



(12) 发明专利申请

(10) 申请公布号 CN 102073828 A

(43) 申请公布日 2011. 05. 25

(21) 申请号 201010567683. 0

(22) 申请日 2010. 11. 23

(30) 优先权数据

12/624, 407 2009. 11. 23 US

(71) 申请人 柯尼卡美能达系统研究所公司

地址 美国加利福尼亚州

(72) 发明人 田宜彬 明伟

(74) 专利代理机构 北京集佳知识产权代理有限公司

公司 11227

代理人 王萍 陈炜

(51) Int. Cl.

G06F 21/24 (2006. 01)

G06K 19/06 (2006. 01)

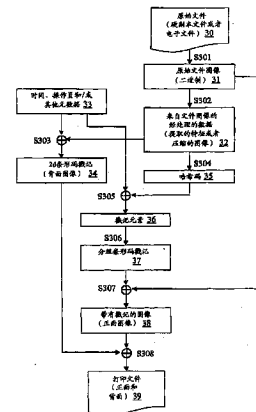
权利要求书 3 页 说明书 7 页 附图 3 页

(54) 发明名称

使用分级条形码戳记来检测条形码的更改的文件认证

(57) 摘要

本发明涉及一种生成自认证打印文件和对打印文件进行认证的方法。打印文件的正面包含对所提取的文件内容特征进行编码的 2d 条形码。这些特征被哈希编码为哈希码, 转换为条形码戳记元素, 并且通过重复该戳记元素而变换为分级条形码戳记。该分级条形码戳记作为灰色背景图案被打印在打印文件的同一页的正面上。为了对打印文件进行认证, 读取背面上的条形码以提取文件特征。将这些特征哈希编码为哈希码并且与从文件正面上的分级条形码戳记提取的哈希码进行比较以检测背面的条形码的任何更改。此外, 比较从文件的正面和背面提取的文件特征。



1. 一种在数据处理和打印系统中实现的用于生成自认证打印文件的方法,包括:
  - a、获得原始文件图像;
  - b、处理所述原始文件图像以生成经处理的数据;
  - c、生成第一条形码戳记,其对步骤 b 中生成的所述经处理的数据进行编码;
  - d、通过根据预先定义的模式重复条形码戳记元素来生成分级条形码戳记,所述条形码戳记元素对根据步骤 b 中生成的所述经处理的数据来计算的码进行编码;
  - e、将所述分级条形码戳记和所述原始文件图像打印在记录介质的正面上,并且将所述第一条形码戳记打印在同一记录介质的正面或背面上,以生成所述打印文件。
2. 如权利要求 1 所述的方法,其中,步骤 e 包括生成表示所述分级条形码戳记的背景图案并且将所述背景图案与所述原始文件图像重叠地打印在所述记录介质的正面上。
3. 如权利要求 2 所述的方法,其中,所述背景图案包括以灰度形式打印的或者未打印的条形码码块,以及其中,所述原始文件图像是被打印为黑色的二进制图像。
4. 如权利要求 1 所述的方法,其中,步骤 d 包括:
  - d1、根据步骤 b 中生成的所述经处理的数据来生成哈希码;
  - d2、生成对所述哈希码进行编码的所述条形码戳记元素;以及
  - d3、通过按照所述预先定义的模式重复所述条形码戳记元素来根据所述条形码戳记元素生成所述分级条形码戳记。
5. 如权利要求 1 所述的方法,其中,在步骤 c 中所述第一条形码进一步对与所述打印文件相关的元数据进行编码,以及其中,在步骤 d 中所述分级条形码戳记进一步对所述元数据进行编码。
6. 如权利要求 1 所述的方法,其中,所述经处理的数据包括提取的图形对象、提取的位图图像对象、提取的文本、所述原始文件图像的低空间分辨率的版本和所述原始文件图像的压缩版本中的一个或多个。
7. 一种在数据处理系统中实现的用于对打印文件进行认证的方法,所述打印文件包括打印在记录介质的正面上的分级条形码戳记和文件图像以及打印在同一记录介质的正面或背面上的第一条形码戳记,所述方法包括:
  - a、从所述打印文件获得正面图像和背面图像;
  - b、从所述正面图像提取所述文件图像和所述分级条形码戳记;
  - c、处理在步骤 b 中提取的所述文件图像以获得第一经处理的数据;
  - d、从在步骤 b 中提取的所述分级条形码戳记提取第一码;
  - e、读取和解码所述正面图像和 / 或所述背面图像中的所述第一条形码戳记以获得被编码在其中的第二经处理的数据;
  - f、根据所述第二经处理的数据计算第二码;
  - g、比较所述第一码和所述第二码以确定所述第一条形码戳记是否已被更改;以及
  - h、比较第一经处理的数据和第二经处理的数据以确定所述打印文件是否已被更改。
8. 如权利要求 7 所述的方法,其中,所述分级条形码戳记形成所述文件的正面上的背景图案并且所述文件图像与所述背景图案重叠。
9. 如权利要求 8 所述的方法,其中,所述背景图案包括以灰度形式打印的或者未打印的条形码码块,其中,所述文件图像是被打印为黑色的二进制图像,以及其中,步骤 b 包括

区分所述正面图像中的灰色像素和黑色像素。

10. 如权利要求 7 所述的方法,其中,步骤 d 包括:

d1、根据所述分级条形码戳记生成条形码戳记元素,其中,所述分级条形码戳记包括根据预先定义的模式重复的所述条形码戳记元素;以及

d2、对所述条形码戳记元素进行解码以获得所述第一码。

11. 如权利要求 7 所述的方法,进一步包括:

i、从在步骤 b 中提取的所述分级条形码戳记提取第一元数据;

j、获得被编码在所述第一条形码戳记中的第二元数据;以及

k、比较所述第一元数据和所述第二元数据以确定所述打印文件是否已被更改。

12. 如权利要求 7 所述的方法,其中,所述第一经处理的数据包括提取的图形对象、提取的位图图像对象、提取的文本、所述文件图像的低空间分辨率的版本和所述文件图像的压缩版本中的一个或多个。

