(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114330621 A
(43)申请公布日 2022.04.12

(21)申请号 202111391274.4

(22)申请日 2021.11.23

(71)申请人 深圳市祯源科技有限公司
地址 518041 广东省深圳市福田区沙头街道天安社区泰然四路6号天安数码时代大厦主楼2013

(72)发明人 黄楚雄

(74)专利代理机构 广州市华学知识产权代理有限公司 44245
代理人 于波

(51)Int.Cl.
G06K 19/06(2006.01)
G06T 1/00(2006.01)

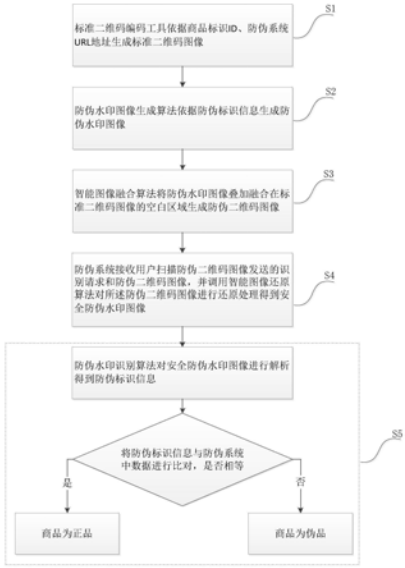
权利要求书2页 说明书8页 附图4页

(54)发明名称

一种基于标识信息的二维码防伪方法、装置、存储介质

(57)摘要

本发明涉及一种基于标识信息的二维码防伪方法、装置、存储介质，属于防伪技术和图像处理技术领域，二维码防伪方法包括：依据商品标识ID、防伪系统URL地址生成标准二维码图像；依据防伪标识信息生成防伪水印图像；将防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像；防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像，并对防伪二维码图像进行还原处理得到安全防伪水印图像；对安全防伪水印图像进行解析得到防伪标识信息，并将防伪标识信息与防伪系统中数据进行比对验证；本发明实现了标准二维码图像与安全防伪水印图像叠加融合生成防伪二维码图像，两者合为一体，外观上与标准二维码一致，具有更好的整体性。



CN 114330621 A

1.一种基于标识信息的二维码防伪方法,其特征在于,包括如下步骤:

S1、标准二维码编码工具依据商品标识ID、防伪系统URL地址生成标准二维码图像;

S2、防伪水印图像生成算法依据防伪标识信息生成防伪水印图像;

S3、智能图像融合算法将所述防伪水印图像叠加融合在所述标准二维码图像的空白区域生成防伪二维码图像;

S4、防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像,并调用智能图像还原算法对所述防伪二维码图像进行还原处理,得到安全防伪水印图像;

S5、防伪水印识别算法对所述安全防伪水印图像进行解析,得到所述防伪标识信息,并将所述防伪标识信息与防伪系统中数据进行比对,如果相等则商品为正品,否则商品为伪品。

2.根据权利要求1所述的二维码防伪方法,其特征在于,所述S3步骤包括:

S31、依据所述标准二维码图像的空白区域对所述防伪水印图像进行可逆无损安全变换,转换成安全防伪水印图像,其中所述安全防伪水印图像的面积与所述标准二维码图像的空白区域面积相等;

S32、智能图像融合算法将所述安全防伪水印图像叠加融合在所述标准二维码图像的空白区域生成所述防伪二维码图像。

3.根据权利要求2所述的二维码防伪方法,其特征在于,所述S31步骤中进行所述可逆无损安全变换时,向所述安全防伪水印图像中增加易失性特征以提高抗复制性。

4.根据权利要求1所述的二维码防伪方法,其特征在于,所述S4步骤包括:

S41、防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像,并对所述二维码图像进行预处理,包括畸变消除处理、角度矫正处理;

S42、调用智能图像还原算法对预处理后的所述防伪二维码图像进行还原处理,得到安全防伪水印图像。

5.根据权利要求3所述的二维码防伪方法,其特征在于,所述S5步骤包括:

S51、设定易失性特征损失度容许阈值,所述防伪水印识别算法对所述安全防伪水印图像进行计算得到易失性特征损失度,并进行解析得到所述防伪标识信息;

S52、当所述防伪标识信息与防伪系统中数据比对相等,且所述易失性特征损失度小于所述易失性特征损失度容许阈值时,则商品为正品,否则商品为伪品。

6.一种二维码防伪装置,其特征在于,包括:

二维码图像生成单元,用于标准二维码编码工具依据商品标识ID、防伪系统URL地址生成标准二维码图像;

防伪水印图像生成单元,用于防伪水印图像生成算法依据防伪标识信息生成防伪水印图像;

图像融合单元,用于智能图像融合算法将所述防伪水印图像叠加融合在所述标准二维码图像的空白区域生成防伪二维码图像;

图像接收还原单元,用于防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像,并调用智能图像还原算法对所述防伪二维码图像进行还原处理,得到安全防伪水印图像;

图像解析比对单元,用于防伪水印识别算法对所述安全防伪水印图像进行解析,得到

防伪标识信息，并将所述防伪标识信息与防伪系统中数据进行比对，如果相等则商品为正品，否则商品为伪品。

7.根据权利要求6所述的二维码防伪装置，其特征在于，所述图像融合单元包括：

图像转换模块，用于依据所述标准二维码图像的空白区域对所述防伪水印图像进行可逆无损安全变换，转换成安全防伪水印图像，其中所述安全防伪水印图像的面积与所述标准二维码图像的空白区域面积相等；

图像叠加融合模块，用于智能图像融合算法将所述安全防伪水印图像叠加融合在所述标准二维码图像的空白区域生成所述防伪二维码图像。

8.根据权利要求7所述的二维码防伪装置，其特征在于，所述图像转换模块包括：

易失性特征增加部件，用于在所述图像转换模块中进行所述可逆无损安全变换时，向所述安全防伪水印图像中增加易失性特征以提高抗复制性。

9.根据权利要求8所述的二维码防伪装置，其特征在于，所述图像解析比对单元包括图像解析模块、易失性特征计算模块、比对模块；

所述图像解析模块，用于所述防伪水印识别算法对所述安全防伪水印图像进行解析获得所述防伪标识信息；

所述易失性特征计算模块，用于设定易失性特征损失度容许阈值，所述防伪水印识别算法对所述安全防伪水印图像进行计算得到易失性特征损失度；

所述比对模块，用于当所述防伪标识信息与防伪系统中数据比对相等，且所述易失性特征损失度小于所述易失性特征损失度容许阈值时，则商品为正品，否则商品为伪品。

10.一种存储介质，所述存储介质上存储有指令，其特征在于，所述指令被处理器执行时实现权利要求1-5中任一项所述的二维码防伪方法。

一种基于标识信息的二维码防伪方法、装置、存储介质

技术领域

[0001] 本发明涉及防伪技术和图像处理技术领域，特别涉及一种基于标识信息的二维码防伪方法、装置、存储介质。

背景技术

[0002] 随着移动互联网的发展，在许多应用场景中使用二维码技术，目前二维码技术已应用于商品防伪溯源，现有技术通常采用如下技术方案满足商品防伪溯源需求：一、在普通二维码中编码一个加密字串，在该二维码旁边加印一个遮盖处理的验证码，客户进行商品防伪溯源操作时，必须先购买商品后擦除遮盖层获取验证码，使用智能手机扫该二维码解密出加密字串，进行验证码和加密字串的比对实现商品防伪溯源，此技术方案无法满足客户先验真再购买的需求，应用场景受到诸多限制；二、在普通二维码中编码一个标识ID，在该二维码旁边加印一个随机特征图案作为验证图，同时在系统中存储该验证图，进行商品防伪溯源操作时，使用智能手机扫该二维码识别出对应的系统存档验证图，对随机特征图案进行拍照获取验证图，进行系统存档验证图和验证图的比对实现商品防伪溯源，此技术方案需使用特殊印刷工艺和材料制作验证图，同时在系统中存储海量的对应存档验证图，成本较高，操作繁琐。因此需研发一种操作简单、制作成本低、用户体验好的二维码防伪技术。

