(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2006 年9 月28 日 (28.09.2006)

PCT

(10) 国际公布号
WO 2006/099788 A1

(51) 国际专利分类号:
G06T 1/00 (2006.01) H04N 1/387 (2006.01)

(21) 国际申请号: PCT/CN2006/000202

(22) 国际申请日: 2006 年2 月6 日 (06.02.2006)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200510055680.8
2005 年3 月23 日 (23.03.2005) CN

(71) 申请人 (对除美国外的所有指定国): **北京华旗数码影像技术研究院有限责任公司(HUAQI RESEARCH INSTITUTE OF IMAGE COMPUTING CO. LTD.)** [CN/CN]; 中国北京市海淀区北洼西里22号中海雅园丽华阁8A, Beijing 100089 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **田新(TIAN, Xin)** [CN/CN]; 中国北京市海淀区北洼西里22号中海雅园丽华阁8A, Beijing 100089 (CN)。 **刘曼(LIU, Man)** [CN/CN]; 中国北京市海淀区北洼西里22号中海雅园丽华阁8A, Beijing 100089 (CN)。 **杨祥辉(YANG, Xianghui)** [CN/CN]; 中国北京市海淀区北洼西里22号中海雅园丽华阁8A, Beijing 100089 (CN)。

(74) 代理人: **北京元中知识产权代理有限责任公司 (BEIJING YUANZHONG INTELLECTUAL PROPERTY AGENT LTD.)**; 中国北京市西城区北三环中路甲29号2号楼尊邸1103室, Beijing 100029 (CN)。

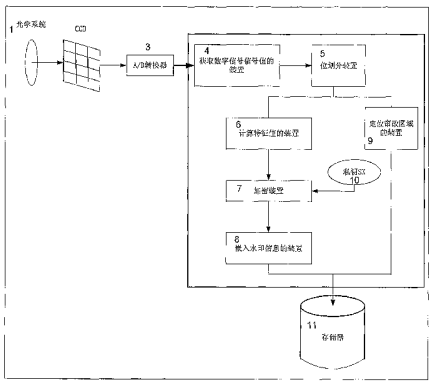
(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS,

[见续页]

(54) **Title:** THE METHOD OF DIGITAL WATERMARK AND THE CORRESPONDING DEVICE, AND DIGITAL CAMERA WHICH CAN APPEND WATERMARK

(54) **发明名称:** 数字图像水印的方法及相应装置和可添加水印的数码相机



1 OPTICAL SYSTEM
3 A/D CONVERTER
4 DIGITAL SIGNAL VALUE OBTAINING DEVICE
5 BIT DIVIDING DEVICE
6 EIGENVALUE CALCULATING DEVICE
7 ENCOPRTING DEVICE
8 WATERMARK EMBEDDING DEVICE
9 POSITION ALTERATION REGION INITIALIZING DEVICE
10 SECRET KEY
11 MEMORY

(57) **Abstract:** A digital camera with watermark appending device includes digital signal obtaining device, bit dividing device, position alteration region initializing device, eigenvalue calculating device, encrypting device, and watermark embedding device. The digital signal obtaining device can read out the value of the digital signal. The bit dividing device can divide the bits the data of each of the pixel points in recorded digital image into the bits of calculated image eigenvalue based on the bits, hidden the bits of the water, and locate the bits of alteration region. The position alteration initializing device can fully set the bits of the position alteration region to 0 or 1.The eigenvalue calculating device can calculate the eigenvalue of the digital signal. The encrypting device can encrypt the calculated eigenvalue. The watermark embedding device embeds the eigenvalue information to the digital signal.

[见续页]

WO 2006/099788 A1

IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(57) 摘要：

一种带添加水印装置的数码相机，包括获取数字信号的装置、位划分装置、初始化定位窜改区域的装置、计算特征值的装置、加密装置和水印嵌入装置。获取数字信号的装置可以读出数字信号的值。位划分装置可以将记录数字图像中各像素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位。初始化定位窜改区域的装置可以将定位窜改区域的位全部置 0 或置 1。计算特征值的装置可以算出数字信号的特征值。加密装置加密算出的特征值。水印嵌入装置向数字信号嵌入特征值信息。

数字图像水印的方法及相应装置和可添加水印的数码相机

【技术领域】

本发明涉及向数字图像中嵌入水印的方法和装置，以及验证数字图像的方法和装置和一种可以向所拍照片嵌入水印的数码相机，特别涉及一种可鉴别数字图像真实性的水印的添加、验证方法和装置及带添加水印装置的数码相机。

【背景技术】

由于逐步提高的图像质量和日益简化的桌面 PC 界面，数码照相机已经变得非常流行。数码照相机能够拍摄数字化的图像，从而允许你把它们通过互联网来传送或打印到彩色打印机上。时至今日，数码相机差不多已经成为我们生活中的必备品了。在数码技术日渐普及的今天，利用各种软件对数码照片进行修改、编辑已非难事，这给窜改数码照片所记录的信息带来了便利，尤其是对于一些想作为电子证据的保险、合同、票据等照片，它们的真实完整性就显得尤为重要。因此就引出了数码照片真实完整性认证的问题。我们解决这个问题的办法就是通过数码相机内置的照片保真装置来实现的。

数字水印技术可以有效防止数字图像被伪造。数字水印技术因目的不同有两个分支：一种是鲁棒水印，它用来保护作者的版权，在发生版权纠纷的时候用来提供法律依据；一种是脆弱水印（或半脆弱水印），它用来检测多媒体作品是否受到了恶意的窜改和损坏。对于鲁棒水印而言，其必须足够鲁棒，以至于在多媒体作品受到攻击和窜改后，仍然能够正确的被提取出来，兹以证明作者的版权。而脆弱水印的主要目的在于证明多媒体作品的真实性。现在多媒体照片不能作为法庭的证据，就是因为多媒体照片可以很容易的被各种软件（如 Photoshop）修改而不被发现；而医学图像中的任意一点变化都可能使医生对病情做出错误的判断。因此在这些场合，对多媒体产品的真实性认证比版权认证更加重要。

