

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 7/58 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200780005452.7

[43] 公开日 2009年3月11日

[11] 公开号 CN 101384993A

[22] 申请日 2007.2.12

[21] 申请号 200780005452.7

[30] 优先权

[32] 2006.2.15 [33] EP [31] 06003029.3

[86] 国际申请 PCT/EP2007/001187 2007.2.12

[87] 国际公布 WO2007/093347 英 2007.8.23

[85] 进入国家阶段日期 2008.8.14

[71] 申请人 杰克里普托有限公司

地址 英国霍恩彻什

[72] 发明人 杰伊·布萨瑞

[74] 专利代理机构 北京东方亿思知识产权代理有限公司

代理人 李晓冬 南 霆

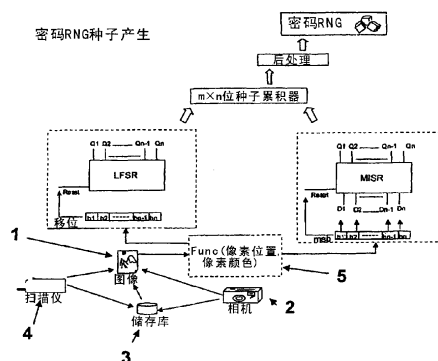
权利要求书4页 说明书7页 附图3页

[54] 发明名称

产生密码学随机数发生器种子的方法和设备

[57] 摘要

本发明涉及产生密码学随机数发生器种子的方法和设备。为了产生密码学随机数发生器的种子，图像被使用。选择所输入图像的像素，每个像素提供有相关联的位置和颜色信息。与所选择的像素相关联的位置和颜色信息用于计算预定数量的位，然后这些预定数量的位用于产生随机数发生器的种子。使用者可通过相机、扫描仪或储存库输入图像。



1. 一种产生密码学随机数发生器种子的方法，其中，所述方法包括步骤：

输入图像（1）的至少一部分；以及

选择所述图像（1）的像素，每个像素提供有相关联的位置和颜色信息；以及

利用与所选择的像素相关联的所述位置和颜色信息来计算预定数量的位；

输出计算得到的数量的位，用于产生所述密码学随机数发生器的种子。

2. 一种产生密码学随机数的方法，其中，所述方法包括步骤：

输入图像（1）的至少一部分；以及

选择所述图像（1）的像素，每个像素提供有相关联的位置和颜色信息；以及

利用与所选择的像素相关联的所述位置和颜色信息来计算预定数量的位；

输出计算得到的数量的位作为密码学随机数。

3. 如权利要求 1 或 2 所述的方法，其中，所述输入图像（1）的至少一部分的步骤由已经选择所述图像（1）的使用者执行。

4. 如权利要求 1 至 3 中任一项所述的方法，其中，所述输入的步骤包括输入要被用于随后步骤中的多个图像（1）。

5. 如权利要求 1 至 4 中任一项所述的方法，其中，所述输入的步骤利用相机（2）和/或扫描仪（4）和/或储存库（3），其中，至少一幅图像（1）被存储在所述储存库（3）中。