发明内容

[0003] 为解决上述技术问题，本发明提供一种基于标识信息的二维码防伪方法、装置、存储介质。

[0004] 本发明采用以下技术方案来实现：

[0005] 一方面，本发明实施例提供一种基于标识信息的二维码防伪方法，包括如下步骤：

[0006] S1、标准二维码编码工具依据商品标识ID、防伪系统URL地址生成标准二维码图像；

[0007] S2、防伪水印图像生成算法依据防伪标识信息生成防伪水印图像；

[0008] S3、智能图像融合算法将防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像；

[0009] S4、防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像，并调用智能图像还原算法对防伪二维码图像进行还原处理，得到安全防伪水印图像；

[0010] S5、防伪水印识别算法对安全防伪水印图像进行解析，得到防伪标识信息，并将防伪标识信息与防伪系统中数据进行比对，如果相等则商品为正品，否则商品为伪品。

[0011] 在一些实施例中，S3步骤包括：

[0012] S31、依据所述标准二维码图像的空白区域对所述防伪水印图像进行可逆无损安全变换，转换成安全防伪水印图像，其中所述安全防伪水印图像的面积与所述标准二维码图像的空白区域面积相等；

[0013] S32、智能图像融合算法将安全防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像。

[0014] 在一些实施例中，S31步骤中进行可逆无损安全变换时，向安全防伪水印图像中增加易失性特征以提高抗复制性。

[0015] 在一些实施例中，S4步骤包括：

[0016] S41、防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像，并对二维码图像进行预处理，包括畸变消除处理、角度矫正处理；

[0017] S42、调用智能图像还原算法对预处理后的防伪二维码图像进行还原处理，得到安全防伪水印图像。

[0018] 在一些实施例中，S5步骤包括：

[0019] S51、设定易失性特征损失度容许阈值，防伪水印识别算法对安全防伪水印图像进行计算得到易失性特征损失度，并进行解析得到防伪标识信息；

[0020] S52、当防伪标识信息与防伪系统中数据比对相等，且易失性特征损失度小于易失性特征损失度容许阈值时，则商品为正品，否则商品为伪品。

[0021] 另一方面，本发明实施例提供了一种二维码防伪装置，包括：

[0022] 二维码图像生成单元，用于标准二维码编码工具依据商品标识ID、防伪系统URL地址生成标准二维码图像；

[0023] 防伪水印图像生成单元，用于防伪水印图像生成算法依据防伪标识信息生成防伪水印图像；

[0024] 图像融合单元，用于智能图像融合算法将防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像；

[0025] 图像接收还原单元，用于防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像，并调用智能图像还原算法对防伪二维码图像进行还原处理，得到安全防伪水印图像；

[0026] 图像解析比对单元，用于防伪水印识别算法对安全防伪水印图像进行解析，得到防伪标识信息，并将防伪标识信息与防伪系统中数据进行比对，如果相等则商品为正品，否则商品为伪品。

[0027] 在一些实施例中，图像融合单元包括：

[0028] 图像转换模块，用于依据标准二维码图像的空白区域对防伪水印图像进行可逆无损安全变换，转换成安全防伪水印图像，其中安全防伪水印图像的面积与标准二维码图像的空白区域面积相等；

[0029] 图像叠加融合模块，用于智能图像融合算法将安全防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像。