与数字水印和数码相机相关的背景技术可参阅以下几篇文献。

[1] GL.Friedman “The trustworthy digital camera restoring credibility to the photographic image” IEEE Trans, Consumer Electron, Vol. 39, PP.905-910, Nov. 1993

[2] S. Walton, Information authentication for a slippery new age[J], Dr. Dobbs Journal, 1995, 20(4):18-26

[3] 中国专利文献“向图像嵌入鉴定信息的系统及图像改变检测系统” 申请号：97121196.9，申请日：97.10.27

[4] Wong P W. *A public key watermark for image verification and authentication* [A]. In: Proc of the IEEE International Conference on Image Processing (ICIP'98) [C], Chicago, Illinois, USA, 1998,1:455~459

文献[1]中 Friedman 提出了一种基于数字签名的方法，用来确认数码相机照片的真实性，此方法是利用公开密钥体制，再通过相机中的私有密钥来生成图像的数字签名，作为另一文件保存，与图像一同发行。这样普通用户通过公开密钥，再结合图像文件及其数字签名文件，即可验证图像的真实性，但这种方法具有增加了存储空间、不便管理数字签名信息、不能探测失真情况的缺点。

文献[2]提出用 checksum（校验和）的方法计算图像的特征值。这样不能象使用哈希算法那样保证图像的真实性。因为使用校验和的方法，有可能图像变了，计算出的值却一样。

文献[3]中的专利把图像分成两个区域，从图像的一个区域计算散列值，然后把得到的散列值利用像素块编码方法嵌入到图像的另一个区域，再用区域组合单元把两个区域合并起来。这个方法最大的缺点就是不能定位出图像被窜改的区域。

文献[4]提出了一种用于图像认证的公开密钥水印方法。这种数字图像的水印算法是利用为图像分块来定位窜改的区域的，这种分块处理图像的方法如果使用在数码相机上，将大大降低数码相机的拍照速度，因此，用在数码相机上实用性并不理想。

此外，现有技术中已有多种成熟的计算图像特征值的算法。例如 SHA-1 算法，关于该算法的描述和 C 语言源代码在 internet rfcs3174 中有详细的描述（http://www.faqs.org/rfcs/rfc3174.html），这是一份最权威的文档。

【发明内容】

本发明“数字图像水印的添加、验证方法和装置及带添加水印装置的数码相机”的目的在于：公开一种在数字图像中添加、验证水印的方法和装置，以及一种带添加水印装置的数码相机，用这种数码相机拍出的照片，可以验证其真实完整性。当图片被编辑、修改、增删后，可以通过验证图片真实完整性的方法，得知照片已经被改动过了，从而实现了数码照片的保真，使得数码照片作为电子证据成为可能。

为了达到上述目的，本发明是这样进行的。

首先，第一个发明提供了一种在数字图像中添加水印的方法。该方法具有：获取表示数字图像每个象素的数据值；将记录数字图像中各像素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位的步骤，利用数字图像中计算图像特征值的位计算图

像的特征值的步骤；将定位窜改区域的位全部置 0（或置 1）即初始化的步骤；将计算出的特征值加密的步骤，以及利用脆弱数字水印技术在数字图像中隐藏加密后的特征值的步骤。

第二个发明提供了一种验证数字图像真实完整性的方法。该方法具有：将记录数字图像中各像素点的数据按位标识为计算图像特征值的位、隐藏水印的位和定位窜改区域的位的步骤，利用数字图像中计算图像特征值的位计算图像的特征值的步骤；从图像隐藏水印的位中提取隐藏的水印信息的步骤；解密提取出的信息的步骤；定位窜改区域的步骤；以及比对计算出的特征值和解密后的信息是否相等的步骤，如果相等，并且也没有定位出图像的窜改区域，说明图像是真实没有被窜改过的，否则说明照片的真实性没有保障，这个时候，我们还可以给出图像的窜改区域。

第三个发明提供了一种在数字图像中添加水印的装置。该装置具有：用于得到表示数字图像每个象素的数据值的装置；用于将记录数字图像中各像素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位的装置，利用数字图像中计算图像特征值的位计算图像的特征值的装置；将定位窜改区域的位全部置 0（或置 1）的装置即初始化定位窜改区域的装置；将计算出的特征值加密的装置，以及利用脆弱数字水印技术在数字图像中隐藏加密后的特征值的装置。

第四个发明提供了一种验证数字图像真实完整性的装置。该装置具有：用于将记录数字图像中各像素点的数据按位标识为计算图像特征值的位、隐藏水印的位和定位窜改区域的位的装置，利用数字图像中计算图像特征值的位计算图像的特征值的装置；从图像中提取隐藏的水印信息的装置；解密提取出的信息的装置；定位窜改区域的装置；以及比对计算出的特征值和解密后的信息是否相等的装置，如果相等，并且也没有定位出图像的窜改区域，说明图像是真实没有被窜改过的，否则说明照片的真实性没有保障，这个时候，我们还可以给出图像的窜改区域。

我们还设计了一种带添加水印装置的数码相机。这种数码相机将接收到的模拟信号转换为数字信号后，将记录数字图像中各像素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位，然后利用某种诸如 SHA-1、MD5、CRC16、CRC32 或 CRC-CCITT 的计算特征值的算法，计算出这个数字信号中用于计算图像特征值的位的唯一特征值，然后利用私钥加密计算出的特征值，再利用脆弱水印技术将加密后的特征值嵌入到数字信号隐藏水印的位中，然后将定位窜改区域的位全部置 0（或者置 1），再成像成无损格式的数码相片。当需要验证数码相片的真实完整性时，我们先从数码照片中还原出数字信号，将记录数字图像中各像素点的数据按位标识为计算图像特征值的位、隐藏水印的位和定位窜改区域的位，