6. 如权利要求 1 至 5 中任一项所述的方法，其中，所述输入图像（1）的步骤还包括：

基于所输入图像的尺寸、颜色密度和/或颜色变化，计算反映所输入图像适合性的品质因素；以及

将计算得到的品质因素与预定的阈值进行比较；以及
如果比较结果是所述图像（1）不合适，则拒绝，或者输出警告；以及

如果比较结果是所述图像（1）合适，则接受所述图像（1）。

7. 如权利要求 6 所述的方法，其中，对于已使用过的图像，通过拒绝和/或输出警告来防止图像被再选择。

8. 如权利要求 1 至 7 中任一项所述的方法，其中，选择所述图像（1）的像素的步骤包括：

随机选择所述图像（1）的像素的子组，特别是基于当前选择的像素的颜色和/或位置来选择下一个像素。

9. 如权利要求 1 至 8 中任一项所述的方法，其中，所述计算预定数量的位的步骤使用线性反馈移位寄存器或多输入移位寄存器。

10. 如权利要求 1 至 9 中任一项所述的方法，其中，选择所述图像（1）的像素的步骤还包括利用多个寄存器元件调整像素尺寸。

11. 如权利要求 1 至 10 中任一项所述的方法，其中，所述计算预定数量的位的步骤包括对位进行缓冲，使得预定数量的输出位能够被改变。

12. 一种随机数种子，通过权利要求 1 至 10 中任一项所述的方法获得。

13. 一种设备，用于产生密码学随机数发生器的种子，包括：

输入装置，适于输入图像（1）的至少一部分；以及

选择装置（5），适于选择所述图像（1）的像素，每个像素提供有相关联的位置和颜色信息；以及

计算装置，适于利用与所选择的像素相关联的所述位置和颜色信息来计算预定数量的位；

输出装置，适于输出计算得到的数量的位，用于产生所述密码学随机数发生器的种子。

14. 一种设备，用于产生密码学随机数，包括：

输入装置，适于输入图像（1）的至少一部分；以及

选择装置（5），适于选择所述图像（1）的像素，每个像素提供有相

关联的位置和颜色信息；以及

计算装置，适于利用与所选择的像素相关联的所述位置和颜色信息来计算预定数量的位；

输出装置，适于将计算得到的数量的位输出作为所述密码学随机数。

15. 如权利要求 13 或 14 所述的设备，其中，所述输入装置适于使得使用者能够选择所述图像（1）。

16. 如权利要求 13 至 15 中任一项所述的设备，所述输入装置适于使得要被用于随后步骤中的多个图像（1）能够被输入。

17. 如权利要求 13 至 16 中任一项所述的设备，其中，所述输入装置是相机（2）和/或扫描仪（4）和/或储存库（3），其中，至少一幅图像（1）被存储在所述储存库（3）中。

18. 如权利要求 13 至 17 中任一项所述的设备，其中，所述输入装置还包括：

计算装置，适于基于所输入图像的尺寸、颜色密度和/或颜色变化，计算反映所输入图像适合性的品质因素；以及

比较装置，适于将计算得到的品质因素与预定的阈值进行比较；以及

信令装置，适于如果比较结果是所述图像（1）不合适，则拒绝，或者输出警告；并且其中，如果比较结果是所述图像（1）合适，则所述设备适于接受所述图像（1）。

19. 如权利要求 18 所述的设备，其中，所述比较装置和信令装置还适于防止在随后的时间图像被再选择。

20. 如权利要求 13 至 19 中任一项所述的设备，其中，所述选择装置（5）包括：

随机选择装置，适于随机选择所述图像（1）的像素的子组，特别是基于当前选择的像素的颜色和/或位置来选择下一个像素。

21. 如权利要求 13 至 20 中任一项所述的设备，其中，所述计算装置包括线性反馈移位寄存器或多输入移位寄存器。

22. 如权利要求 13 至 21 中任一项所述的设备，其中，所述选择装置还适于利用多个寄存器元件调整像素尺寸。

23. 如权利要求 13 至 22 中任一项所述的设备，其中，所述计算装置包括存储装置，所述存储装置适于对位进行缓冲，使得预定数量的输出位能够被改变。

产生密码学随机数发生器种子的方法和设备

技术领域

本发明一般地涉及密码学领域，具体而言，涉及产生密码学随机数发生器种子的方法和设备。

背景技术

随机数发生器（RNG）可用于很多种电子应用，例如博彩机、游戏机、科学和金融建模仿真、程序和算法测试、解方程以及计算机安全。密码学随机数发生器将更加适用于计算机安全应用，例如密码、数字签名（包括不可否认性）、私人通信协议以及消息完整性。密码学随机数发生器是加强和保护电子通信的机密性、完整性和认证的基本组成部分。密码学随机数发生器也可以用于产生对称或不对称密钥。

通常，密码学随机数发生器通过时钟装置或者来自内建硬件式磁盘驱动的其它信息熵源（entropy source）、鼠标移动、键盘输入计时、运行过程、麦克风线路噪声产生种子，它们甚至都可以用于不同的组合置换（参照 IETF 的 RFC 1750）。由于特殊机制，例如中断和事件处理，这些种子源可能效率下降，并且由于这些系统的固有周期（即重复前就输出的值的数量），这些种子源受到限制。因为计算机系统的主要部件特别希望是确定性的，所以不可能用它们来产生真正的随机数。

产生的随机数通常具有给定数值范围的特定概率、密度和分布。适于密码学应用的理想随机数发生器提供的数值应当在无限的范围内均匀分布，并且是非确定性的。

作为在视频装置中产生伪随机数的另一种方法，已知一种方法包括用于从密码位的输出流中产生伪随机数的视频源和接收装置，密码位用于对视频接收装置进行认证的对称加密和解密过程。基于该方法的这种随机数产生装置的一个实例如美国专利申请公开 No.2004156500 所述。