[0030] 在一些实施例中，图像转换模块包括：

[0031] 易失性特征增加部件，用于在图像转换模块中进行可逆无损安全变换时，向安全防伪水印图像中增加易失性特征以提高抗复制性。

[0032] 在一些实施例中，图像解析比对单元包括图像解析模块、易失性特征计算模块、比对模块；

[0033] 图像解析模块，用于防伪水印识别算法对安全防伪水印图像进行解析获得防伪标

识信息；

[0034] 易失性特征计算模块，用于设定易失性特征损失度容许阈值，防伪水印识别算法对安全防伪水印图像进行计算得到易失性特征损失度；

[0035] 比对模块，用于当防伪标识信息与防伪系统中数据比对相等，且所述易失性特征损失度小于易失性特征损失度容许阈值时，则商品为正品，否则商品为伪品。

[0036] 另一方面，本发明实施例提供了一种存储介质，存储介质上存储有指令，该指令被处理器执行时实现上述的基于标识信息的二维码防伪方法。

[0037] 与现有技术相比，本发明取得的技术效果包括：

[0038] 1.本发明将标准二维码图像的空白区域与防伪水印图像生成算法生成的安全防伪水印图像叠加融合生成防伪二维码图像，两者合为一体，外观上与标准二维码一致，具有更好的整体性。

[0039] 2.本发明安全防伪水印图像与标准二维码合二为一，无需对用户进行引导教育，用户只需一步扫码，即可通过防伪系统实现对商品的验真。

[0040] 3.本发明无需对防伪标识物做遮盖处理，满足了用户先验真再购买的需求，应用场景无限制。

[0041] 4.本发明无需特殊印刷工艺和材料，依托防伪水印识别算法实现对商品的验真，服务器无需存储大量图像，大幅降低了成本。

附图说明

[0042] 图1为本发明基于标识信息的二维码防伪方法流程图；

[0043] 图2为本发明基于标识信息的二维码防伪方法含易失性特征损失度计算的流程图；

[0044] 图3为本发明二维码防伪装置的示意图；

[0045] 图4为本发明二维码防伪装置含易失性特征计算模块的示意图。

具体实施方式

[0046] 为了使本领域技术人员更好地理解本发明的方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然所描述的实施例仅仅是本发明的一部分实施例，而不是全部的实施例。基于本发明的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的其他方案，都应当属于本发明的保护范围。

[0047] 实施例1

[0048] 图1示出了本发明基于标识信息的二维码防伪方法流程图，该基于标识信息的二维码防伪方法包括如下步骤：

[0049] S1、标准二维码编码工具依据商品标识ID、防伪系统URL地址生成标准二维码图像。

[0050] 首先启动标准二维码编码工具，设置需要生成的商品标识ID、防伪系统URL地址，生成标准二维码图像。

[0051] S2、防伪水印图像生成算法依据防伪标识信息生成防伪水印图像。

[0052] 防伪水印图像生成算法获取标准二维码图像大小，生成一个灰度图像，优选地灰

度图像尺寸与标准二维码图像一致，该灰度级次不影响正常标准二维码的识别。使用图像水印技术向灰度图像中嵌入与商品标识ID相关联的防伪标识信息，生成防伪水印图像。

[0053] S3、智能图像融合算法将防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像。

[0054] S31、依据标准二维码图像的空白区域对防伪水印图像进行可逆无损安全变换，转换成安全防伪水印图像，其中安全防伪水印图像的面积与标准二维码图像的空白区域面积相等。

[0055] 首先读取标准二维码图像的空白区域相关信息，如空白区域的总面积，再依据标准二维码图像的空白区域相关信息，对防伪水印图像进行可逆无损安全变换，优选地压缩加密技术，生成与标准二维码的空白区域总面积相等的安全防伪水印图像。

[0056] S32、智能图像融合算法将安全防伪水印图像叠加融合在标准二维码图像的空白区域生成所述防伪二维码图像。

[0057] 首先智能图像融合算法在防伪系统中存储10种自定义的一维数组读取规则，在此只叙述其中一种规则，其他规则不再赘述，该规则如下：

[0058] $$a(i)=\begin{cases} i=\dfrac{n-1}{2}\ n\text{ 为奇数},n\geq 1 \\ i=L-\dfrac{n}{2}\quad n\text{ 为偶数},n\geq 2 \end{cases}$$