然后通过相应的计算特征值的算法，计算出数字信号像素点中用于计算图像特征值的位的唯一特征值，再根据脆弱水印算法提取出隐藏在数字信号中隐藏水印的位的水印信息，然后利用公钥解密提取出的水印信息。之后检查定位图像窜改区域的位，如果定位图像窜改区域的位有的变为了 1（或者变为了 0），说明相应的区域被窜改了。最后比较计算出的哈希值和解密后的水印信息，如果相等，并且也没有定位出照片的窜改区域，说明照片是真实的，否则说明照片被窜改过了，这个时候，我们可以根据定位窜改区域位置上的值变为 1 的情况定位出照片被窜改的区域，从而完成了照片的认证。

本发明中带添加水印装置的数码相机包括数码相机中添加水印的系统和相应的照片验证方法。数码相机中添加水印的系统，包括：获取数字信号信号值的装置、位划分装置、初始化定位窜改区域的装置、计算特征值的装置、加密装置和水印嵌入装置。照片验证的过程，包括数字信号的读取、识别相应的位、通过相应的计算特征值的算法，得到数字信号的唯一特征值、从数字信号中利用相应的脆弱数字水印技术提取出隐藏的水印信息、解密提取出的水印信息、定位出窜改区域、比较计算出的特征值和解密后的水印信息，如果二者相等，并且也没有定位出照片的窜改区域，说明照片是真实没有被窜改过的，否则照片的真实完整性没有保障，这个时候，我们可以利用相应的方法定位出照片窜改的区域。现详细说明如下：

本发明中数码相机内添加水印的系统，包括：

获取数字信号信号值的装置，用于读取出数字信号的值，此数字信号是由光学图像反应到数码相机

内的模拟信号转换成的数字信号。

位划分装置，用于将记录数字图像中各像素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位。

初始化定位窜改区域的装置，用于将定位窜改区域的位全部置 0 或置 1。

计算特征值的装置，用于利用数字图像中计算图像特征值的位将输入的数字信号的唯一特征值计算出来。

加密装置，利用私钥加密计算出的特征值。

水印嵌入装置，利用脆弱的数字水印技术将加密后的特征值嵌入到数字信号隐藏水印的位中。

照片验证的方法，可以看成与水印添加装置所进行的操作相反的步骤：

第一步为数字信号的读取，先从无损格式的照片中还原出数字信号。

第二步将记录数字图像中各像素点的数据按位标识为计算图像特征值的位、隐藏水印的位和定位窜改区域的位。

第三步对计算图像特征值的位中的数据运用相应的计算特征值的算法，得到数字信号的唯一特征值。

第四步为从数字信号隐藏水印的位中利用相应的脆弱数字水印技术提取出隐藏的水印信息。

第五步为利用公钥解密提取出的水印信息。

第六步为定位照片的窜改区域，找出定位窜改区域位置上值为 1（或 0）的区域。

第七步为比较得到的哈希值和解密后的水印信息，如果二者相等，并且也没有定位出照片的窜改区域，说明照片是真实没有被窜改过的，否则说明照片被窜改了，这个时候，我们可以给出照片窜改的区域。

注意，在计算数字信号的特征值时，我们只使用计算图像特征值的位中的数据参与运算。这是为了保证计算的特征值与嵌入的特征值之间是匹配的。如果隐藏水印的位和定位窜改区域的位上的数据都用诸如黑色或白色等颜色信号填充的话，那么这样的数据就可以整个地输入计算特征值的算法。这样，即使嵌入数据之后也能保证正确的验证结果。

另外，本实施例所述的数码相机，还可以在拍出的照片中隐藏诸如相机的 ID，拍摄的日期，及由 GPS 测量的位置等等信息。需要说明的是，我们获取到数码相机的数字信号后，首先要向准备计算特征值的数字信号中嵌入这些信息，然后再进行计算才可。否则将影响照片验证的结果。

而且，为了对付通过打开相机而非法访问保存在数码相机内部的信息，我们可以使用蜂窝式电话中使用的诸如防篡改模块。如果进行这种非法访问，则认为密钥 SK 被盗，并对于由密钥 SK 加密的图像数据，一概认为照片的真实完整性无法保证。这就防止了由第三者非法行为引起的损坏。

我们在验证照片的时候，还可以在 Internet 上建立认证中心，任何人都可以在这里验证图片的真实完整性，公证验证的结果。

此外，虽然上述实施例是对于数码相机说明的，但本发明不限于此，而是可以适用于诸

如数字视频等数字系统。

本发明“数字图像水印的添加、验证方法和装置及带添加水印装置的数码相机”的优点如下：

1．由于本发明采用了适当的计算特征值的算法，使得计算出的特征值具有唯一性。我们把得到

的数字信号输入计算特征值的算法，然后计算出它的唯一的特征值，最后成像时又以无损的形式保存数码照片，这都保证了照片即使一个点的改动都能够正确地检测出来。这为数码照片真实完整性认证的正确性提供了很好的保证。

2．由于本发明的系统内置于数码相机，故使用起来非常方便，并且在照片成像前已经加上了水

印信息，从最开始就保证了数码照片的真实性。

3．本发明把数字信号中各像素点的信息按位分为三部分，一部分用做生成数字信号的唯一特征

值，一部分用来隐藏水印信息，一部分用来定位窜改图像的区域，这就解决了水印的嵌入会改变数字信号，从而改变计算出的特征值的问题。当图像被改动后，它还原出的数字信号中，要么是计算出的特征值变化了，要么是隐藏的水印信息变化了，要么是定位窜改图像的区域变化了。我们比较计算出的特征值和提取出的水印信息，如果它们相同，并且定位窜改图像的区域也没有变化，那么说明图像是真实没有被窜改的，反之就说明图像被改动过了，同时我们还能给出图像窜改的区域。