另一方法和设备集成了基于热噪声产生元件产生的热噪声或者甚至是发光元件基于光产生的噪声的模拟随机数发生器，如 EP 1 544726 A1 所述。相关的方法和设备在 GB 2390271 中被描述。最普通的方法是利用噪声源作为偶然性的起源，利用放大器基于噪声来放大波形，利用时钟信号来指示模数转换器对放大后的噪声波形进行采样的间隔。尽管这种方法能够产生真正的随机数序列，但是更关心的是模拟随机数发生器的噪声产生元件中出现故障的情况。这种失效可能只是局部的并且仅仅限制噪声波形的范围。因为设备会继续输出“随机”数，所以这种类型的故障不会立即显示出来。但是对于密码学系统，这种情况可视为潜在的严重安全隐患。

发明内容

因此，本发明的目的是改善产生密码学随机数发生器种子或者产生随机数的过程。

根据本发明的独立方法权利要求 1 和 2 以及独立设备权利要求 13 和 14 实现了上述目标。在从属权利要求中描述了优选实施例。

下面参照详细的示例性实施例描述本发明。显然本发明能够以多种形式实施，有些形式可以与公开的实施例很不相同。因此，这里所公开的具体结构和功能细节仅仅是代表性的，而不是要限制本发明的范围。

根据本发明的一个实施例，输入图像的至少一部分，但是也可以利用多个图像。然后选择该图像的像素，每个像素提供有相关联的位置和颜色信息。基于与所选择的像素相关联的位置和颜色信息来计算预定数量的位。然后将这些位用于产生密码学随机数发生器的种子。

优选地，使用者可以自己选择和/或输入图像。这样给予使用者独特的优势，能够在任何时候改变产生密码学随机数发生器种子的源，甚至用使用者需要的任何图像来产生种子，这使得使用者对过程有更好的控制。

在本发明的一个实施例中，可包括扫描仪，以便扫描设备使用者提供的打印图像。这是设备使用者提供输入随机数种子发生器的初始图像的机制中的一种简单机制。当根据目标可用性、尺寸和成本设计和建立设备时，这种机制允许有灵活性。

在本发明的一个实施例中，可包括相机，以便在设备使用者进行选择时照相。这是设备使用者提供输入随机数种子发生器的初始图像的机制中的一种简单机制。

当根据目标可用性、尺寸和成本设计和建立设备时，这种机制允许有灵活性。

在本发明的一个实施例中，图像的储存库（repository）（由使用者添加和去除）保持在设备的范围内。这是设备使用者提供输入随机数种子发生器的初始图像的机制中的一种简单机制。当根据目标可用性、尺寸和成本设计和建立设备时，这种机制允许有灵活性。

在本发明的一个实施例中，使用线性反馈移位寄存器（LFSR）来支持种子产生。所使用的 LFSR 的尺寸将取决于需要的种子的尺寸，因此可以使用 n 位 LFSR 配置（其中 n 是 LFSR 中寄存器元件的数量）。LFSR 配置可以是内部 XOR LFSR（第一类）或外部 XOR LFSR（第二类），或者是这两类的组合。

在本发明的一个实施例中，使用多输入移位寄存器（MISR）来支持种子产生。所使用的 MISR 的尺寸将取决于需要的种子的尺寸，因此可以使用 n 位 MISR 配置（其中 n 是 MISR 中寄存器元件的数量）。

通过扫描仪、相机或者通过从图像储存库中选择所提供的图像成分的颜色和位置用作 LFSR 或 MISR 的输入。可以使用图像的每一个像素成分作为 LFSR 或 MISR 的输入，尽管有些情况下这是有用的和期望的，但是如果信息熵没有合适的增益，这通常会很慢。

最佳方案是仅仅使用图像的一组随机像素成分，这一组随机像素成分随机地选择作为各种标准的函数，这些标准例如是时钟计时、前一个像素的颜色和位置、包含像素的当前线路数量、或者甚至是一些系统特定伪随机可变源。这给出更安全的种子产生。

此外，优选基于所输入图像的尺寸、颜色密度和/或颜色变化来计算反映所输入图像适合性的品质因素；然后将计算得到的品质因素与预定的阈值进行比较，例如可基于期望的安全水平选择预定的阈值。如果比较结果是所述图像不合适，则拒绝图像或者输出警告。如果比较结果是所述图像

