[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 17/00

# [12]发明专利说明书

[21] ZL 专利号 97125382.X

[45]授权公告日 2002 年 10 月 30 日

[11]授权公告号 CN 1093665C

[22]申请日 1997.12.10 [21]申请号 97125382.X

[30]优先权

[32]1996.12.26 [33]JP [31]348426/96

[32]1997.9.12 [33]JP [31]247998/97

[73]专利权人 国际商业机器公司

地址 美国纽约

[72]发明人 小出昭夫 森本典繁

清水周一 小林诚士

[56]参考文献

PROCEEDINGS OF EUSIPCO TRIESTE ITASLY VOL.3 1996. 9.13 BORS AND PITAS EMBEDDING PARAMETRIC DIGITAL SIGNATURES IN IMAGES

PROCEEDINGS OF THE NOWRIGHT CONFERENCE PROCEEDINGS OF THE IN 1995. 8.21 ZHAO J ET AL EMBEDDING ROBUST LABELS INTO IMAGES

FOR COPYRIGHT PROTECTION

审查员 盖 浩

[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

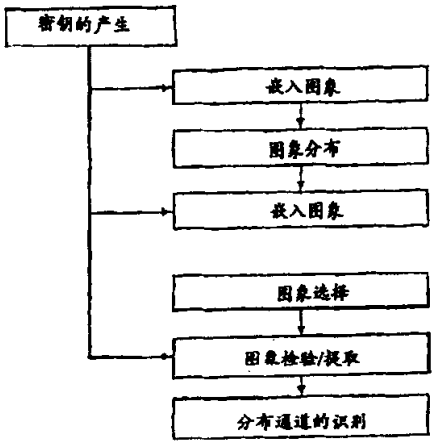
代理人 王以平

权利要求书 1 页 说明书 19 页 附图 1 页

[54]发明名称 利用统计检验的数据隐藏方法和数据提取方法

[57]摘要

本发明的用于将消息嵌入到数据中的数据隐藏方法，包括步骤：通过向一个指定的函数输入一个具有预定值的密钥，得到一个辅助密钥；根据所述的求得的辅助密钥，确定所述消息将被嵌入的隐藏位置，并根据所述辅助密钥选择多个隐藏函数中的一个，使得所述选定的隐藏函数适用于每个所述确定的隐藏位置；以及按照所述选定的、相应于所述隐藏位置的隐藏函数，将消息嵌入到每个所述确定的隐藏位置中。




ISSN1008-4274

# 权 利 要 求 书

1.一种用于将消息嵌入到数据中的数据隐藏方法，包括步骤:

通过向一个指定的函数输入一个具有预定值的密钥，得到一个辅助密钥;

根据所述的求得的辅助密钥，确定所述消息将被嵌入的隐藏位置，并根据所述辅助密钥选择多个隐藏函数中的一个，使得所述选定的隐藏函数用于每个所述确定的隐藏位置；以及

按照所述选定的、相应于所述隐藏位置的隐藏函数，将消息嵌入到每个所述确定的隐藏位置中。

2.一种用于从嵌入了消息的数据中提取消息的数据提取方法，包括步骤:

通过向一个指定的函数输入一个具有预定值的密钥，得到一个辅助密钥;

根据所述求得的辅助密钥，确定所述消息被嵌入的隐藏位置，并根据所述辅助密钥选择多个隐藏函数中的一个，使得所述选定的隐藏函数用于每个所述确定的隐藏位置;

向一个检测基本函数输入所述确定的位置中的信息，按照所述确定的隐藏函数识别该检测基本函数;

将所述检测基本函数的一个输出输入到一个检测函数；以及

根据所述检测函数的一个输出，判断是否嵌入了所述消息。

# 说　　明　　书

## 利用统计检验的数据隐藏方法和数据提取方法

### 技术领域

本发明涉及一种数据隐藏方法和数据提取方法，该方法以一种不可感知的方式将关于所有人或版权的信息嵌入到诸如数字图象、数字视频或数字音频之类的媒体信息中。特别涉及一种数据隐藏方法，该方法在利用统计检验控制信息嵌入操作的同时，以一种不可感知的方式嵌入媒体信息。它还涉及一种数据提取方法，该方法利用统计检验判定是否嵌入了媒体信息，并根据判定结果正确地恢复被嵌入的信息。

### 背景技术

下面所述的利用统计方法的数据隐藏技术已为公众所知。首先，从图象数据中选择两个象素点阵列（此后分别称为“{an}和{bn}”）。每个象素点阵列假设由“n”个象素点构成。然后，通过将一个定值 c 加到一个点阵列{an}中的 n 个象素值 v(an)上，而从另一个点阵列{bn}中的 n 象素值 v(bn)中个减去该定值 c 来执行嵌入操作。

[式 1]

$$v0(an) = v(an) + c$$

$$v0(bn) = v(bn) - c$$

通过计算两个点阵列中 n 个象素的差值并平均该差值，根据其结果判定是否在图象数据中执行了嵌入操作，如下式所示:

[式 2]

$$\frac{1}{N}\sum_{n=1}^{N}(v'(an) - v'(bn))$$

即，当计算在数量上出现了统计特性的象素值之间的差值的平均值时，如果没有加法操作的话，则希望该平均值趋近于 0。另一方面，如果执行了加法操作，则希望该平均值为一个定值 2c。从而，根据在设置了一个临界值的条件下该平均值接近于 0 还是接近于 2c，判定是否执行了嵌入操作。

被嵌入的信息为一位，且两个象素点阵列的位置是保密的，只有执行嵌入操作的人才知道。由于平均值2c不能被执行嵌入操作的人之外的人恢复，除非能识别象素点阵列的位置，所以能提取这个值的事实证明了此人是该数据的所有人。

但是，利用统计方法的现有技术中存在的第一个问题在于，通过执行新的嵌入操作，很容易混淆谁是数据的所有人。即，即使第三者不能操作只有所有人才知道的象素点阵列中的象素值，但是通过选择适当的象素点阵列并在其象素值上执行嵌入操作，就可以重新在另两个适当的象素点阵列中产生该平均值 2c。因此，当执行了这样的操作的第三者根据从他或她识别的点阵列中计算出的平均值，错误地宣称他或她本人即为数据的所有人时，背景技术不能证明谁是真正的所有人。

第二个问题在于没有充分考虑嵌入操作和由它引起的图象质量的下降。由于图象质量的特定特征，即使加上或减去同一个值 c，也会在视觉图象质量的变异上产生重要的差异。因此，最好根据图象质量的特征适应性地改变嵌入操作的数量。即，最好适应性地选择定值 c 和象素点阵列中的象素数量 N。

## 发明内容

从而，本发明的一个目的是提供一种能够准确证明谁是真正的所有人的数据隐藏方法。

本发明的另一个目的是通过在执行嵌入处理的媒体信息中，适应性地确定对特征值，如象素值的操作量来抑制图象质量的下降。

为达到上述目的，本发明的一个特征是利用了一个用于选择一个象素点阵列的密钥。这能防止所有人的错误辨认。本发明的另一个特征是适应性地确定被选定的象素点阵列的大小（N）和将对特征值进行操作的统计量的数值（c）。在数据的恢复中，为了确定是否在一个区域中嵌入了信息，即是否在该区域的特征值上进行了运算操作，而计算可靠性。这样能以一种不可感知的方式，在一个图象中嵌入多位信息（作者、分布 ID 等），并能够从该图象中恢复嵌入的信息，以宣布该图象的所有人或识别分布通道。

具体地，本发明的第一方面是一种用于在数据中嵌入消息的数据隐藏方

法，包括步骤：通过向一个指定的函数输入一个具有预定值的密钥，得到一个辅助密钥；根据得到的辅助密钥，确定在其中将被嵌入消息的隐藏位置，并根据辅助密钥选择多个隐藏函数中的一个，使得选定的隐藏函数适用于每个所确定的隐藏位置；以及按照选定的、相应于隐藏位置的隐藏函数，将消息嵌入到每个所确定的隐藏位置中。

本发明的第二方面是一种用于从嵌入了消息的数据中提取消息的数据提取方法，包括步骤：通过向一个指定的函数输入一个具有预定值的密钥，得到一个辅助密钥；根据得到的辅助密钥，确定其中被嵌入消息的隐藏位置，并根据辅助密钥选择多个隐藏函数中的一个，使得选定的隐藏函数适用于每个所确定的隐藏位置；向一个检测基本函数输入所确定的位置中的信息，按照所确定的隐藏函数识别该检测基本函数；将检测基本函数的一个输出输入到一个检测函数；以及根据该检测函数的一个输出，判断是否嵌入了消息。

因此，本发明能够准确证明谁是真正的所有人，并能通过适应性地确定对特征值，如象素值的操作量来抑制执行了嵌入处理的媒体信息的图象质量的下降。

## 附图说明

图 1 是说明实施例中的图象分布与密钥的产生之间的联系的方框图；以及

图 2 是示出了在被加到一个测试图象上时，一个检测基本函数的特征曲线的结果的图表。

## 具体实施方式

图 1 示出了图象分布与密钥的产生之间的联系。通过首先产生一个密钥并根据该密钥将多位信息嵌入该图象中来对一个图象进行分布（distribute）。如果想加密和分布一个图象，则在结果上将多位信息另外嵌入到解密的图象中。然后，根据该密钥检测一个被分布的图象以观察该图象是否侵犯了版权。如果是，则从被提取的位信息中识别其分布通道。下面，首先描述一个用于检测是否在一个数字内容中执行嵌入处理并恢复

位信息的系统。然后，描述一个用于检测/嵌入多位信息的系统。另外，将详细描述实施例的重要概念、检测基本函数和重写、计算检测函数的特性、嵌入错误的证明以及利用单向函数的嵌入。

（1）检测/恢复系统

该检测/恢复系统包括:

· 一个用于根据一个给定的密钥，确定一个点阵列和一个检测基本函数的机构;