13. 一种包括计算机可用介质的计算机程序产品,所述计算机可用介质具有嵌入在其中的用于控制数据处理装置的计算机可读程序代码,所述计算机可读程序代码被配置为使所述数据处理装置执行用于生成自认证打印文件的过程,所述过程包括:

a、接收原始文件图像;

b、处理所述原始文件图像以生成经处理的数据;

c、生成第一条形码戳记,其对步骤 b 中生成的所述经处理的数据编码;

d、通过根据预先定义的模式重复条形码戳记元素来生成分级条形码戳记,所述条形码戳记元素对根据步骤 b 中生成的所述经处理的数据来计算的码进行编码;

e 控制打印机将所述分级条形码戳记和所述原始文件图像打印在记录介质的正面上,并且将所述第一条形码戳记打印在同一记录介质的正面或背面上,以生成所述打印文件。

14. 如权利要求 13 所述的计算机程序产品,其中,步骤 e 包括生成表示所述分级条形码戳记的背景图案并且将所述背景图案与所述原始文件图像重叠地打印在所述记录介质的正面上。

15. 如权利要求 14 所述的计算机程序产品,其中,所述背景图案包括以灰度形式打印的或者未打印的条形码码块,以及其中,所述原始文件图像是被打印为黑色的二进制图像。

16. 如权利要求 13 所述的计算机程序产品,其中,步骤 d 包括:

d1、根据步骤 b 中生成的所述经处理的数据来生成哈希码;

d2、生成对所述哈希码进行编码的所述条形码戳记元素;以及

d3、通过按照所述预先定义的模式重复所述条形码戳记元素来根据所述条形码戳记元素生成所述分级条形码戳记。

17. 如权利要求 13 所述的计算机程序产品,其中,在步骤 c 中所述第一条形码进一步对与所述打印文件相关的元数据进行编码,以及其中,在步骤 d 中所述分级条形码戳记进一步对所述元数据进行编码。

18. 如权利要求 13 所述的计算机程序产品,其中,所述经处理的数据包括提取的图形对象、提取的位图图像对象、提取的文本、所述原始文件图像的低空间分辨率的版本和所述原始文件图像的压缩版本中的一个或多个。

19. 一种包括计算机可用介质的计算机程序产品,所述计算机可用介质具有嵌入在其

中的用于控制数据处理装置的计算机可读程序代码,所述计算机可读程序代码被配置为使所述数据处理装置执行用于对打印文件进行认证的过程,所述打印文件包括打印在记录介质的正面上的分级条形码戳记和文件图像以及打印在同一记录介质的正面或背面上的第一条条形码戳记,所述过程包括:

a、从所述打印文件接收正面图像和背面图像;

b、从所述正面图像提取所述文件图像和所述分级条形码戳记;

c、处理在步骤 b 中提取的所述文件图像以获得第一经处理的数据;

d、从在步骤 b 中提取的所述分级条形码戳记提取第一码;

e、读取和解码所述正面图像和 / 或所述背面图像中的所述第一条条形码戳记以获得被编码在其中的第二经处理的数据;

f、根据所述第二经处理的数据计算第二码;

g、比较所述第一码和所述第二码以确定所述第一条条形码戳记是否已被更改;以及

h、比较第一经处理的数据和第二经处理的数据以确定所述打印文件是否已被更改。

20. 如权利要求 19 所述的计算机程序产品,其中,所述分级条形码戳记形成所述文件的正面上的背景图案并且所述文件图像与所述背景图案重叠。

21. 如权利要求 20 所述的计算机程序产品,其中,所述背景图案包括以灰度形式打印的或者未打印的条形码码块,其中,所述文件图像是被打印为黑色的二进制图像,以及其中,步骤 b 包括区分所述正面图像中的灰色像素和黑色像素。

22. 如权利要求 19 所述的计算机程序产品,其中,步骤 d 包括:

d1、根据所述分级条形码戳记生成条形码戳记元素,其中,所述分级条形码戳记包括根据预先定义的模式重复的所述条形码戳记元素;以及

d2、对所述条形码戳记元素进行解码以获得所述第一码。

23. 如权利要求 19 所述的计算机程序产品,进一步包括:

i、从在步骤 b 中提取的所述分级条形码戳记提取第一元数据;

j、获得被编码在所述第一条条形码戳记中的第二元数据;以及

k、比较所述第一元数据和所述第二元数据以确定所述打印文件是否已被更改。

24. 如权利要求 19 所述的计算机程序产品,其中,所述第一经处理的数据包括提取的图形对象、提取的位图图像对象、提取的文本、所述文件图像的低空间分辨率的版本和所述文件图像的压缩版本中的一个或多个。

## 使用分级条形码戳记来检测条形码的更改的文件认证

### 技术领域

[0001] 本发明涉及一种文件认证方法,其使用条形码对文件的内容进行编码,具体地,本发明涉及如下的文件认证方法,其中分级条形码戳记被用作背景图案以减小条形码更改的影响。

### 背景技术

[0002] 条形码是用于对数据进行编码的机器可读符号表示法的一种形式,并且已被广泛地引入各种应用领域中。二维条形码(2d 条形码)是该符号表示法的一种模式。其通常可以用于对文本、数字、图像和二进制数据流进行编码,并且已用于身份卡、货运标签、证书和其他文件等。广泛使用的 2d 条形码的示例包括 PDF417 标准和 QR Code<sup>®</sup>,并且软件和硬件产品已可用于打印和读取这些 2d 条形码。

[0003] 可以包括文本、图形、图像等的原始数字文件常常被打印,并且所打印的硬副本被分发、复制等,并且随后常常被扫描回数字形式。这被称为闭环过程。对扫描的数字文件进行认证指的是确定扫描的文件是否是原始数字文件的可信副本,即文件是否在其为硬副本形式时已被更改。更改出现的原因可能是蓄意的行为或者意外的事件。存在两种用于对打印文件进行认证的方法。第一种方法利用存储原始文件图像的数据库,并且将扫描的文件图像与原始图像进行比较。