4．本发明在嵌入特征值时，根据人类的视觉特性，成功的将数据信息隐藏在图像视觉不敏感

的区域，保证嵌入水印前后的图像视觉差别最小。

5．利用公开密钥算法，提高了算法的安全性，使得即使水印算法公开的话，旁人也无法模拟水印的嵌入，因为他们没有嵌入水印的私钥。而公钥又使得任何人都可以验证照片的真实完整性，使得更符合实际的应用。

6．我们知道，数码相机的微处理器速度十分慢，和 PC 上的 CPU 的处理速度无法相提并论。我们没有使用分块的方法处理图像，使得处理速度大大提高，从而使得应用在数码相机中成为可能。

【附图说明】

图 1 是本发明数码相机内的装置图

图 2 是本发明验证照片的方法的流程图

图 3 是用带添加水印装置的数码相机拍出的照片

图 4 是图 3 的验证结果

图 5 是图 3 被窜改后的照片

图 6 是图 5 的验证结果及定位出的窜改区域

【具体实施方式】

下面结合附图对本发明作进一步的详细描述，并请参阅附图。图 1 中数码相机内的装置可以分为 6 个部分。图 2 验证照片的操作可以分成 7 个步骤。

带添加水印装置的数码相机，包括：获取数字信号信号值的装置，这个装置用于读取出数字信号的

值，此数字信号是由光学图像反应到数码相机内的模拟信号转换成的数字信号；位划分装置，用于将记录数字图像中各像素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位；初始化定位窜改区域的装置，这个装置将定位图像窜改区域的位上的数据全部置成某个固定值，诸如全 0 或全 1，以便于在验证时定位出图像的被窜改区域；计算特征值的装置，这个装置用于根据数字图像中计算图像特征值的位将输入的数字信号的唯一特征值计算出来；加密装置，这个装置利用私钥加密计算出的特征值；水印嵌入装置，这个装置利用脆弱数字水印技术将加密后的特征值嵌入到数字信号隐藏水印的位中。

验证数码照片的操作的步骤如下：第一步为数字信号的读取，先从无损格式的照片中还原出数字信号。第二步将记录数字图像中各像素点的数据按位标识为计算图像特征值的位、隐藏水印的位和定位窜改区域的位；第三步根据数字图像中计算图像特征值的位的数据运行相应的计算特征值的算法，得到数字信号的唯一特征值。第四步为从数字信号隐藏水印的位中利用相应的脆弱数字水印技术提取出隐藏的水印信息。第五步为利用公钥解密提取出的水印信息。第六步为定位图像的被窜改区域，记录下和原来在定位窜改区域相应位上赋的值不同的值的位置，得到图像被窜改的区域。第七步为比较得到的特征值和解密后的水印信息，如果二者相等，并且也没有定位出照片的窜改区域，那么说明照片是真实没有被窜改过的，否则说明照片被窜改了，同时我们可以给出照片被窜改过的区域。

具体装置和流程，参见附表 1 和附表 2。

值得一提的是，我们在所举的例子中，处理的数字信号是 8－4－4 格式的 YUV 数据。YUV 是一种颜色编码方法，8－4－4 格式的 YUV 数据，其中“8－4－4”指的是 YUV 数据的排列方式。当然实际应用中并非仅限于此，一般来说，只要是图像的数字信号即可，比如 RGB 格式的图像数据，我们可以使用 B 分量的最低位定位图像的窜改区域，把 G 分量的最低位隐藏图像的特征值，其余的数据用作特征值的计算等等。另外，在此具体实施例中，我们使用 Y 值的最低位定位窜改区域，Y 值的次低位嵌入加密的特征值，其余的数据全部用来计算图像的特征值。实际应用中也并非局限于此。理论上讲，只要计算特征值的数据、嵌入加密特征值的数据和定位窜改区域的数据覆盖了全部像素的所有数据位，并且定位窜改区域的位要涉及到全部像素即可，并且要保证有足够的空间隐藏加密的特征值。比如，我们使用 Y 值的最低位嵌入加密的特征值，使用 Y 值的次低位定位窜改的图像区域或者组合某几位去隐藏加密的特征值等等。又或者，我们可以使用 U 值的最低位嵌入加密的特征值，使用 V 值的最低位定位窜改的图像区域，其余的数据去计算特征值。再举一个例子，我们还可以使用一部分 Y 值的最低位嵌入加密的特征值，另一部分 Y 值的最低位定位窜改的图像区域，其余的数据去计算特征值。当然，我们更可以只使用一部分象素数据去隐藏加密的特征值和定位窜改的图像区域。比如，我们可以使用一部分象素的次低位嵌入加密的特征值，最低位定位图像的窜改区域，这部分象素的其他位和另一部分象素的所有位的数据都用来计算特征值等等。划分数据的方法有很多，但是特别注意的是，划分数据的方法一定要保证图像的质量，不能造成可感知的改变。比如我们选取在 Y 值的最低位和次低位上修改数据，都是基于这个考虑，尽量的不要使图像质量有较明显的变化。

这里之所以利用了每个像素的每个位，是为了让随意一个像素的变化都能检测出来。但如果用户知道可能的改动都不止一个像素，或者他只想检测出一个区域的变化，那么就可以相应地减少像素和位数的改变率。比如就不需要将每个像素都设置定位窜改区域的位，也不需要三个部分的组合覆盖所有像素的每个位。

表 1 数码相机内添加水印的系统

	装置	作用
1	获取数字信号信号值的装置	用于读取出数字信号的值，此数字信号是由光学图像反应到数码相机内的模拟信号转换成的数字信号
2	位划分装置	用于将记录数字图像中各像素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位
3	初始化定位窜改区域的装置	用于将定位窜改区域的位全部置 0 或置 1
4	计算特征值的装置	用于根据计算图像特征值的位中的数据将输入的数字信号的唯一特征值计算出来
5	加密装置	利用私钥加密计算出的唯一特征值
6	水印嵌入装置	利用脆弱的数字水印技术将计算出的特征值嵌入到数字信号隐藏水印的位中