· 一个用于根据点阵列和检测基本函数获得每个点的值，并用于计算它们的和的机构;

· 一个用于确定一个检测函数的机构；以及

· 一个用于通过将该检测函数加到计算出的和上，来确定位信息和它的概率可靠性的机构。

点阵列用于确定一个数字内容被嵌入的位置。如果该数字内容是一维的，则它是一个一维坐标的数组，而如果该数字内容是二维的，则它是一个二维坐标的阵列。点阵列被分成多个组，每个组中嵌入一个 1 位信息。根据嵌入的数字内容恢复相应于组数的位长度信息。点阵列中的每个点用 xna 表示。添加双下标便于表明该点阵列被分成了多个组，其中 a 代表它所属的组。

检测基本函数的特点是利用一个指定点附近的数字数据计算一个值。后面将说明检测基本函数的具体示例。一个通用的检测基本函数可以适用于点阵列中的所有点，而一个区别检测基本函数可以根据用于每个点的密钥来从多个检测基本函数中选择。为了防止一个有预谋的第三者消除嵌入的信息，设计成根据密钥为每个点选择一个检测基本函数，使得每个点具有不同的检测基本函数。下面用 fna 表示点 xna 的检测基本函数。

在点阵列和检测基本函数的基础上为每个点确定一个值，以计算它们在每个组（下标 a）中的和 sa。

[式 3]

$$Sa = \sum_{n=1}^{Na} \int_{na} (\chi_{na})$$

其中，Na 是属于组 a 的点数，且每个组的点数可以彼此不同。没有必

要保存点阵列和检测基本函数。逐一产生密钥并在其和被加到一个累计存储器中之后立即破坏掉这些密钥是重要的。

假设点阵列和检测基本函数是随机选择的，为了提供一种其总和大于和低于一个特定值的概率，定义一个检测函数。其中，点阵列的总和 N 大于 s 的概率用 E+ (N: s)表示，而和低于 s 的概率用 E- (N: s) 表示。此时，从计算出的和 sa 中发现位信息及其概率可靠性如下:

[式 4]

E+ (Na, sa) > E- (Na, sa)

如果满足上式，则确定位 0 被嵌入，且确定 E+ (Na, sa)为其可靠性。相反，如果

[式 5]

E+ (Na, sa) < E- (Na, sa),

则确定位 1 被嵌入，且确定 E- (Na, sa)为其可靠性。如果建立了等式关系，则对位 0 和位 1 来说，概率是相等的。即，不能检测该位信息。如果检测函数满足下式，则上述用于确定位信息及其概率可靠性的机构可能更为简化。

[式 6]

E+ (N, s) + E- (N, s) = 1

此时，如果

[式 7]

E+ (Na, sa) > 0.5,

则则确定位 0 被嵌入，且确定 E+ (Na, sa)为其可靠性。相反，如果

[式 8]

E+ (Na, sa) < 0.5,

则确定位 1 被嵌入，且确定 1-E+ (Na, sa)为其可靠性。此处，对位 0 和位 1 的检测规则是相反的。

根据是否超过了由一个实际的子系统用户为其个人目的而确定的可靠性的事实，判定位信息是否被嵌入到一个数字内容中。由于检测/提取系统需要对数字内容数据进行随机存取，所以该系统可被配置如下以将数字内容数据作为一个流进行处理，而不是将其保存在存储区中:

· 一个用于根据其位置（点）和一个给定的密钥，判定哪个检测基本函数 f 适用于数字内容的流数据和它的值被加到哪个和 sa 中的机构；

· 一个用于临时产生检测基本函数 f 的值，并将其加到和 sa 上进行累加的机构；

· 一个用于累加根据流数据获得检测函数所必需的数据的机构；以及

· 一个用于在处理了所有流数据之后获得一个检测函数，并将该检测函数加到累加和 sa 上以确定位信息及其概率可靠性的机构。

（2）嵌入系统概述

嵌入系统包括:

· 一个用于根据给定的密钥确定一个点阵列和一个检测基本函数的机构；

· 一个用于得到一个检测函数的机构；

· 一个用于根据概率可靠性和检测函数，确定嵌入到位信息中所必需的总和的大小的机构；以及

· 一个用于在保持不可感知性的同时，操作点阵列中的每个点附近的数字数据，使得检测基本函数的总和超过一个预定值的机构。

点阵列和检测基本函数分别用 xna 和 fna 表示。由嵌入系统根据密钥产生的点阵列组数通常应设计成大于检测/提取系统中所用的组数，以使得数字内容的重要统计特性不会由于操作而改变，而属于每个组 a 的点数 Na 应被设计成大于需要以更高的可靠性嵌入位信息的组的点数。检测函数用 E+ (N, s)或 E- (N, s) 表示。当位信息被以可靠性 pa 或更高的可靠性嵌入到组 a 中时，对位 0 执行嵌入操作，以使得检测函数的和 sa 为

[式 9]

$E+ (Na, sa) > pa.$

对位 1 执行嵌入操作，以使得检测函数的和 sa 为

[式 10]