[0004] 第二种方法消除了对原始图像的数据库的依赖。具体地,已开发了使用二维(2d)条形码对打印文件进行认证的方法。典型地,该方法将原始文件的内容或者从原始文件提取的可用于对文件进行认证的其他信息(通常被称为认证信息)编码为 2d 条形码(被称为认证条形码)。条形码被打印在与打印文件相同的记录介质上,例如打印在打印文件的正面或背面上。文件的内容可以是文件页面的位图图像,文件中包含的文本、图形或图像,或者它们的混合。为了对标有认证条形码的打印文件进行认证,对文件进行扫描以获得表示文件内容的扫描数据,例如位图图像、通过使用光学字符识别(OCR)技术提取的文本等。认证条形码也被扫描并且其中包含的数据(认证数据)被提取。随后将扫描数据与认证数据进行比较以确定从文件最初被打印开始打印文件的任何部分是否已被更改,即文件是否是可信的。一些认证技术仅确定是否已发生任何更改,一些认证技术能够确定什么内容已被更改以及更改是什么。标有认证条形码的打印文件被称为自认证的,这是因为不需要打印文件上的信息以外的信息用于对其内容进行认证。

### 发明内容

[0005] 在标有 2d 条形码的自认证文件中,在文件被发行之时条形码自身易于被更改。因此,本发明涉及一种文件认证方法和相关装置,其基本上消除了由于相关技术的限制和缺陷引起的一个或多个问题。

[0006] 本发明的目的在于提供一种文件认证方法,其允许检测认证条形码的任何更改。

[0007] 在后面的描述中将阐述本发明的另外的特征和优点,并且其中一部分通过该描述

这些特征和优点会是明显的,或者可以通过实施本发明来被认识到。通过所撰写的说明书及其权利要求以及附图中具体指出的结构,将实现和达到本发明的这些目的和其他优点。

[0008] 为了实现这些和 / 或其他目的,如所实施的和广泛描述的,本发明提供了一种在数据处理和打印系统中实现的用于生成自认证打印文件的方法,其包括:(a) 获得原始文件图像;(b) 处理原始文件图像以生成经处理的数据;(c) 生成第一条形码戳记,其对步骤(b) 中生成的经处理的数据进行编码;(d) 通过根据预先定义的模式重复条形码戳记元素来生成分级条形码戳记,条形码戳记元素对根据步骤(b) 中生成的经处理的数据来计算的码进行编码;(e) 将分级条形码戳记和原始文件图像打印在记录介质的正面上,并且将第一条形码戳记打印在同一记录介质的正面或背面上,以生成打印文件。

[0009] 在另一方面,本发明提供了一种在数据处理系统中实现的用于对打印文件进行认证的方法,该打印文件包括打印在记录介质的正面上的分级条形码戳记和文件图像以及打印在同一记录介质的正面或背面上的第一条形码戳记,该方法包括:(a) 从打印文件获得正面图像和背面图像;(b) 从正面图像提取文件图像和分级条形码戳记;(c) 处理在步骤(b) 中提取的文件图像以获得第一经处理的数据;(d) 从在步骤(b) 中提取的分级条形码戳记提取第一码;(e) 读取和解码正面图像和 / 或背面图像中的第一条形码戳记以获得被编码在其中的第二经处理的数据;(f) 根据第二经处理的数据计算第二码;(g) 比较第一码和第二码以确定第一条形码戳记是否已被更改;以及(h) 比较第一经处理的数据和第二经处理的数据以确定打印文件是否已被更改。

[0010] 在另一方面,本发明提供了使数据处理装置执行以上方法的计算机程序产品。

[0011] 应当理解,前面的一般描述和后面的详细描述是示例性的和解释性的,意在提供对要求保护的本发明的进一步的解释。

## 附图说明

[0012] 图 1 图示了使用克罗内克 (Kronecker) 积运算生成分级条形码戳记的示例。

[0013] 图 2 图示了根据本发明的实施例的具有作为背景的条形码图案的打印文件的正面。

[0014] 图 3 示意性地图示了根据本发明的实施例的生成自认证文件的方法。

[0015] 图 4 和 5 示意性地图示了根据本发明的实施例的确定打印文件的可信性的方法。

## 具体实施方式

[0016] 本发明的实施例提供了一种生成自认证打印文件并且随后对打印文件进行认证的方法。该自认证文件具有其背面 (或正面) 上的 2d 条形码戳记,该条形码戳记对文件正面上的文件图像或从文件内容提取的特征进行编码。为了增强 2d 条形码的安全性,可选地与所期望的元数据组合的文件图像或者所提取的文件特征被哈希编码为合理地短的哈希码,并且被转换为 2d 条形码戳记元素。随后通过根据预先定义的模式重复该戳记元素,将该戳记元素变换为分级条形码戳记,这可以通过使用克罗内克积矩阵运算来实现。分级条形码戳记被打印作为用于打印文件正面的背景图案 (诸如灰色图案);文件的图像被打印在该背景图案上。正面图像和背面图像 (如果存在) 被打印在单张记录介质上以流通。

[0017] 为了对打印文件进行认证,被编码为背面 (或正面) 上的 2d 条形码的数据 (所提

取的特征、压缩图像等)被提取并且被哈希编码为哈希码,并且与从文件正面上的分级条形码提取的哈希码进行比较。这有助于确定文件的背面(或正面)上的2d条形码是否已被更改。

[0018] 2d条形码可以被打印在打印文件的正面和/或背面上。一般说来,如果2d条形码对诸如所提取的文本的相对少量的数据进行编码,则由于2d条形码戳记的数目会相对小,因此2d条形码可以被打印在文件的正面上。如果2d条形码对原始文件图像进行编码,则2d条形码戳记的数目会相对大,并且在正面上打印所有2d条形码可能不实用。在以下实施例描述中,2d条形码被打印在背面上,然而应当理解,其也可以被打印在正面上或者被打印在正面和背面上。