表 2 验证数码照片的方法的步骤

步骤	操作	作用
1	从无损格式的照片中还原出数字信号	数字信号的获取
2	将记录数字图像中各像素点的数据按位识别为计算图像特征值的位、隐藏水印的位和定位窜改区域的位	识别带有不同性质的信息的位
2	根据计算图像特征值的位中的数据运行相应的计算特征值的算法，得到数字信号的唯一特征值	计算出数字信号的特征值
3	从数字信号隐藏水印的位中利用相应的脆弱数字水印技术提取出隐藏的水印信息	提取出隐藏的水印信息
4	利用公钥解密提取出的水印信息	得到解密后的水印信息
5	判断定位窜改区域位上的数据有哪些有变化	得到图像被窜改的区域
6	比较得到的特征值和水印信息	得出验证结论。如果二者相等，并且没有找到图像窜改的区域，那么说明照片是真实没有被窜改过的，否则说明照片被窜改了，同时可以给出图像窜改的区域

图 3 是用具有本发明的装置的数码相机拍出的照片，这拍的是一起恶性交通事故的现场，我们用它来作例子。拍照时，在数码相机内部，我们先利用 CCD 或 CMOS 将光学图像转换成模拟信号，然后由 A/D 转换器把得到的模拟信号转换为数字信号。我们这个实施例中，接收到的数字信号是 8—4—4 格式的 YUV 数据流。然后，我们把 YUV 数据流中每个 Y 值的 LSB 位（最低有效位）都置 0，用做定位窜改图像区域的位。之后，我们把 YUV 数据流中 Y 值次低位上的数据也全部置 0。需要说明的是，就象前面已经提到的，我们划分数据的方法并非一种；并且初始值也不一定是 0，1 也可以。然后，我们通过 SHA-1 算法，计算出此时 YUV 数据流的 160 位哈希值，以 16 进制表示，为“E6C2BD995EDCF316887EFD24EC5492A8C2991C53”。然后我们利用私钥加密这 160 位哈希值，之后我们将加密后的哈希值顺序且重复的嵌入每个 Y 值的次低位内，如果当前要嵌入的哈希值中的位为“1”，那么我们就把当前要嵌入的 Y 值的次低位置 1；如果当前要嵌入的哈希值中的位为“0”，那么我们就不进行任何操作，直至最后一个 Y 值。这样，YUV 数据流已经经过了水印添加装置的处理。最后，我们通过照片成像装

置，把 8－4－4 的 YUV 数据流转换成 2－1－1 的 YUV 数据流，然后保存成 TIF 格式的数字图像。

图 4 是图 3 的数码照片的验证结果。验证的时候，从 TIF 格式的数码照片中读出 2－1－1 格式的 YUV 数据流，然后把 2－1－1 格式的 YUV 数据流转换成 8－4－4 格式的 YUV 数据流，之后我们把 8－4－4 格式的 YUV 数据流拷贝到一个数组中，然后我们把这个数组中每个表示 Y 值数据的 LSB 位和次低位都置 0，然后通过 SHA-1 算法，得到这个数组的 160 位哈希值，以 16 进制表示，为“E6C2BD995EDCF316887EFD24EC5492A8C2991C53”。然后我们读取 8－4－4 格式的 YUV 数据流中每个 Y 值的次低位的值，组成一个序列，此序列再用公钥解密，得到解密后的哈希值，用 16 进制表示，为“E6C2BD995EDCF316887EFD24EC5492A8C2991C53”。然后，我们再查看 YUV 数据流中每个 Y 值的 LSB 的值，发现这些值全为 0。我们可以看出，计算出的 YUV 数据流的 160 位哈希值和解密后的水印信息是相同的，并且定位窜改区域也没有找到图像有改动的区域，这说明照片是没有被窜改过的，这时候返回的验证对话框提示我们“图像完整无损！”

图 5 是一个窜改图 3 所示的照片的实例。在实例中，我们把图 3 所示的照片中的车牌号码由“沪 D 00000”改为“沪 D 10000”。这种对于电子版照片的改动是非常简便易行、容易实现的，但是对于拍照这种文件或者拍的照片想作为电子证据，那么它的真实性是我们迫切需要知道的问题。

图 6 是图 5 所示的窜改后的数码照片的验证结果。验证的时候，从 TIF 格式的数码照片中读出 2－1－1 格式的 YUV 数据流，然后把 2－1－1 格式的 YUV 数据流转换成 8－4－4 格式的 YUV 数据流，之后我们把 8－4－4 格式的 YUV 数据流拷贝到一个数组中，然后我们把这个数组中每个表示 Y 值数据的 LSB 位和次低位都置 0，然后通过 SHA-1 算法，得到这个数组的 160 位哈希值，以 16 进制表示，为“E5442CC3B4281EAAAAFBAD00BECAB7C957226E26”。然后我们读取 8－4－4 格式的 YUV 数据流中每个 Y 值的次低位的值，组成一个序列，此序列是没有规律的值。我们无需再用公钥解密，就可以知道，计算出的 YUV 数据流的 160 位哈希值和水印信息不可能相同，这样照片的真实完整性就没有保证，这时候返回的验证对话框提示我们“图像已被窜改!”，这个时候，由于数据值已改变，所以通过连接数据值已改变的点，就可以得到图像的窜改区域，如图中黑框所示。

至此，本发明中已经描述了数字图像水印的添加、验证方法和装置及带添加水印装置的数码相机。对本领域普通技术人员来说，在不脱离本发明所附权利要求所限定的精神和范围的情况下，可以作出各种改变和变形。