合适，则接受所述图像。此外在后一种情况下，可将信息给予使用者。这个特点使得使用者能够确信他输入的图像会给出充分安全的密钥。尽管如此，使用者仍然完全地控制过程。

另一最佳方案是像素尺寸对准 MISR 或 LFSR 中寄存器元件的数量，即，为了输入 32 位 MISR，256 位像素缩小为 32 位像素。如果需要或要求进一步的处理，则可将 LFSR 或 MISR 的输入（或者输出）通过功能电路。

LFSR 或 MISR 的输出累积在 m 位存储器缓冲中，其中 m 是要求的密码学种子的尺寸，并且是 LFSR 或 MISR 的输出的 n 位的倍数。在存储器缓冲中不同的累积方式都是可行的。当放弃溢出的最高有效位值时，可以利用 XOR 功能或者简单的算术累积对上述到后面的 m 位存储器缓冲的输出进行轮叫调度分配。

大多数密码学随机数发生器采用固定尺寸的种子，因此种子中的信息熵程度直接或间接地影响受所保护的数据的安全水平。根据安全水平和应用领域的要求，本发明允许要使用的种子尺寸可变。如果或者当设备使用者需要时，本发明还允许新的密码学种子的再产生。

也可以直接使用信息熵，而不是产生密码学随机数发生器的种子。对于有些密钥（除了取决于进一步测试和处理的不对称密钥之外），可以直接从信息熵源产生密钥，即，作为结果的 m 位密码学种子直接用作密钥，不需要产生密码学随机数发生器的种子。

附图说明

图 1 是现有技术的内部 n 阶线性反馈移位寄存器（又称为第一类 LFSR）的示意图。

图 2 是另一种现有技术的外部 n 阶线性反馈移位寄存器（又称为第二类 LFSR）的示意图。

图 3 是现有技术的多输入移位寄存器（MISR）的实施例的示意图。

图 4 是根据本发明一个实施例的密码学随机数种子产生系统的高级示意图。

图 5 是本发明的图像处理单元的方块流程图。

具体实施方式

参照附图，下面描述本发明的一个实施例。图 1 是示出本发明一个实施例中使用的内部 n 阶线性反馈移位寄存器（第一类 LFSR）的示意图。图 1 的 LFSR 包括一系列双稳态多谐振荡器（flip-flop），其输出按照异或（XOR）配置来组合，以便形成反馈机制。每个双稳态多谐振荡器的输出通过寄存器从一个位前进到次高有效位（the next significant bit）。两个或更多个双稳态多谐振荡器的输出被通过执行 XOR 而组合在一起，并且被馈入后面的双稳态多谐振荡器的输入。RESET 位是每个双稳态多谐振荡器的另一个输入，用于复位或者设定双稳态多谐振荡器的状态。一系列的 N 个双稳态多谐振荡器的输出组合形成 LFSR 的 n 位输出（ Q_1 至 Q_n ）。

图 2 是示出本发明另一实施例中如上所述使用的外部 n 阶线性反馈移位寄存器（第二类 LFSR）的示意图。

图 3 是示出根据本发明另一实施例的 n 位多输入移位寄存器（MISR）的示意图。图 3 的 MISR 包括一系列双稳态多谐振荡器，其输出按照异或（XOR）配置与输入数据位（ D_1 至 D_n ）组合，用作系列中下一个双稳态多谐振荡器的输入。最后一个双稳态多谐振荡器的输出也反馈给系列中第一个双稳态多谐振荡器。RESET 位是每个双稳态多谐振荡器的另一个输入，用于复位或者设定双稳态多谐振荡器的状态。MISR 中一系列的 N 个双稳态多谐振荡器的输出组合形成 MISR 的 n 位输出（ Q_1 至 Q_n ）。

图 4 的方块图中，相机 2 或扫描仪 4 用于提供由设备使用者选择、要被直接用于密码学随机数种子产生的图像 1 或多个图像。相机 2 或扫描仪 4 也可用于提供要被存储在储存库 3 中的多个图像 1，设备使用者可从多个图像 1 中做出一个或多个选择，选择的图像 1 用于密码学随机数种子的产生。

图 5 的方块流程图中示出的例子是，使用者选择的图像 1 或多个图像怎样通过功能电路被馈入的，该功能电路选择部分或所有像素。选择单元 5 利用像素待处理的位置值（基于图像尺寸的 X , Y 轴）和颜色值（取决