[0019] 由 $\otimes$ 表示的克罗内克积是针对两个矩阵的运算,得到分块矩阵。如果A是 $m \times n$ 矩阵并且B是 $p \times q$ 矩阵,则克罗内克积 $\mathbf{A} \otimes \mathbf{B}$ 是 $mp \times nq$ 矩阵。图1图示了戳记元素11以及戳记元素11和其自身的克罗内克积(分级条形码)12。该示例中的克罗内克积可以以矩阵形式表述如下:

$$[0020] \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

[0021] 在该示例中,戳记元素是 $m \times n = 3 \times 2$ 矩阵并且该戳记元素和其自身的克罗内克积是 $m^2 \times n^2 = 9 \times 4$ 矩阵。

[0022] 分级条形码还可以通过形成戳记元素与预先定义的矩阵的克罗内克积来生成。换言之,该分级条形码是通过按预先定义的方式重复戳记元素而形成的。例如,预先定义的矩阵可以是

[0023]  $(1 \ 0 \ 1)$ 、

[0024]  $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$  或者

[0025]  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  等。

[0026] 尽管克罗内克积运算是一种用于生成分级条形码的便利方法,但是分级条形码也可以通过其他适当的方式生成。更一般地,通过根据预先定义的模式重复戳记元素来生成分级条形码。重复的次数不必是整数;例如,由于记录介质的尺寸,戳记元素的最后一次重复可能仅包括整个戳记元素的一部分。再者,可以允许在重复的戳记元素之间具有所期望的宽度的空白空间。只要戳记元素被重复,则分级条形码可以包括任何这样的模式。在以下描述中,克罗内克积运算被用作用于生成分级条形码的示例。

[0027] 图2图示了标有作为背景图案的分级条形码21的文件20的正面。分级条形码21的每个码块(tile)21a表示二进制值。分级条形码是以灰度形式打印的;换言之,每个条形码码块21a是灰色的或白色的(未打印)。灰度的灰阶值可以是例如100(如果255是黑色)。文件的内容22(例如,文本、图形、图像等)被以黑色打印在背景图案21上(即它们

重叠)。

[0028] 条形码码块 21a 的尺寸大于文件认证中使用的常规的 2d 条形码的码块尺寸。在常规的 2d 条形码中,由于需要使码块尺寸最小以便于使信息密度最大,码块尺寸可以小至 4 至 7 个像素。在本发明的实施例中,由于分级条形码被用作背景图案并且条形码码块 21a 被打印在文件内容下面,因此条形码码块优选地具有合理的码块尺寸,从而大部分码块不会因打印的文件内容而完全变得模糊。码块尺寸优选地被选择为,即使当码块因打印的文件内容而部分地变得模糊时,仍可以读取大部分码块的二进制值。在一个示例中,码块 21a 的尺寸是  $60 \times 60$  个像素(具有 600dpi 的分辨率);形成分级条形码的条形码戳记元素具有  $21 \times 21$  个码块,并且条形码戳记元素通过克罗内克乘法与 5(竖直) $\times$ 4(水平)矩阵相乘以形成配合信纸尺寸纸张的具有  $150 \times 84$  个码块的分级条形码。在另一示例中,码块 21a 的尺寸是  $100 \times 100$  个像素(具有 600dpi 的分辨率);形成分级条形码的条形码戳记元素据有  $21 \times 21$  个码块,并且条形码戳记元素通过克罗内克乘法与 3(竖直) $\times$ 2(水平)矩阵相乘以形成配合信纸尺寸纸张的具有  $63 \times 42$  个码块的分级条形码。

[0029] 应当注意,图 2 中的码块 21a 的尺寸和内容 22 的尺寸出于说明的目的而被放大。图 1 中图示的示例性分级条形码 12 用于构造图 2 中的示例性背景图案 21(重复三次)。这是非常简化的示例并且仅用于说明的目的。

[0030] 尽管在图 2 中将背景条形码图案示出为基本上覆盖整个页面,但是背景图案可以仅覆盖一部分页面,例如,条形码可以仅呈现在页面上的空白空间或者页边中,行之间的空间中,等等。

[0031] 如前面所述,分级条形码 21 是条形码元素和另一矩阵(其可以是该条形码元素自身(参见图 1))的克罗内克积。分级条形码是冗余的,使得其更加鲁棒并且易于解码。因此,例如,如果一些条形码码块因打印的内容而变得模糊并且不能被读取,则可以使用其他码块(可以被读取的码块)的值并且仍可以对分级条形码进行解码。

[0032] 图 3 示意性地图示了根据本发明的实施例的用于生成标有作为正面的背景图案的分级条形码的自认证文件的编码和打印方法。如图 3 中所示,可以对硬副本形式或者电子形式的原始文件 30 进行处理以生成二进制原始文件图像 31(步骤 S301)。如果原始文件 30 为硬副本形式,则步骤 S301 可以包括扫描,而如果扫描的文件或者原始的电子文件是灰阶图像,则步骤 S301 可以包括阈值化处理。

[0033] 对二进制原始文件图像 31 进行处理以从该文件图像生成经处理的数据 32(步骤 S302)。该处理步骤可以包括从文件图像提取图形或位图图像对象,通过 OCR 技术提取文本等,在该情况中经处理的数据 32 是提取的特征。从文件图像提取特征在许多文件认证方法中的常见步骤,并且任何适当的技术可以用于实现该步骤。经处理的数据 32 还可以是原始文件图像的低空间分辨率的版本。可替代地,经处理的数据 32 可以是原始文件图像自身的压缩版本。更一般地,处理步骤 S302 对原始文件图像 31 进行处理以减少数据量;可以应用任何适当的处理。经处理的数据 32 是通过该处理步骤生成的数据并且可以是任何适当的数据类型。