权 利 要 求

1. 一种在数字图像中添加水印的方法，其特征在于：方法包括以下步骤：

获取图像数据，得到表示数字图像每个象素的数据的数据值；

划分数据位，根据使用目的的不同对数据位进行划分；

数字图像特征值的计算，利用特征值计算算法计算数字图像的唯一特征值；

将定位窜改区域的位全部置 0（或置 1）；

加密计算出的特征值；

利用脆弱数字水印技术在数字图像中隐藏加密后的特征值。

2. 如权利要求 1 所述的方法，其特征在于：所述的划分数据位的步骤将记录数字图像中各像素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位。

3. 一种数字图像真实完整性的验证方法，其特征在于：

通过相应的计算特征值的算法，得到无损格式数字图像的唯一特征值；

再从数字图像中利用相应的脆弱数字水印技术提取出隐藏的水印信息，之后将提取出的水印信息解密；

然后定位图像的窜改区域；

最后比较计算出的特征值和解密后的水印信息，如果二者相等，并且也没有定位出图像的窜改区域，那么说明图像是真实没有被窜改过的，否则图像的真实完整性没有保障，这个时候，我们可以定位出图像的窜改区域。

4. 如权利要求 3 所述的方法，其特征在于：所述得到无损格式数字图像的唯一特征值的步骤包括：

第一步将记录数字图像中各像素点的数据按位进行划分；

第二步利用数字图像中计算图像特征值的位计算图像的特征值。

5. 如权利要求 4 所述的方法，其特征在于：所述划分步骤中，将记录数字图像中各象素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位。

6. 如权利要求 3 所述的方法，其特征在于：所述对所提取的水印信息解密的步骤包括：

第一步，从数字图像隐藏水印的位提取隐藏的水印信息；

第二步，根据所提取的隐藏的水印信息对所提取的水印信息进行解密。

7. 一种在数字图像中添加水印的装置，包括：

获取数据的装置，用于得到表示数字图像每个象素的数据的数据值；

位划分装置，用于将记录数字图像中各像素点的数据按位进行划分；

特征值产生装置，用来计算数字图像的特征值；

初始化定位窜改区域的装置，用来设置定位窜改区域的值；

加密装置，用来加密计算出的特征值；

隐藏装置，利用脆弱数字水印技术在数字图像中隐藏加密后的特征值。

8. 如权利要求 7 所述的装置，其特征在于所述的位划分装置可以将记录数字图像中各象素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位。

9. 一种数字图像真实完整性的验证装置，包括：

位划分装置，用于将记录数字图像中各像素点的数据按位进行划分；

特征值产生装置，用于计算数字图像的特征值；

提取水印装置，用于从图像中提取隐藏的水印信息；

解密装置，用于解密提取出的信息；

定位窜改区域的装置，用于给出图像窜改的区域；

比对装置，比对计算出的特征值和解密后的信息是否相等，如果相等，并且也没有定位出图像的窜改区域，说明图像是真实没有被窜改过的，否则说明图像的真实性没有保障，这个时候，我们还可以给出图像的窜改区域。

10. 如权利要求 9 所述的装置，其特征在于所述的位划分装置可以将记录数字图像中各象素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位。

11. 一种带添加水印装置的数码相机包括：

获取数字信号信号值的装置，用于读取出数字信号的值；

位划分装置，用于将记录数字图像中各像素点的数据按位划分；

初始化定位窜改区域的装置，用于设置定位窜改区域的值的装置；

计算特征值的装置，用于计算出数字信号的唯一特征值；

加密装置，用于加密计算出的特征值；

水印嵌入装置，根据计算出的特征值向数字信号中嵌入脆弱水印信息。

12. 如权利要求 11 所述的数码相机，其特征在于所述的获取数字信号信号值的装置中的“数字信号”是由光学图像反映到数码相机内的模拟信号转换成的数字信号。

13. 如权利要求 11 所述的数码相机，其特征在于所述的位划分装置可以将记录数字图像中各像素点的数据按位划分为计算图像特征值的位、隐藏水印的位和定位窜改区域的位。