[0059] 其中a(i)为每次读取的数组元素，i为每次读取数组元素的下标值，n为第几次读取数组元素值，每读取一个数组元素n自动加一，L为一维数组元素总个数。

[0060] 然后智能图像融合算法利用随机方法，随机选择一种一维数组读取规则，并将其存储在相应的防伪系统数据库中，为智能图像还原算法提供还原规则。

[0061] 智能图像融合算法将防伪水印图像转换成一维数组序列，读取标准二维码图像的空白区域每个像素的坐标值，依据上述一维数组读取规则依次将相应元素叠加融合到标准二维码的空白区域处，其中空白区域的选取规则，可依据空白区域每个像素的坐标值从上到下，从左到右依次叠加融合，还可选择从下到上，从右到左的方式，或者其他方式就不再赘述。智能图像融合算法依据上述方法将防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像。

[0062] S4、防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像，并调用智能图像还原算法对防伪二维码图像进行还原处理，得到安全防伪水印图像。

[0063] 用户扫描防伪二维码图像访问防伪系统并发出防伪二维图像识别请求，同步将防伪二维码图像发送给防伪系统，防伪系统进行相应的响应，接收用户扫描防伪二维码图像发送的识别请求，并接收扫描的防伪二维码图像。

[0064] S41、对防伪二维码图像进行预处理，包括畸变消除处理、角度矫正处理。

[0065] 由于每个用户扫描防伪二维码图像的技术水平参差不齐，扫描发送的防伪二维码图像会出现多种因素影响防伪标识信息的识别，影响防伪二维码图像验真的准确性，优选地对接收的防伪二维码图像进行预处理，包括畸变消除处理，角度矫正处理，以降低图像质量因素对验真结果的影响。

[0066] S42、调用智能图像还原算法对预处理后的防伪二维码图像进行还原处理，得到安

全防伪水印图像。

[0067] 防伪系统识别出标准二维码图像的商品标识ID,从防伪数据库中获取智能图像还原算法的还原规则,依此对预处理后的防伪二维码图像进行还原处理,得到一维数组序列,再转换成安全防伪水印图像。

[0068] S5、防伪水印识别算法对安全防伪水印图像进行解析,得到防伪标识信息,并将防伪标识信息与防伪系统数据库中数据进行比对,如果相等则商品为正品,否则商品为伪品。

[0069] 首先防伪水印识别算法用解压解密技术对安全防伪水印图像进行解压还原解密生成防伪水印图像,再使用图像水印识别技术从防伪水印图像中解析出防伪标识信息。

[0070] 防伪系统将防伪标识信息与对应防伪系统数据库中商品防伪信息数据进行比对,如果两者相等,响应用户商品为正品,否则提醒用户此商品为伪品。

[0071] 本实施例利用图像水印技术将防伪标识信息嵌入灰度图像中生成防伪水印图像,并使用压缩加密技术将防伪水印图像进行压缩加密生成安全防伪水印图像,进一步地提高了防伪二维码的安全性和防伪能力,再使用智能图像融合算法将该安全防伪水印图像叠加融合在标准二维码的空白区域处生成防伪二维码,以此实现了安全防伪水印图像与标准二维码图像的有机统一。防伪二维码即不影响标准二维码的识别,又增加了可识别,防伪造复制,外观上与普通二维码一致,具有更好的整体性。

[0072] 用户对商品进行验真,只需与扫描普通标准二维码一样,一步扫描防伪二维码图像发送验真请求并传送防伪二维码图像,防伪系统对防伪二维码图像进行解析生成防伪标识信息,并将该防伪标识信息与防伪系统数据库中数据进行比对即可判断商品真伪,而无需在防伪系统数据库中存储图像,只需存储文字信息即可,极大地减少了防伪系统的存储空间,节约了防伪系统的使用成本。