[0034] 经处理的数据 32 随后被编码为 2d 条形码戳记 34 以被打印在打印文件的背面上(步骤 S303)。可选地,与打印文件相关的诸如时间信息、操作员信息等所期望的元数据 33 也可以与经处理的数据一起被编码为 2d 条形码 34(步骤 S303)。



[0035] 作为可替换方案,2d 条形码戳记可以直接对(未压缩的)原始文件图像进行编码,在该情况中未执行步骤 S302。然而,原始文件图像典型地牵涉大量的数据,并且直接将原始文件图像(不经压缩)直接编码为 2d 条形码常常是不实用的。

[0036] 同时,将哈希函数应用于经处理的数据 32 以生成哈希码 35(步骤 S304)。优选地,哈希码是合理地短的,诸如 64、128 或 256 位等。随后根据哈希码 35 生成戳记元素 36(步骤 S305)。可选地,元数据 33 也与哈希码一同被编码在戳记元素中(步骤 S305)。随后,将克罗内克运算应用于戳记元素 36 以生成分级条形码戳记 37(步骤 S306)。分级条形码戳记 37 可以是戳记元素 36 和其自身的克罗内克积,或者戳记元素 36 和预先定义的矩阵的克罗内克积。这里应当注意,戳记元素 36 和分级条形码戳记 37 可以是矩阵的形式(例如,存储在计算机中的数据)并且它们不一定是条形码戳记的二维图像。

[0037] 在生成分级条形码戳记 37 之后,其与二进制原始文件图像 31 组合以生成将被打印在打印文件的正面上的带有戳记的图像 38(步骤 S307)。带有戳记的图像 38 具有包括表示分级条形码戳记 37 的灰色(打印)和白色(未打印)码块的背景图案。二进制(黑色和白色)原始文件图像 31 被叠置在该背景图案上。图 2 中示出了带有戳记的图像 38 的示例。

[0038] 正面图像 38 被打印在记录介质的正面上并且 2d 条形码戳记 34 被打印在同一记录介质的背面上,以生成打印文件 39(步骤 S308)。

[0039] 在打印文件 39 发行和流通之后,可以使用图 4 和 5 中图示的方法对该文件或其副本进行认证。如图 4 中所示,对打印文件 400 的两面进行扫描(步骤 S501 和 S502)以获得正面图像 401 和背面图像 402。正面图像 401(据称基本上与正面图像 38 相同)是包含背景图案和文件内容的带有戳记的图像,而背面图像 402 包含 2d 条形码(据称与 2d 条形码戳记 34 相同)。这里,“据称相同”意味着如果打印文件未曾被更改,则打印文件 400 中的相关项目将基本上与打印文件 39 中的相应的项目相同(当然,作为打印和扫描过程中的正常的部分,可能引入某些伪像(artifact),但是它们基本上不会改变图像)。

[0040] 对正面图像 401 进行分析以提取文件图像(文件内容)403(步骤 S503)并且提取分级条形码戳记 404(步骤 S504)。在步骤 S503 和 S504 中,可以通过像素的灰阶值来区分分级条形码戳记 404 与文件图像 403。

[0041] 如果在编码和打印过程(图 3)期间,步骤 S302 包括从原始文件图像提取特征或者生成原始文件图像的低分辨率版本,则将同一提取过程应用于文件图像 403 以生成经处理的数据 405。如果步骤 S302 仅生成原始文件图像的压缩版本并且不包括提取特征或者生成低分辨率版本,则不执行步骤 S505。

[0042] 对所提取的分级条形码戳记 404 进行进一步的分析以提取戳记元素 406(步骤 S506)。在步骤 S504 和 S506 的优选实现方案中,认证算法具有关于分级条形码戳记的先验知识,诸如码块尺寸、戳记元素的规模( $m$ 和 $n$ )、克罗内克积中使用的预先定义的矩阵(如果存在)等。如前面提到的,分级条形码的许多码块会因文件内容而(部分地或者甚至完全地)变得模糊;分级条形码戳记的先验知识使得该算法能够利用分级条形码中的冗余来准确地确定戳记元素的值。可替换地,诸如码块尺寸、戳记元素的规模( $m$ 和 $n$ )等的关于分级条形码戳记的信息可以被编码在 2d 条形码戳记 34 中,或者被编码在打印在文件正面或背面上的分立的条形码戳记中。如果认证算法不具有关于分级条形码戳记的这种知识(先验

知识或者从条形码戳记获得的知识),则需要更加精密的匹配算法来确定与观察到的正面图像 401 的数据最佳匹配的这些参数(码块尺寸、m 和 n 等)的值。

[0043] 当然,在步骤 S506 期间,如果根据关于分级条形码戳记的知识发现背景图案与克罗内克积形式不一致,则确定文件已被更改。

[0044] 在确定戳记元素 406 之后,对其进行解码以获得被编码在其中的哈希码 407 以及元数据 408(如果存在)(步骤 S507 和 S508)。该解码过程是步骤 S305 的编码过程的逆过程。

[0045] 同时,读取背面图像中的 2d 条形码 402 以获得条形码数据 409(位流)(步骤 S509)。如前面所述,条形码数据 409 对元数据(可选)和在步骤 S302 中生成的经处理的数据 32(其可以从原始图像提取的特征、原始图像的分辨率减小的版本、原始图像数据的压缩版本等)进行编码。因此,对条形码数据 409 进行解码以获得被编码在其中的元数据 410 以及经处理的数据 411(步骤 S510 和 S511)。该解码过程是步骤 S303 的编码过程的逆过程。经处理的数据 411 可以包括所提取的特征、分辨率减小的版本、压缩图像等。哈希函数(与步骤 S304 中使用的哈希函数相同)被应用于经处理的数据 411 以计算哈希码 412(步骤 S512)。