$E-(Na, sa) > pa.$

此处，假设可靠性 pa 大于 0.5. 即可靠性被设计成对位 0 来说，小于检测基本函数的和 sa，其中 $E+ (Na, sa) = pa$，而对位 1 来说，大于检测基本函数的和 sa，其中 $E- (Na, sa) = pa$。其中，在上述位嵌入过程中，用于位

0 和位 1 的嵌入规则可以是相反的。

由于检测函数依赖于数字内容的统计特性，所以嵌入系统中的点阵列的组数被设计成大于检测/提取系统中的组数，多余的组被用来消除在统计特性中的变化。特别是，通过设置用于多余组的检测基本函数的总和的一个目标值，执行嵌入操作，以使得用于整个数字内容的检测基本函数的平均值不会在操作之前被改变。用于消除的多余组数可能是一个或更多。每执行一次一位嵌入，就执行一次消除嵌入，以使得进行了位嵌入的组数等于多余组数。

通过在保持不可感知性的同时，对位于点阵列中的每个点 xna 附近的点值进行运算来执行嵌入操作。假设检测基本函数的总和为 $sa^0$ 时，$\Delta sa=sa-sa^0$ 即为每个组的目标变化范围。如果点阵列中每个点的变化范围是相等的，则 $\Delta sa / Na$ 为检测基本函数值在每个点的目标变化范围。

为了在保持不可感知性的同时提供干扰阻力（tampering resistance），通过对嵌入明显的区域利用一个较窄的变化范围，对嵌入不明显的区域利用一个较宽的变化范围取代相等的变化范围，计算点阵列中每个点 xna 附近的点值来执行嵌入操作。为了嵌入到数字内容中，计算对于一个点阵列中每个点的不可感知性(unperceptivity)的指数(index)，并确定用于检测基本函数的一个目标变化范围以计算该点附近的点值。

不可感知性指数是一个根据位于一给定点 x 附近的点上的数字内容值计算出的值，包括下述类型:

- 比例指数: 一个用于在每个点 x 的变化范围与指数 g(x)成比例时，以近似数值提供可感知性的指数
- 识别临界指数: 一个用于在每个点 x 的变化范围小于指数 g(x)时，以近似数值提供可感知性的指数
- 混合指数: 一个组合了上述内容的指数

对于比例指数来说，通过下式确定一个比例常数 r，且 rg(xna)为在每个点 xna 的一个目标变化范围。

[式 11]

$$r = \Delta Sa / \sum_{n=1}^{Na} g(X_{na})$$

对于识别临界指数来说，如果

[式 12]

$$|\Delta Sa| \le \sum_{n=1}^{Na} g(X_{na}),$$

则沿着Δsa 的符号方向，利用一个变化范围（xna）对每个点 xna 连续进行运算，直到大于|Δsa|为止。然后，在被超出的点中止该变化运算，或对所有的点 xna 执行下述运算。

[式 13]

$$g(X_{na})\Delta S_a / \sum_{n=1}^{Na} g(X_{na})$$

此外，如果

[式 14]

$$|\Delta Sa| \ge \sum_{n=1}^{Na} g(X_{na}),$$

则按照Δsa 的符号，对每个点 xna 执行变化范围为

[式 15]

$$g(X_{na}) + (|\Delta S_a| - \sum_{n=1}^{Na} g(X_{na}) / N_a$$

的运算。对于混合指数，通过组合上述内容执行嵌入操作。

（3）检测基本函数和重写

密钥规定了一个点阵列和一个检测基本函数。这里给出关于检测基本函数、相关的嵌入操作以及重写技术的说明。检测基本函数是一个用于利用数字数据计算在一规定点附近的点上的值的机构。检测基本函数用 fα 表示，其中α是一个用于区别多个检测基本函数的下标。

首先，给出关于系数和为 0 的线性滤波器的说明。尽管在原理上，检测基本函数可以采用任何形式，但由于一个数字内容通常被提供给一个整数值阵列，所以就希望它的输入端接收一个整数值，并输出另一个整数值，并且为了满足不可感知性，检测基本函数的值被集中在它们的平均值附近，在对于改变检测基本函数值所必需的附近点，这些平均值的变化范围较小。尤其是，对于后面的情况，在假设σ是用于整个数字内容的检测基本函数的标准差时，希望该检测基本函数是这样一个函数：在对于通过σ增加/减

小该检测基本函数所必需的点周围的值的变化范围的平均值应小于用于整个数字内容的每个点的值的标准差。

一个具有这样的特点的检测基本函数包括一个用下述等式表示的线性滤波器:

[式 16]

$$f_a(x) = \sum_y F_a(y)v(x+y)$$

其中 v(x+y)是数字内容在一个从点 x 移动了 y 的点上的值，且滤波器系数 Fα(y)是一个用下式表示的整数

[式 17]

$$0 = \sum_y F_a(y)$$

x 和 y 是用于数字图象和数字视频信息的二维向量。系数和为 0 的原因是为了使嵌入的信息不依赖于数字数据在该点的绝对值，而是依赖于数字数据在该点周围的状态或一个相对值。例如，认为下述的为用于数字图象的最简单的线性滤波器。给定的检测基本函数系数 fS0 为

[式 18]

$(F_{S0}(0,0);\quad F_{S0}(1,0)) = (1,-1)$,

且给定的检测基本函数系数 fS1 为

[式 19]

$(F_{S1}(0,0);\quad F_{S1}(0,1)) = (1,-1)$.