14. 如权利要求 11 所述的数码相机，其特征在于所述的水印嵌入装置利用脆弱的数字水印技术将加密后的特征值嵌入到数字信号中。

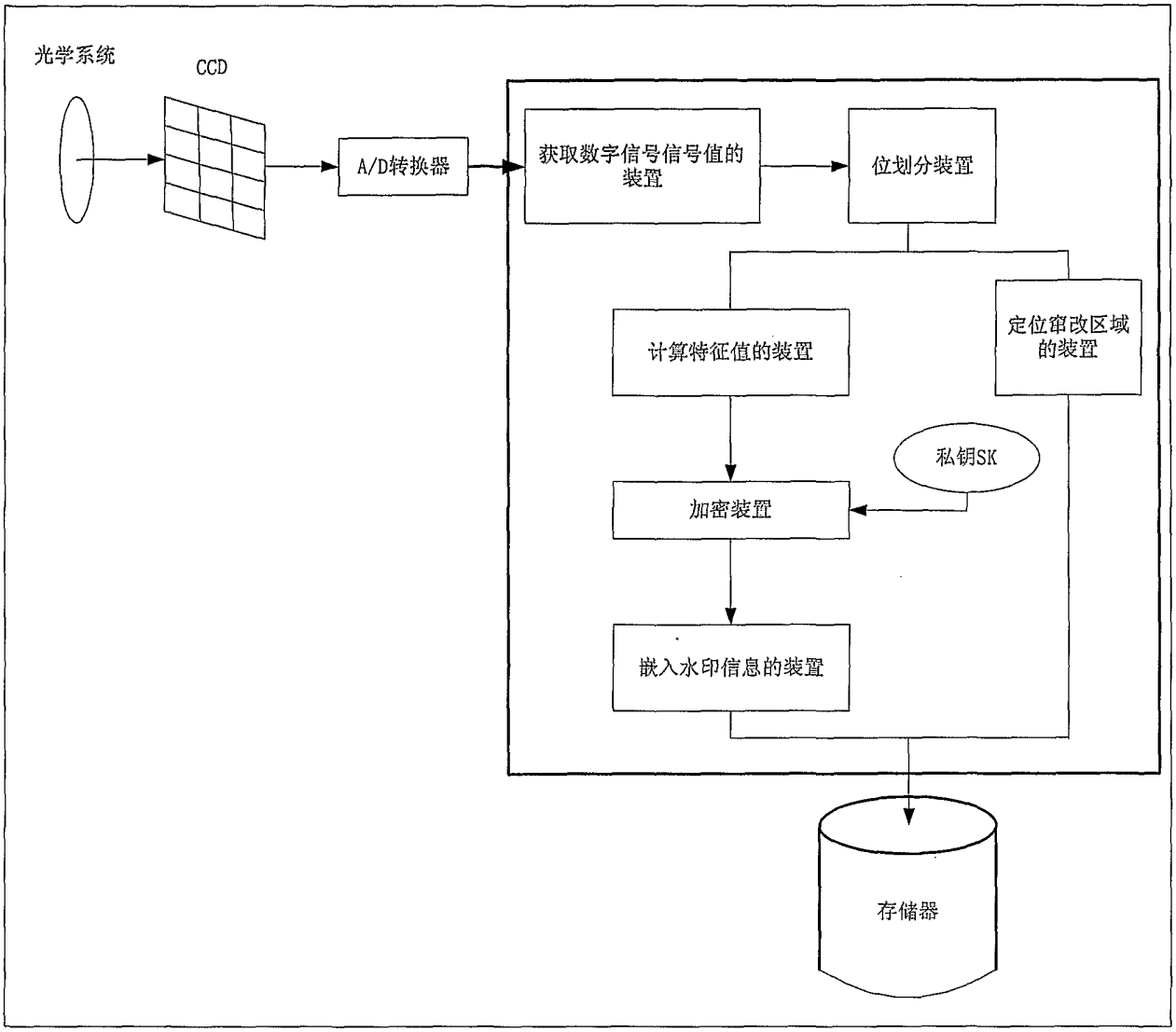

光学系统
CCD
A/D转换器
获取数字信号信号值的装置
位划分装置
计算特征值的装置
定位窜改区域的装置
私钥SK
加密装置
嵌入水印信息的装置
存储器

图 1

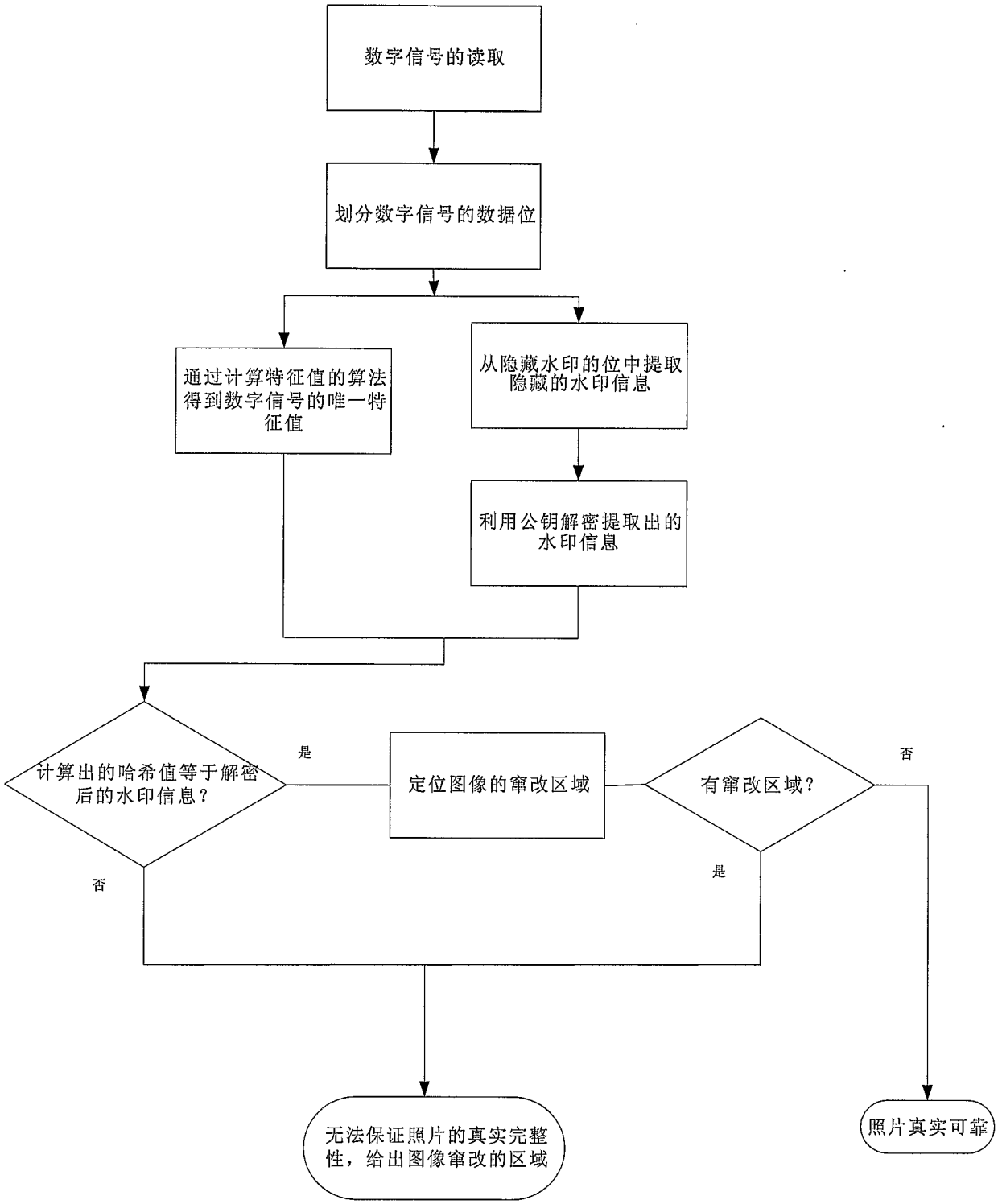

数字信号的读取
划分数字信号的数据位
通过计算特征值的算法得到数字信号的唯一特征值
从隐藏水印的位中提取隐藏的水印信息
利用公钥解密提取出的水印信息
计算出的哈希值等于解密后的水印信息？
是
否
定位图像的窜改区域
有窜改区域？
否
是
无法保证照片的真实完整性，给出图像窜改的区域
照片真实可靠