[0046] 随后,如图 5 中所示,执行比较过程以确定打印文件 400 的可信性。首先,在步骤 S513 中,将从戳记元素 406(来自正面图像)获得的哈希码 407 与从 2d 条形码 402(来自背面图像)获得(计算)的哈希码 412 进行比较。如果这两个哈希码不同(步骤 S514 中的“否”),则这指示了 2d 条形码已被更改,并且判断打印文件 400 已被更改并且是不可信的(步骤 S517)。

[0047] 如果这两个哈希码相同(步骤 S514 中的“是”),则将从戳记元素 406(来自正面图像)获得的元数据 408 与从 2d 条形码 402(来自背面图像)获得的元数据 410 进行比较(步骤 S515)。如果这两个元数据不同(步骤 S516 中的“否”),则这也指示了 2d 条形码已被更改,并且判断打印文件 400 已被更改并且是不可信的(步骤 S517)。步骤 S515 和 S516 是可选的并且在元数据已被编码在条形码中的情况下执行。此外,步骤 S515 和 S516 可以在步骤 S513 和 S514 之前执行。

[0048] 如果这两个哈希码相同(步骤 S514 中的“是”)并且这两个元数据相同(步骤 S516 中的“是”),则将从正面图像 401 获得的文件图像 403 与从背面图像 402 获得的经处理的数据 411 进行比较(步骤 S518)。依赖于经处理的数据 411 包括的数据的类型,该比较步骤可以具有许多可替代的实现方案。首先,如果经处理的数据 411 包括原始图像的压缩版本,则该压缩数据被解压缩以生成文件图像,并且可以针对文件图像 403 执行逐个像素的图像比较。在该实施例中,步骤 S505 不是必需的。其次,如果经处理的数据 411 包括所提取的特征或者低分辨率图像,则将这些特征与经处理的数据 405 中的相应的特征比较。如果基于该比较,文件图像 403 和经处理的数据 411 彼此匹配(步骤 S519 中的“是”),则判断打印文件 400 是可信的(步骤 S520)。否则(步骤 S519 中的“否”),判断打印文件 400 是被更改的并且是不可信的(步骤 S521)。

[0049] 以上描述的文件认证方案具有许多优点。分级条形码戳记由于其结构上的冗余和分级的本质而耐受污染并且防篡改。此外,由于分级戳记是作为背景图案而呈现在文件的正面上,因此分级戳记不太可能被篡改。此外,哈希编码减少了信息量,这使得条形码戳记

元素能够以简单的方式被译码并且改进了分级条形码戳记的可靠性和鲁棒性。认证过程需要三级比较,这显著改进了认证方法的安全性。

[0050] 在可替代的实施例中,在文件为硬副本的形式期间,分级条形码戳记对于人(肉眼)是不可见的。在该情况中,通过使用淡色版(tint block)技术,可以将条形码戳记隐藏在文件的正面中。特别地,戳记的每个码块可以由不可见的分散的微点形成,从而在将硬副本文件扫描回数字形式时,条形码戳记可以被检测或显现。

[0051] 以上描述的文件认证方法可以通过软件或固件实现,该软件或固件存储在存储器中并且由诸如计算机、具有数据处理部分的打印机或扫描仪等的任何适当的数据处理装置执行。在这一点上,作为用于实现图3至5的过程的代码的计算机可执行软件可以被存储在由适当的数据处理装置的中央处理单元(CPU)或微处理单元(MPU)访问的计算机存储器中。打印和扫描步骤可以由任何打印机和扫描仪或者在单个设备中组合了打印部分和扫描部分的全能设备执行。这些设备和装置的结构是公知的并且在这里不做详细描述。

[0052] 可替代地,作为扫描仪的替换,可以在步骤S501和S502中使用数字相机或者其他成像设备。在这一点上,如本公开内容和权利要求中所广泛使用的术语“扫描的图像”指的是通过扫描或摄影或者其他适当的方法生成的数字图像。

[0053] 对于本领域的技术人员明显的是,在不偏离本发明的精神或范围的情况下,可以对本发明的更改检测方法和相关装置进行各种修改和变化。因此,本发明旨在涵盖落入所附权利要求及其等同物的范围内的修改和变化。

