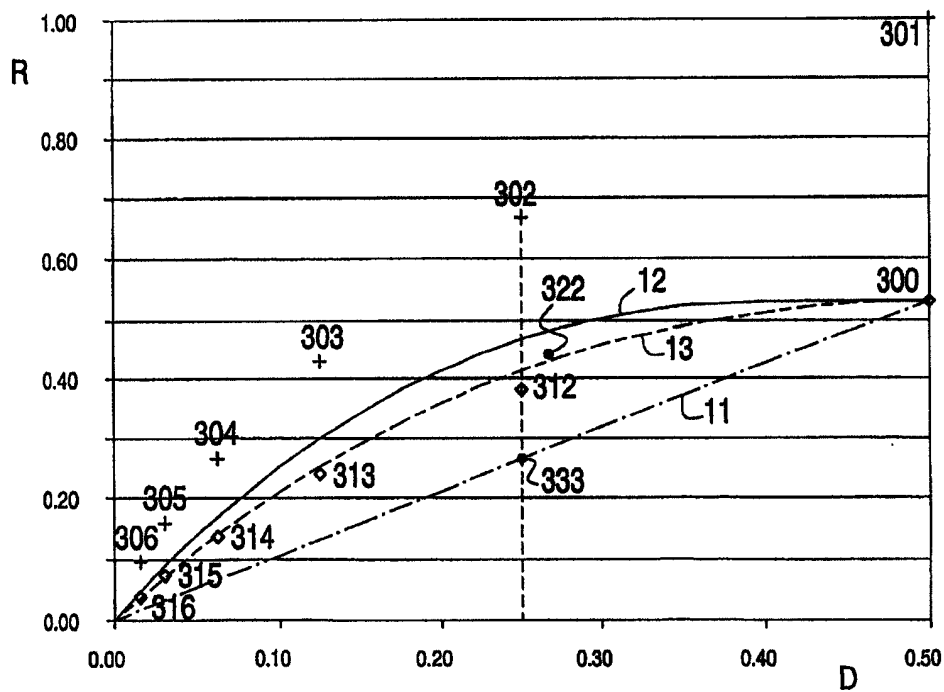


图 3

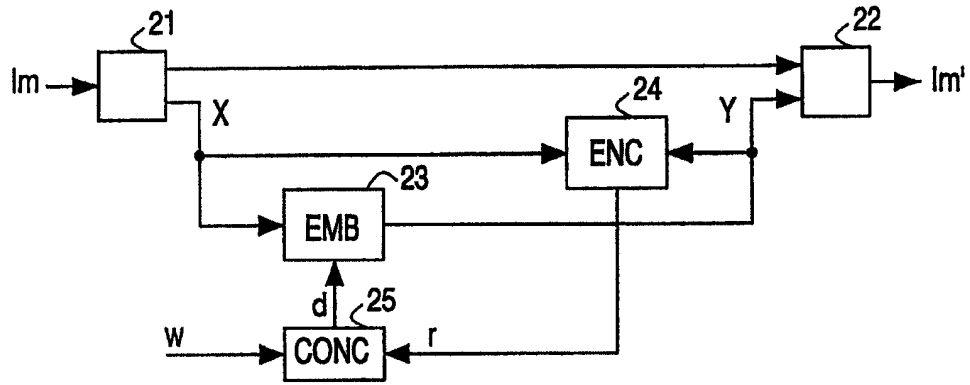


图 2

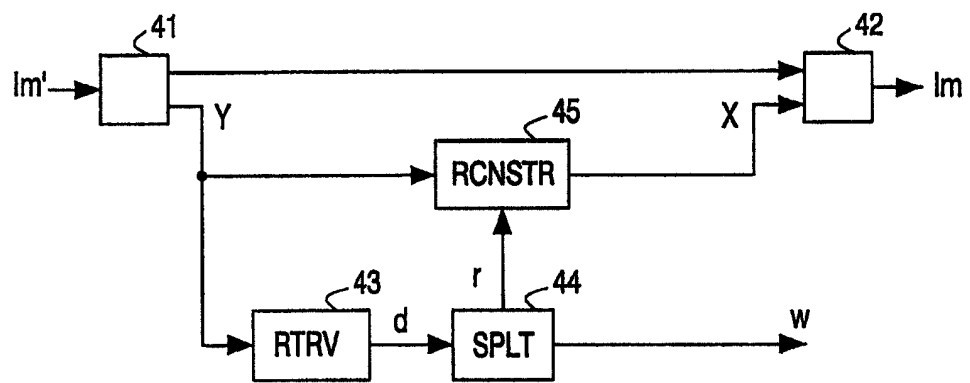


图 4

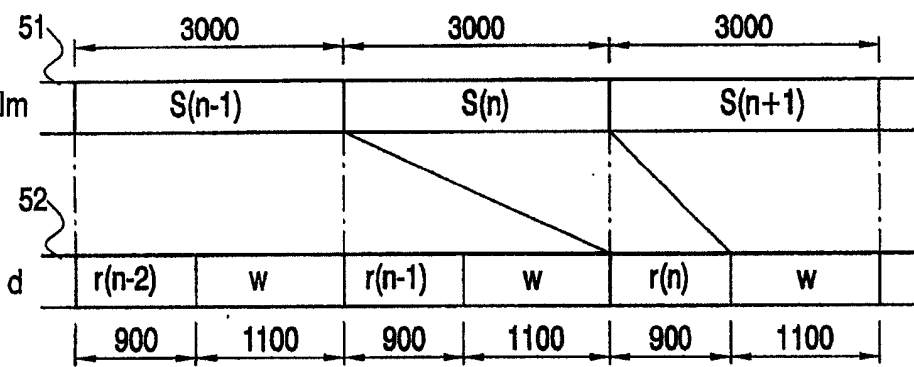