于颜色空间的类型和位深)提取某些随机像素,以产生并累积作为 n 位缓冲数据。

所选择的像素具有位置 (x, y) 和颜色(可以是灰度, rgb 、 cym 、 hsb 、 yuv 或者可能颜色空间的任意组合,与相应的位深一起用于获得更高的精度)值,这些值用于计算具有 N 位($b1$ 至 b_n)的结果。根据使用者选择的图像 1 或多个图像的所选择的像素可以按照需要反复多次计算 N 位的结果。通过只接受那些尺寸、颜色密度和颜色变化超过一些阈值的图像 1 能够进一步提高使用者选择的图像 1 或多个图像的质量。可以单独地、也可以一次性全部地估计这些特性。在后一种情况下,基于代表不同特性的值计算出一个值。以同样的方式,也可以确定是否发出警告。

此外,通过保持每个图像的无用数据(通过单向散列函数产生)可以记住已经用于产生密码学随机数种子的图像,从而防止下一次图像被再选择,然后每个图像的无用数据可用于拒绝图像和/或输出警告。

图 4 示出利用移位寄存器的两个不同替代实施例。图 4 中,取左侧所示的选项,通过将每个时钟周期的每个位进行位移作为图 1 或图 2 的 LFSR 的 RESET 位的输入,前一步骤产生的作为结果的 N 位($b1$ 至 b_n)被使用。虽然方块图示出最高有效位(msb)的位移,但是也可以将最低有效位(lsb)进行位移作为 LFSR 的 RESET 位的输入。也可以用任一个位作为 LFSR 的 RESET 位的输入。随后的从前一步骤产生的作为结果的 N 位用作 LFSR 的 RESET 位的其它输入。LFSR 的每个时钟周期产生 N 个输出位($Q1$ 至 Q_n),这些输出位将被累积作为用于密码学随机数发生器的 $m \times n$ 位种子(其中 m 是任意倍数,并且 m 是整数,用于确定所需的种子位数)。

图 4 方块图的右侧示出本发明的另一实施例,其中,上述功能电路产生的作为结果的 N 位($b1$ 至 b_n)用作 n 位 MISR 的输入,同时,任一个位(虽然图中标出最高有效位)用作每个时钟周期 MISR 的 RESET 位的输入。所有 N 个位($b1$ 至 b_n)平行地用作 MISR 的输入($D1$ 至 D_n)。MISR 的每个时钟周期产生 N 个输出位($Q1$ 至 Q_n),以累积作为用于密码学随机数发生器的 $m \times n$ 位种子(其中 m 是任意倍数,用于确定所需的