[0073] 实施例2

[0074] 本实施例与实施例1不同之处为:在S2步骤中将灰度图像分成N块区域、N>＝2,优选地N＝8,使用图像水印技术在每块区域都嵌入与商品标识ID相关联的防伪标识信息。

[0075] 在S31步骤中对防伪水印图像按照N块区域分别进行可逆无损安全变换,转换成安全防伪水印图像,并在每块区域中加入易失性特征,用以设置防复制安全级别,提高防伪二维码图像的抗复制性。

[0076] 本实施例在实施例1的基础上,增加易失性特征,提高了防伪二维码的整体抗复制性,并设置了防复制安全级别,可根据实际需求设置防伪二维码的安全级别。

[0077] 实施例3

[0078] 本实施例在实施例2基础上增加了易失性特征损失度计算用以提高抗复制性,并以此可设置防复制安全级别,与实施例2实质性不同之处,如图2所示:将步骤S5做相应的改变,将改变后的步骤S5记作步骤S5'。步骤S5'在步骤S5基础上增加设定易失性特征损失度容许阈值,并使用防伪水印识别算法对安全防伪水印图像进行易失性特征损失度计算,如:安全防伪水印图像有N块区域,计算现存易失性特征有m个,此时易失性特征损失度等于(N-m)/N。在步骤S5'中还增加有易失性特征损失度判断,即当防伪标识信息与防伪系统数据库中数据进行比对相等时,再判断易失性特征损失度是否小于易失性特征损失度容许阈值,如果为是,则商品为正品,否则商品为伪品。还可依据易失性特征损失度容许阈值设定不同的防复制安全级别,以满足不同市场不同商品防伪需求。

[0079] 本实施例通过增加易失性特征损失度计算用以提高抗复制性，设置防复制安全级别，提高防伪二维码防伪水平，进一步地提高了二维码防伪方法的安全性、准确性、抗攻击性能力。

[0080] 实施例4

[0081] 图3示出了本发明二维码防伪装置的示意图，该二维码防伪装置包括：

[0082] 二维码图像生成单元10，用于标准二维码编码工具依据商品标识ID、防伪系统URL地址生成标准二维码图像。

[0083] 二维码图像生成单元10先设置商品标识ID、防伪系统URL地址，再调用标准二维码编程工具生成标准二维码图像。

[0084] 防伪水印图像生成单元20，用于防伪水印图像生成算法依据防伪标识信息生成防伪水印图像。

[0085] 防伪水印图像生成单元20获取标准二维码图像大小，再调用防伪水印图像生成算法生成一个灰度图像，优选地灰度图像尺寸与标准二维码图像一致，该灰度级次不影响正常标准二维码的识别。使用图像水印技术向灰度图像中嵌入与商品标识ID相关联的防伪标识信息，生成防伪水印图像。

[0086] 图像融合单元30，用于智能图像融合算法将防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像；图像融合单元30包括以下模块：

[0087] 图像转换模块301，用于依据标准二维码图像的空白区域对防伪水印图像进行可逆无损安全变换，转换成安全防伪水印图像，其中安全防伪水印图像的面积与标准二维码图像的空白区域面积相等。

[0088] 首先读取标准二维码图像的空白区域的总面积，再依据此面积对防伪水印图像进行可逆无损安全变换，优选地压缩加密技术，生成与标准二维码的空白区域总面积相等的安全防伪水印图像。

[0089] 图像叠加融合模块302，用于智能图像融合算法将标准二维码图像的空白区域与安全防伪水印图像叠加融合生成防伪二维码图像。

[0090] 首先智能图像融合算法在防伪系统中存储10种自定义的一维数组读取规则，在此只叙述其中一种规则，其他规则不再赘述，该规则如下：

[0091] $$a(i)=\begin{cases} i=\dfrac{n-1}{2}n \text{ 为奇数}, n\geq 1 \\ i=L-\dfrac{n}{2} \quad n \text{ 为偶数}, n\geq 2 \end{cases}$$