图 2 是示出了将检测基本函数的特性加到测试图象上的图表。每个检测基本函数的标准差被认为是小于象素值的标准差。因此，就希望通过使用 fS0 和 fS1 采用一个较窄的变化范围作为检测基本函数，取代原有的利用象素值本身作为检测基本函数。

为了符合 JPEG 和 MPEG 标准，宽度和高度与用于 DCT 转换的 8*8 块相匹配的线性滤波器被用作检测基本函数。即使用 4*4、4*8、8*4、8*8、16*8、8*16 或 16*16 线性滤波器。例如，下面使用 8*8 滤波器 fJ0,fJ1,fJ2,fJ3:

[式 20]

$$F_{J0}(j,k) = \begin{pmatrix} 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & -1 & 0 & 0 & 1 & 1 \\ -1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 \end{pmatrix}$$

[式 21]

$$F_{J1}(j,k) = \begin{pmatrix} 0 & 0 & -1 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & -1 & 0 & 0 & 1 & 1 \\ -1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 \\ 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 \end{pmatrix}$$

[式 22]

$$F_{J2}(j,k) = \begin{pmatrix} 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 \\ -1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & -1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

[式 23]

$$F_{J3}(j,k)=\begin{pmatrix} 0 & 0 & -1 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & -1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 \\ -1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

通过利用不可理解性指数确定用于点阵列中每个点的检测基本函数值的目标变化值$\Delta f\alpha(X)=f\alpha(x)'-f\alpha(x)$。这里在给定了一个线性滤波器的情况下，详细描述为达到这样的目标值而在嵌入点阵列中的点周围的每个点对数字数据的操作。下面，用 w(x,y)表示用于嵌入点阵列中的一个点 x 周围的每个点(x+y)的变化值。即，在一个点(x+y)的数字数据值 v(x+y)变成了 v(x+y)+w(x,y)。

为用于检测基本函数 fff 的线性滤波器系数 Fα（y）定义了一个系数 Gff(y):

[式 24]

$$\sum_{y} F_{\alpha}(y)G_{\alpha}(y)=D_{\alpha}\rangle 0$$

然后根据

[式 25]

$$d(x)=\Delta F_{\alpha}(x)/D_{\alpha}$$

得到 d(x)。根据

[式 26]

$$w(x,y)=d(x)G_{\alpha}(y)$$

得到变化值。

一个选定的最简单的系数 Gα（y）为 Gα（y）=Fα（y）。如果 d(x)的绝对值大于 1，则通过稍微改变和求 d(x)Gα（y）的平均值以使该值逐渐变化而增强其不可感知性。例如，如果对于 GJ1(j,k)=FJ1(j,k), d(x)=4，则利用[式

28]代替[式 27]来求其平均值。

[式 27]

$$d(x)G_{J1}(j,k)=\begin{pmatrix} 0 & 0 & -4 & -4 & 0 & 0 & 4 & 4 \\ 0 & 0 & -4 & -4 & 0 & 0 & 4 & 4 \\ -4 & -4 & 0 & 0 & 4 & 4 & 0 & 0 \\ -4 & -4 & 0 & 0 & 4 & 4 & 0 & 0 \\ 0 & 0 & 4 & 4 & 0 & 0 & -4 & -4 \\ 0 & 0 & 4 & 4 & 0 & 0 & -4 & -4 \\ 4 & 4 & 0 & 0 & -4 & -4 & 0 & 0 \\ 4 & 4 & 0 & 0 & -4 & -4 & 0 & 0 \end{pmatrix}$$

[式 28]

$$w(x,y)=\begin{pmatrix} 0 & 0 & -3 & -4 & 0 & 0 & 4 & 3 \\ 0 & 0 & -4 & -4 & 0 & 1 & 3 & 4 \\ -3 & -4 & 0 & 0 & 4 & 3 & 1 & 0 \\ -4 & -4 & 0 & 0 & 4 & 4 & 0 & 0 \\ 0 & 0 & 4 & 4 & 0 & 0 & -4 & -4 \\ 0 & 1 & 3 & 4 & 0 & 0 & -4 & -3 \\ 4 & 3 & 1 & 0 & -4 & -4 & 0 & 0 \\ 3 & 4 & 0 & 0 & -4 & -3 & 0 & 0 \end{pmatrix}$$

下述方法被用于通过重写嵌入多个消息:

· 正交嵌入; 以及

· 分层嵌入。

其中，正交嵌入通过利用相互之间高度独立的检测基本函数进行位重写。在线性滤波器的情况下，通过一组正交系数执行:

[式 29]

$$\sum_{y} F_{\alpha}(y)G_{\beta}(y)=D_{\alpha}\neq 0, \quad \text{如果}\ \alpha=\beta$$

$$=0, \quad \text{其它}$$

如果α和β不相等，则由系数Fα（y）给定的检测基本函数fα没有检测用$w(x,y)=d(x)G\beta(y)$执行的嵌入过程。

此外，分层嵌入意味着这样一种情况：在被应用到不同大小的区域上的检测基本函数之间，其中一个检测函数被应用到的较小区域被扩大到另一个函数被加到的较大区域时，它们之间具有高度独立性。例如，一个 2*1 大小的线性滤波器能被扩大到后面的 2*2 大小的线性滤波器：

[式 30]

$$F_{S0.0}(i,j)=\begin{pmatrix}1 & -1\\ 0 & 0\end{pmatrix}$$

$$F_{S0.1}(i,j)=\begin{pmatrix}0 & 0\\ 1 & -1\end{pmatrix}$$

[式 31]

$$F_{SS}(i,j)=\begin{pmatrix}1 & 1\\ -1 & -1\end{pmatrix}$$

按照上述的正交嵌入，它们与后面的线性滤波器是正交的。因此，fSS 和 fS0 能被重写。

这里，说明检测函数的计算。当确定了一个数字内容时，对整个内容中的检测基本函数 fα 值为 f 的频率进行记数以产生一个频率分布（直方图）h(f)。它用于计算检测基本函数 fα 值为 f 时的概率 p(f):

[式 32]

$$p(f)=h(f)/\sum_{f}h(f)$$

即使直方图是通过在随机选定的点，而不是在内容的所有点计算检测基本函数值而产生的，但是只要选定的点数足够大，在实际应用中就不会出现问题。按照下列等式，根据概率 p(f)的结果就可以求出在 N 个检测基本函数的和为 s 时的概率 PN(s):

[式 33]

$$p_N(s)=\sum_{f_1}\sum_{f_2}\cdots\sum_{f_{N-1}}p(f_1)p(f_2)\cdots p(f_{N-1})p(s-f_1-f_2\cdots-f_{N-1})$$

据此可求出检测函数如下：

[式 34]

$$E_+(N,s)=\sum_{s'>s}P_N(s')$$

$$E_-(N,s)=\sum_{s'<s}P_N(s')$$

检测函数的近似计算

下面，说明一种用于有效求出检测函数的方法，该方法根据一个检测基本函数的统计矩(statistical moment)或<fn>次方的平均值近似求出一个检测函数。其中，假设通过下式计算统计矩:

[式 35]

$$\langle f^n\rangle=\sum_x\sum_\alpha f_\alpha(x)^n/\sum_x\sum_\alpha 1$$

如下所述，由于没有必要根据直方图 h(f)计算概率 PN(s)，所以存储量和计算量能被保持在一个低水平。利用$<f^n>^c=<(f-<fi>)^n>$来简化公式。即，

[式 36]

$$\begin{aligned}\langle f\rangle_c &= 0\\ \langle f^2\rangle_c &= \langle f^2\rangle-\langle f\rangle^2\\ \langle f^3\rangle_c &= \langle f^4\rangle-3\langle f^2\rangle\langle f\rangle+2\langle f\rangle^3\\ \langle f^4\rangle_c &= \langle f^4\rangle-4\langle f^3\rangle\langle f\rangle+6\langle f^2\rangle\langle f\rangle^2-3\langle f\rangle^4\end{aligned}$$

其中，对于足够大的 N，可将其近似为

[式 37]

$$P_N(s)^{(0)}=\frac{1}{\sqrt{2\pi N\langle f^2\rangle_c}}\exp\left(-\frac{(s-N\langle f\rangle)^2}{2N\langle f^2\rangle_c}\right)$$

从而，通过下式得到检测函数:

[式 38]

$$E_+(N,s)^{(0)} = \frac{1}{\sqrt{2\pi N\langle f^2\rangle_c}}\int_s^{\infty} ds' \exp(-\frac{(s'-N\langle f\rangle)^2}{2N\langle f^2\rangle_c})$$

$$E_-(N,s)^{(0)} = \frac{1}{\sqrt{2\pi N\langle f^2\rangle_c}}\int_{\infty}^{s} ds' \exp(-\frac{(s'-N\langle f\rangle)^2}{2N\langle f^2\rangle_c})$$

通过下式计算近似检测函数中的修正项 E+(N,s)$^{(n)}$ 和 E-(N,s)$^{(n)}$:

[式 39]

$$E_+(N,s)^{(n)} = -Q_n(N,s)P_N(s)^{(0)}$$

$$E_-(N,s)^{(n)} = Q_n(N,s)P_N(s)^{(0)}$$

为简化起见，如果

[式 40]

v = s - N<f>

且

[式 41]

$$w = \frac{(s-N\langle f\rangle)^2}{N\langle f^2\rangle_c},$$

则通过下式求出 Qn(N,s):