图 2



图 3

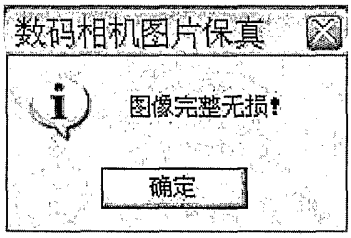


图 4



图 5



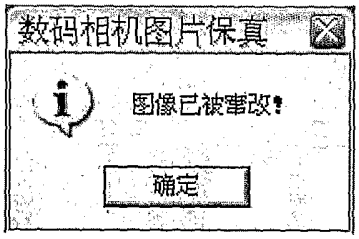


图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2006/000202

A. CLASSIFICATION OF SUBJECT MATTER

IPC8: See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06T, H04N, G06K, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, PAJ:
digital, watermark, image, eigenvalue, bit?, authentication, camera, encode or encrypt or encipher,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 1091329C （国际商业机器公司）18.Sep.1996 (18. 09.1996), whole	1-14
A	US 6725372B1 （VERIZON LAB INC）20. Apr. 2004 (20. 04.2004), whole	1-14
A	JP 2001-268339A（HITACHI LTD）28. Sep. 2001 (28. 09. 2001), whole	1-14
A	CN 1450495A （佳能株式会社）22. Oct. 2003 (22. 10.2003), whole	1-14
A	US 6285775B1 （UNIV PRINCETON）04. Sep. 2001 (04. 09.2001), whole	1-14
A	WO 01/80169A1 （DIGIMARC CORP）25. Oct. 2001 (25. 10.2001), whole	1-14

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09. May. 2006 (09. 05. 2006)	29 · 6月 2006 (29 · 06 · 2006)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer LIU, Jingfeng Telephone No. 86-10-62085712

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CN2006/000202

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1091329C	18-09-2002	EP0845758 A2	03-06-1998
		JP10164549 A	19-06-1998
		CA2222346 A	28-05-1998
		TW342477 A	11-10-1998
		KR98041902 A	17-08-1998
		US6005936 A	21-12-1999
		SG78279 A1	20-02-2001
		KR264635 B1	01-09-2000
		CN1184294 A	10-06-1998
		DE69719922E	24-04-2003
US 6725372B1	20-04-2004	None	
JP 2001-68339A	28-09-2001	None	
CN 1450495A	22-10-2003	JP2004241938 A	26-08-2004
		EP1349370 A2	01-10-2003
		JP2003298830 A	17-10-2003
		US2003210803 A1	13-11-2003
US 6285775B1	22-10-2003	None	
WO 01/80169A1	25-10-2001	US2002009208 A1	24-01-2002
		AU0155445 A	30-10-2001
		US2003138128 A1	24-07-2003

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2006/000202

CLASSIFICATION OF SUBJECT MATTER

IPC8: G06T 1/00 (2006.01) i
H04N 1/387 (2006.01) n

国际检索报告

国际申请号
PCT/CN2006/000202

A. 主题的分类

IPC8: 参见附加页

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06T, H04N, G06K, H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT, WPI, EPODOC, PAJ:

数字，水印，图像，图象，特征值，加密，解密，鉴定，鉴别，位，相机;

digital, watermark, image, eigenvalue, bit?, authentication, camera, encode or encrypt or encipher, decode or decrypt or decipher;

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 1091329C （国际商业机器公司）18. 9 月 1996 (18. 09.1996) 全文	1-14
A	US 6725372B1 （VERIZON LAB INC）20. 4 月 2004 (20. 04.2004) 全文	1-14
A	JP 2001-268339A（HITACHI LTD）28. 9 月 2001 (28. 09. 2001) 全文	1-14
A	CN 1450495A （佳能株式会社）22. 10 月 2003 (22. 10.2003) 全文	1-14
A	US 6285775B1 （UNIV PRINCETON）04. 9 月 2001 (04. 09.2001) 全文	1-14
A	WO 01/80169A1 （DIGIMARC CORP）25. 10 月 2001 (25. 10.2001) 全文	1-14

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
25. 5 月 2006 (25. 05. 2006)	29 · 6月 2006 (29 · 06 · 2006)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 电话号码：(86-10)62085712

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2006/000202

索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 1091329C	2002-09-18	EP0845758 A2	1998-06-03
		JP10164549 A	1998-06-19
		CA2222346 A	1998-05-28
		TW342477 A	1998-10-11
		KR98041902 A	1998-08-17
		US6005936 A	1999-12-21
		SG78279 A1	2001-02-20
		KR264635 B1	2000-09-01
		CN1184294 A	1998-06-10
		DE69719922E	2003-04-24
US 6725372B1	2004-04-20	无	
JP 2001-68339A	2001-09-28	无	
CN 1450495A	2003-10-22	JP2004241938 A	2004-08-26
		EP1349370 A2	2003-10-01
		JP2003298830 A	2003-10-17
		US2003210803 A1	2003-11-13
US 6285775B1	2003-10-22	无	
WO 01/80169A1	2001-10-25	US2002009208 A1	2002-01-24
		AU0155445 A	2001-10-30
		US2003138128 A1	2003-07-24

国际检索报告

国际申请号
PCT/CN2006/000202

主题的分类

IPC8：G06T 1/00 (2006.01) i
H04N 1/387 (2006.01) n