种子位数)。

本发明并不限于上述实施例，在所附权利要求书所提出的本发明的范围内可以作出各种变型和改型。因此，希望这样的变型和改型也涵盖在本发明的技术范围内。

多输入移位寄存器MISR

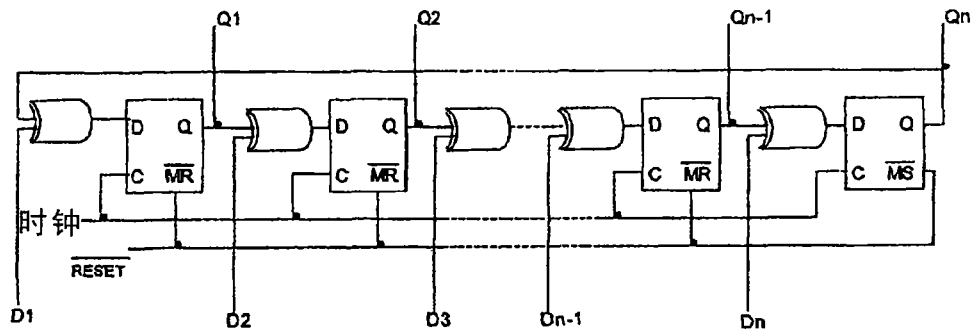


图3

密码RNG种子产生

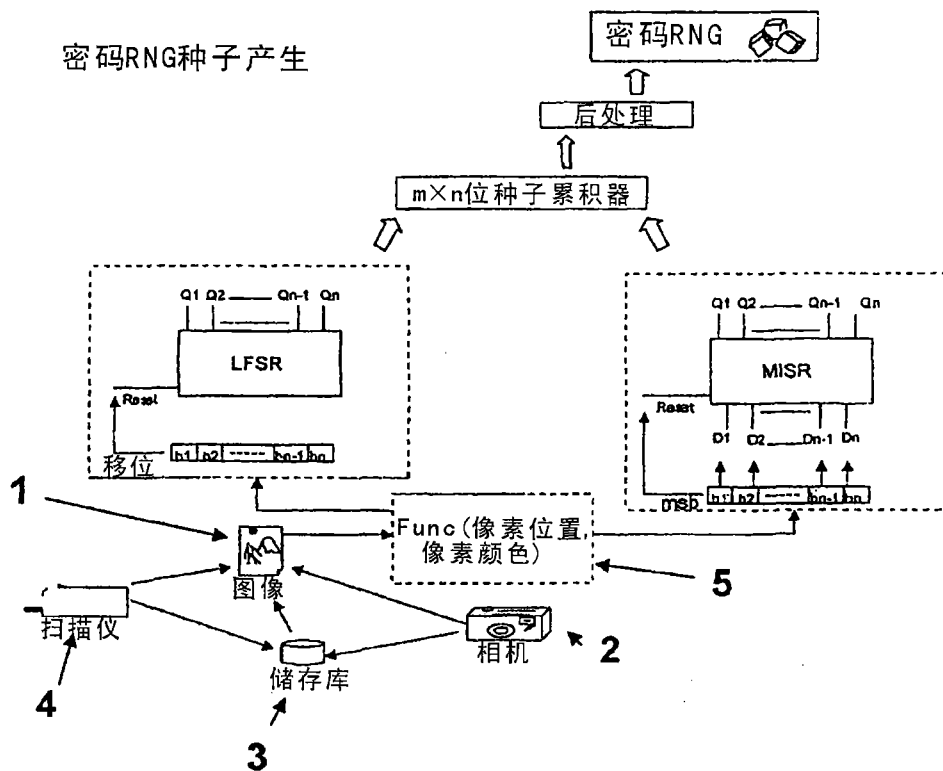


图4

Func (像素位置, 像素颜色)

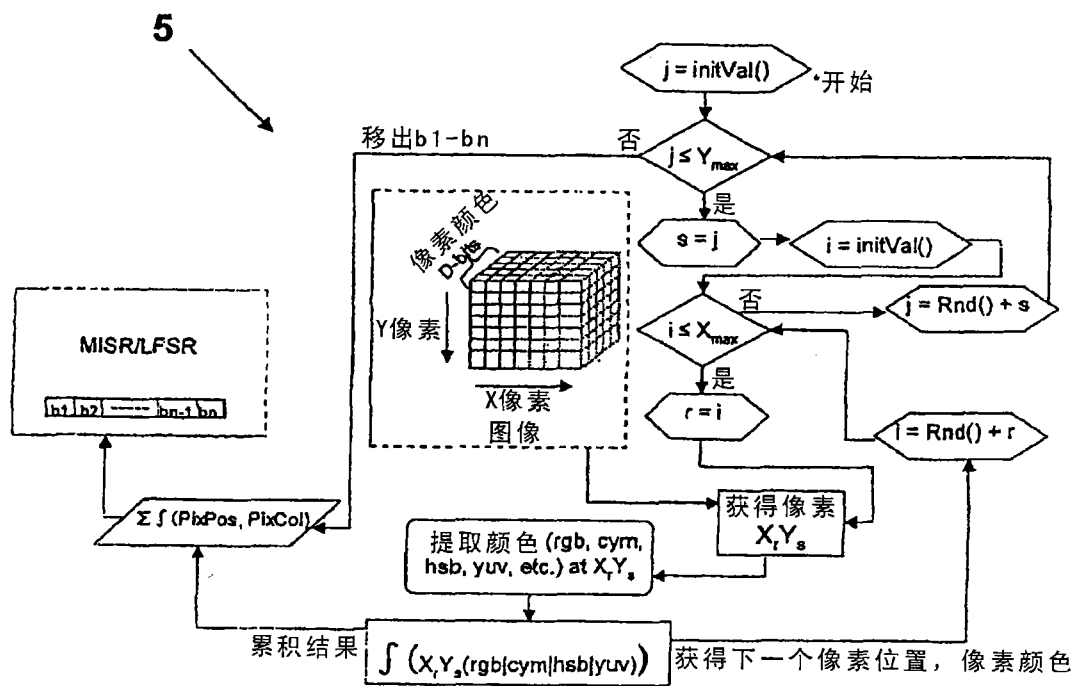


图5