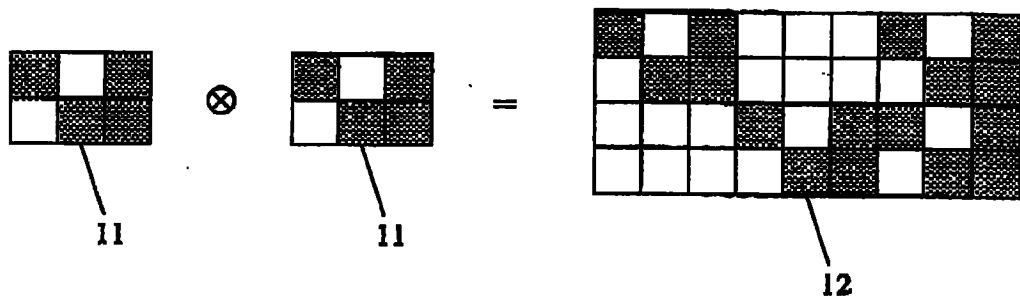


图 1

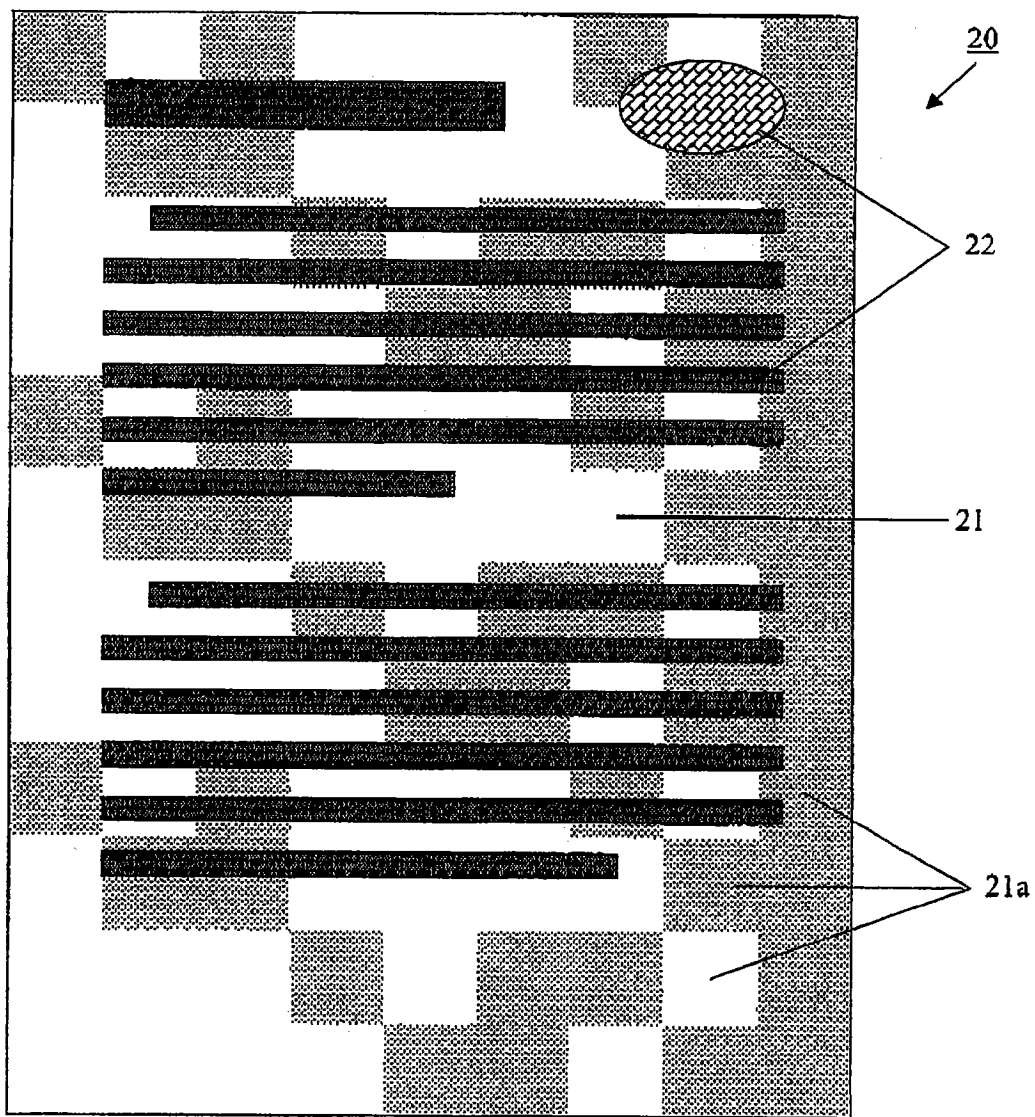


图 2

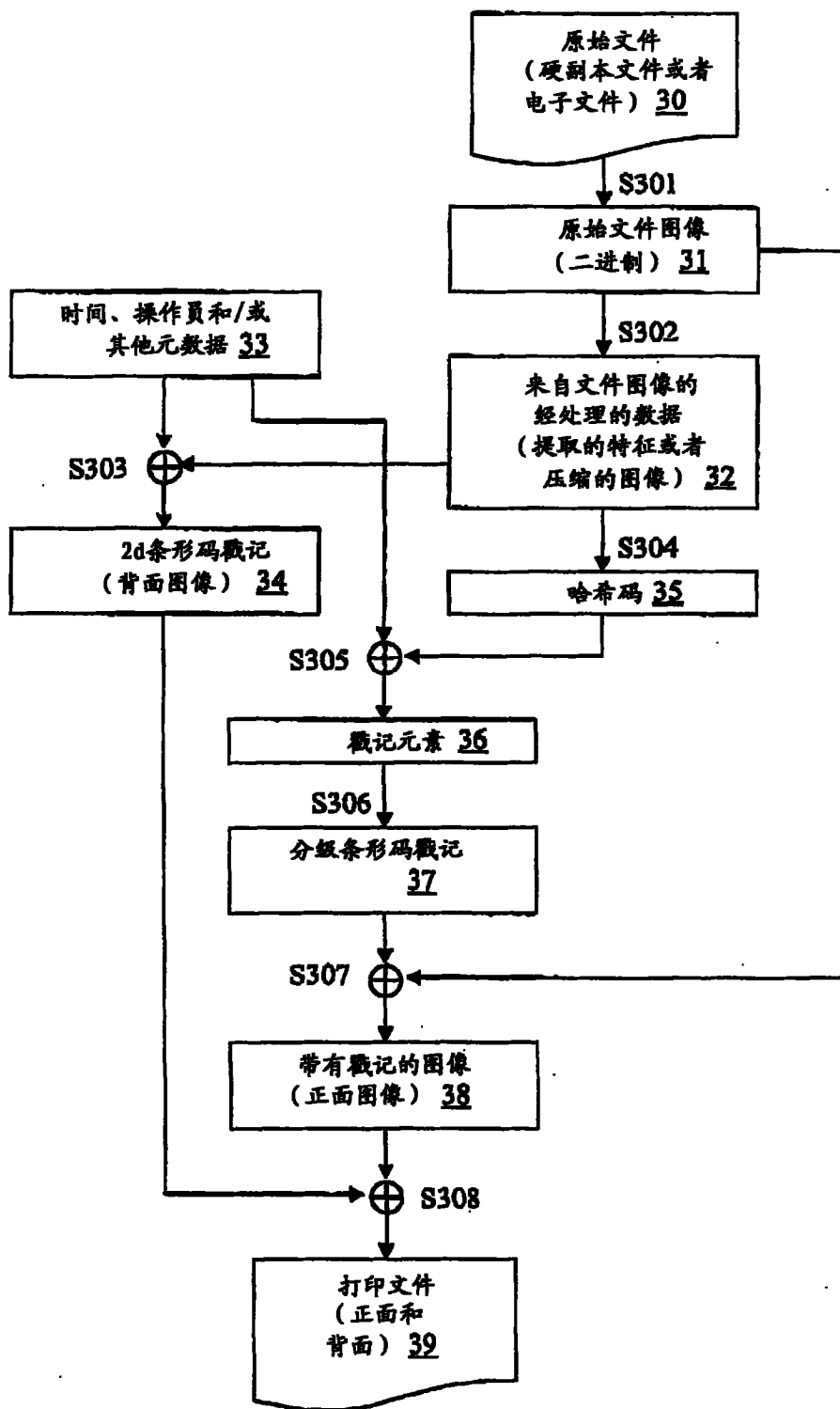