图 5

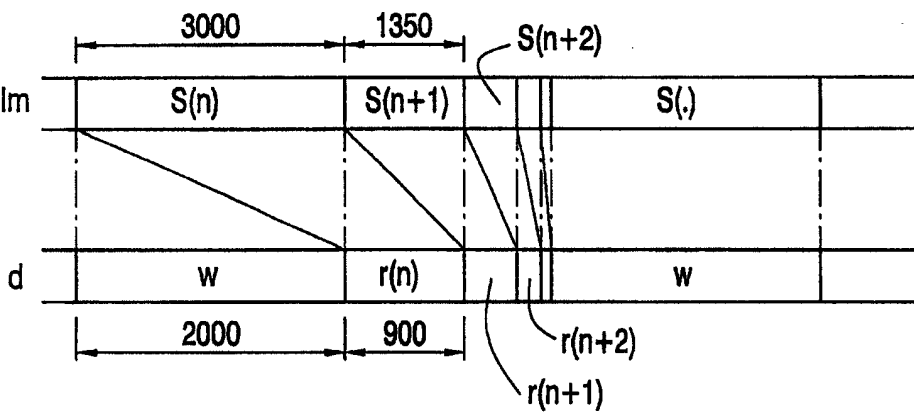


图 6

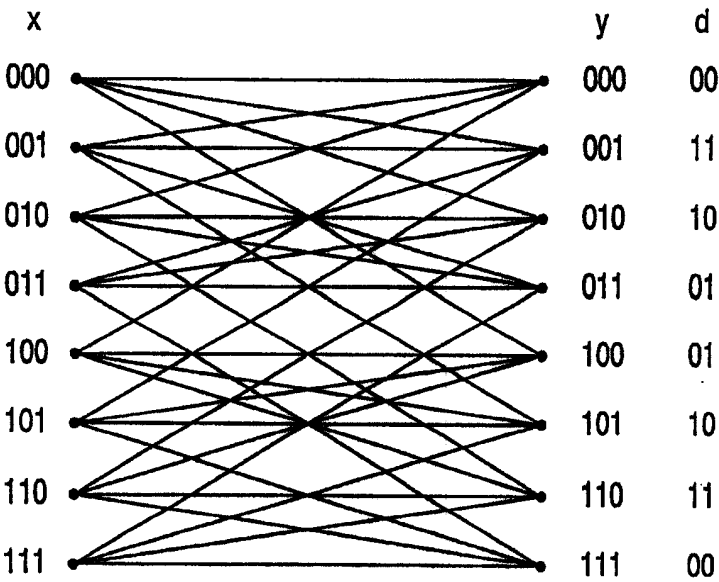


图 7

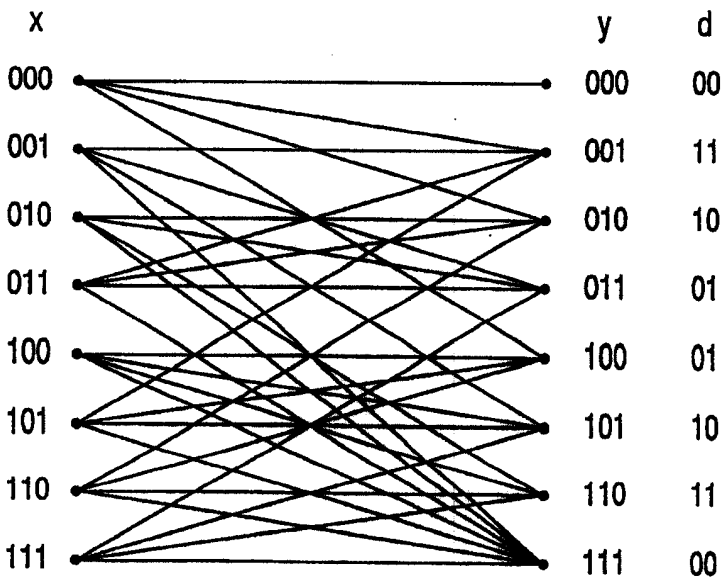


图 8