[式 42]

$$Q_1(N,s) = \frac{\langle f\rangle_c^3}{3!\langle f^2\rangle_c}(w-1)$$

[式 43]

$$Q_2(N,s) = \frac{u}{N}\left[\frac{(\langle f^4\rangle_c - 3\langle f^2\rangle_c^2)}{4!\langle f^2\rangle_c^2}(w-3) + \frac{\langle f^3\rangle_c^2}{2!3!3!\langle f^2\rangle_c^3}(w^2-10w+15)\right]$$

当通过 E+$^{(0)}$+E+$^{(1)}$，E+$^{(0)}$+E+$^{(1)}$+E+$^{(2)}$，E-$^{(0)}$+E-$^{(1)}$和 E-$^{(0)}$+E-$^{(1)}$+E-$^{(2)}$估计修正项时，如果提供了一个负值，则用 0 代替该值。

检测函数的精确计算

为了求出准确的概率 PN(s)，利用了一个递归公式:

[式 44]

$$P_{N+N'}(s)=\sum_{s'}P_N(s')P_{N'}(s-s')$$

例如，对于 N=2M，足以重复上述递归公式 M 次。其缺点在于存储器的大小。它被用于试验阶段或不允许近似的情况下。

嵌入的错误证明

当确定了一个数字内容时，对整个内容中的检测基本函数 fα 值为 f 的频率进行记数，产生一个频率分布（直方图）h(f)以求出后面的点阵列，并计算该频率分布 h(f)以产生一个与点阵列相对应的频率分布 ha(f):

- 使点阵列上的检测基本函数的和超过一个目标值;
- 使点阵列上的检测基本函数的和接近一个目标值；以及
- 使两个点阵列上的检测基本函数的和接近一个目标值。

如果没有带有一个单向函数的密钥系统，则可能产生一个错误证明，证明在一个数字内容中，已经对没有被嵌入到系统中的位信息执行了嵌入操作。下面，本发明将给予详细说明。

假设对于整个数字内容的检测基本函数值的频率分布为 h(f)，而对于点阵列组 a 的检测基本函数值的频率分布为 ha(f)时，

[式 45]

$$0\le h_a(f)\le h(f)$$

满足于所有的 f，通过下式给定点阵列组 a 中检测基本函数值的和:

[式 46]

$$s_a=\sum_f fh_a(f)$$

并通过下式给定点阵列组 a 中的点数:

[式 47]

$$N_a=\sum_f h_a(f)$$

此时，

[式 48]

$s_a/N_a=-s_b/N_b=c$

实际上是为位提取条件公式（式 1）设定的，该公式用于说明利用下式求出 ha(f)和 hb(f)的背景技术:

[式 49]

$N_a = N_b = N$ 且 $h_a(f)+h_b(f) \le h(f)$

此外，在注意到如果用于检测函数的 Na 足够大而使得依据本发明的具有检测函数的位提取条件近似于正常分布时，为位 1 设立如下式子:

[式 50]

$s_a / \sqrt{N_a} \ge c$

另一方面，为位 0 建立下式:

[式 51]

$s_a / \sqrt{N_a} \ge -c$

[式 52]

$\sum_a = h_a(f) \le h(f)$

从而，得到 ha(f)。

一个用于生成错误嵌入证明的系统通过第一次扫描从数字内容中产生一个频率分布 h，然后产生一个满足于上述 h(f)的频率分布 ha，并通过第二次扫描从数字内容中选择点 f=f(x)的 ha(f)，从而它们的集合成为了一个用于错误证明的点阵列。

通过对所有 a 重复执行在后述的预定规则下计算 f 的基本操作，直到和 Σ fha(f)达到一个值 Na 为止，从整个频率分布 h 中产生频率分布 ha，所述的预定规则是以 ha(f)=0 为初值，如果 h(f)是正的，就使 h(f)减 1，而 ha(f)加 1。对 a 的循环是内部的。

为了产生用于具有检测函数的位提取的情况下的频率分布 ha，按照嵌入位 1 所用的频率分布 f 的递减顺序，嵌入位 0 所用的频率分布 f 的递增顺序执行基本操作。

用于说明背景技术的位提取条件公式（式 1）按如下设定运算。其中以 Delta0(+) = 0,elta0(-) = 0 为初值，求出 fna 接近于

[式 53]

$f_{na} = c + \Delta_n(+)$，

且在 ha 的基础上执行基本操作以求出

[式 54]

$\Delta_{n+1}(+) = c + \Delta_n(+) - f_{na}$

然后，求出 fnb 接近于

[式 55]

$f_{nb} = -c + \Delta_n(-)$,

且在 hb 的基础上执行基本操作以求出

[式 56]

$\Delta_{n+1}(-) = -c + \Delta_n(-) - f_{nb}$

通过ΔN（+）=N 和ΔN（-）=N 确定最后的错误。

利用双向函数的嵌入

如上所述，通过选择一个似乎被嵌入的点阵列能够从一个没有嵌入操作的数字内容中提取出预定的位信息。因此，它不能只根据知道用于从数字内容中提取预定位信息的点阵列这个事实，就判定该人是否就是数字内容的所有人。而作为这个问题的解决方法，是设想利用一个公正的第三方组织预先登记如下事实：利用一个特定的点阵列将位信息嵌入到一个特定的数字内容中。这种解决方法具有如下缺点：