图 3

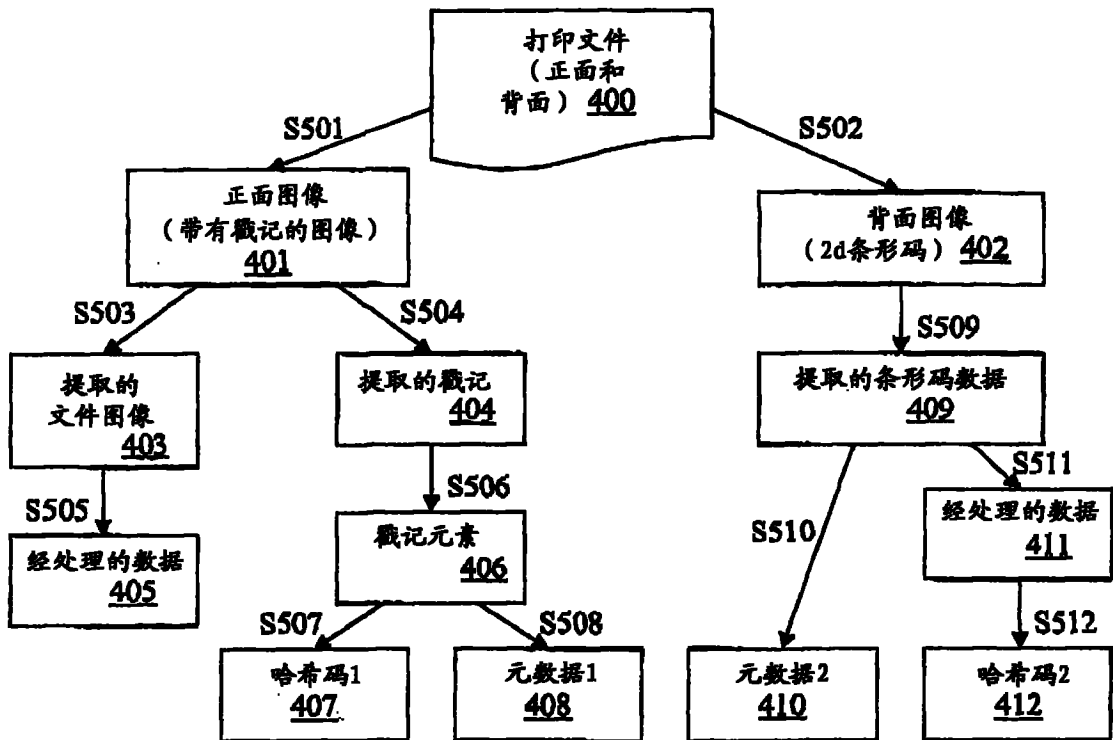


图 4

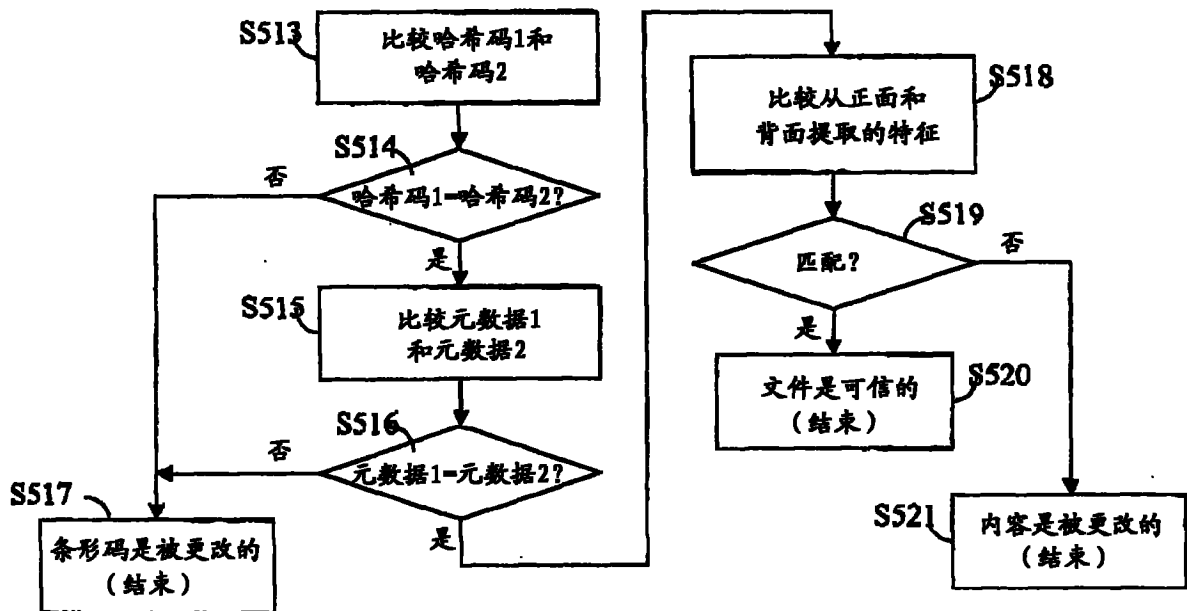


图 5