· 需要对每次嵌入执行登记过程，从而需要用于登记的成本。

· 由于通过第三方组织登记被嵌入的点阵列，所以增加了嵌入的点阵列被暴露的危险性和嵌入信息被消除的危险性。

因此，本发明的用于嵌入位信息的方法和系统可以作为所有人错误认证问题的解决方法，本发明所公开的方法根据利用一个单向函数的整数值（此后称为“密钥”），确定一个嵌入位置，其中“密钥”是秘密的且只有所有人本人知道。只要采用了本方法，即使能够从一个特定的数字内容中得到一个能够错误认证所有人的点阵列，但由于单向函数的特性而使得来自点阵列的“密钥”不能被计算出来，所以根据一个已知的私人密钥也不可能进行所有人的错误认证。

根据利用了单向函数的密钥，产生用于确定进行嵌入的位置的点阵列的方法可以通过如下步骤实现：利用该单向函数产生一个“辅助密钥”，并根据该“辅助密钥”产生点阵列。由于密钥和“辅助密钥”都是非负的整数值，所以可以使用一个普通的单向函数。也可以通过从利用单向函数的密钥中产生一个“辅助密钥”来实现根据利用了单向函数的密钥，产生用于确定进行嵌入的位置的点阵列的方法。

下面将详细描述用于根据一个“辅助密钥”产生一点阵列的方法。一个

数字内容被分成N个区域，每个区域具有一个号码，这里用n表示该号码。每个区域n被分成M个子区，检测基本函数被加于该子区之上，且每个子区有一个号码。此外，假设选择了L个检测基本函数。此时，辅助密钥从每个子区n中选择一个子区的号码mn，和被加到这个子区上的检测基本函数fln。即，假设辅助密钥（非负整数值）k生成一个用以确定子区和检测基本函数的整数:

[式57]

$$j=\sum_{n=0}^{N-1}L^{n}M^{n}(m_{n}+Ml_{n})$$

辅助密钥的可能范围（k的位长）通常短于一个整数j的可能范围（j的位长）。因此，如果假设k0为辅助密钥，则通过从ki开始连续计算ki+1，确定子区和检测基本函数，然后计算

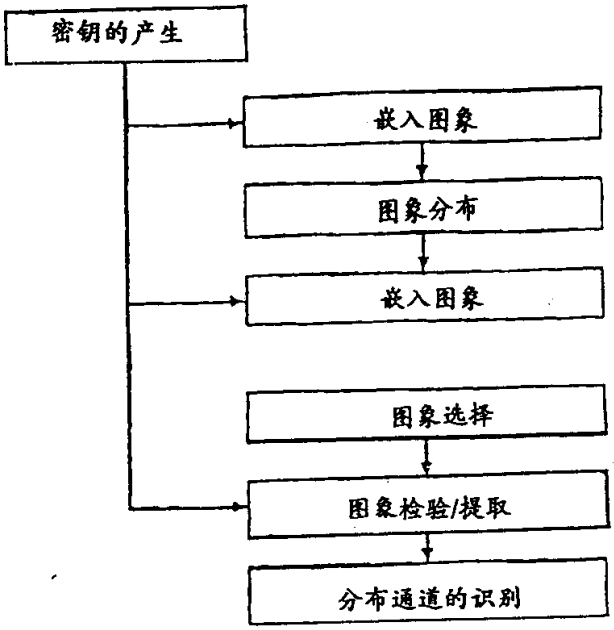
[式58]

$$j=\sum_{i=0}K^{i}k_{i}$$

其中，K是非负整数值ki的上限。用于从ki开始计算ki+1的机构可以是一个单向函数或一种普通算术操作。它最好是一个一对一函数。通过将子区的数目M和检测基本函数的数目L作为2的幂数，从整数j开始逐位计算Mn和ln。

# 说　明　书　附　图

## 图 1




## 图 2

| 样本图象 | 象素值的标准差 | $f_{s0}$ 的标准差 | $f_{s1}$ 的标准差 |
|---|---|---|---|
| 200000 红 | 68.3396 | 9.4510 | 9.0329 |
| 200000 绿 | 59.6419 | 9.5007 | 9.0248 |
| 200000 蓝 | 60.9283 | 9.7633 | 9.2070 |
| 200001 红 | 58.7429 | 16.2642 | 17.1555 |
| 200001 绿 | 54.6655 | 16.3756 | 17.1682 |
| 200001 蓝 | 53.0666 | 15.9594 | 16.8779 |
| 200002 红 | 52.5882 | 4.4696 | 8.5511 |
| 200002 绿 | 45.1880 | 4.1811 | 8.1316 |
| 200002 蓝 | 37.9568 | 4.0256 | 7.8376 |
| 200011 红 | 16.0885 | 3.2931 | 3.4074 |
| 200011 绿 | 18.8486 | 3.3313 | 3.4857 |
| 200011 蓝 | 21.4928 | 3.4299 | 3.6075 |