[0092] 其中a(i)为每次读取的数组元素，i为每次读取数组元素的下标值，n为第几次读取数组元素值，每读取一个数组元素n自动加一，L为一维数组元素总个数。

[0093] 然后智能图像融合算法利用随机方法，随机选择一种一维数组读取规则，并将其存储在相应的防伪系统数据库中，为智能图像还原算法提供还原规则。

[0094] 智能图像融合算法将防伪水印图像转换成一维数组序列，读取标准二维码图像的空白区域每个像素的坐标值，依据上述一维数组读取规则依次将相应元素叠加融合到标准二维码的空白区域处，其中空白区域的选取规则，可依据空白区域每个像素的坐标值从上到下，从左到右依次叠加融合，还可选择从下到上，从右到左的方式，或者其他方式就不再

赘述。智能图像融合算法依据上述方法将防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像。

[0095] 图像接收还原单元40，用于防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像，并调用智能图像还原算法对防伪二维码图像进行还原处理，得到安全防伪水印图像。

[0096] 用户扫描防伪二维码图像访问防伪系统并发出防伪二维图像识别请求，同步将防伪二维码图像发送给防伪系统，防伪系统进行相应的响应，接收用户扫描防伪二维码图像发送的识别请求，并接收扫描的防伪二维码图像。

[0097] 对防伪二维码图像进行预处理，包括畸变消除处理、角度矫正处理。

[0098] 由于每个用户扫描防伪二维码图像的技术水平参差不齐，扫描发送的防伪二维码图像会出现多种因素影响防伪标识信息的识别，影响防伪二维码图像验真的准确性，优选地对接收的防伪二维码图像进行预处理，包括畸变消除处理，角度矫正处理，以降低图像质量因素对验真结果的影响。

[0099] 调用智能图像还原算法对预处理后的防伪二维码图像进行还原处理，得到安全防伪水印图像。

[0100] 防伪系统识别出标准二维码图像的商品标识ID，从防伪数据库中获取智能图像还原算法的还原规则，依此对预处理后的防伪二维码图像进行还原处理，得到一维数组序列，再转换成安全防伪水印图像。

[0101] 图像解析比对单元50，用于防伪水印识别算法对所述安全防伪水印图像进行解析，得到防伪标识信息，并将防伪标识信息与防伪系统中数据进行比对，如果相等则商品为正品，否则商品为伪品。

[0102] 首先防伪水印识别算法用解压解密技术对安全防伪水印图像进行解压还原解密生成防伪水印图像，再使用图像水印识别技术从防伪水印图像中解析出防伪标识信息。

[0103] 防伪系统将防伪标识信息与对应防伪系统数据库中商品防伪信息数据进行比对，如果两者相等，响应用户商品为正品，否则提醒用户此商品为伪品。

[0104] 实施例5

[0105] 图4示出了本发明二维码防伪装置含易失性特征计算模块的示意图。在实施例4的基础上，在图像转换模块301中增加易失性特征增加部件3011，用于在图像转换单元30中进行可逆无损安全变换时，向安全防伪水印图像中增加易失性特征用以提高抗复制性。

[0106] 本实施例还将图像解析比对单元50分成图像解析模块501、易失性特征计算模块502、比对模块503；

[0107] 图像解析模块501，用于防伪水印识别算法对安全防伪水印图像进行解析获得所述防伪标识信息；

[0108] 易失性特征计算模块502，用于设定易失性特征损失度容许阈值，并调用防伪水印识别算法对安全防伪水印图像进行易失性特征损失度计算；

[0109] 比对模块503，用于增加如下比对功能：如果防伪标识信息与防伪系统数据库中数据进行比对相等且易失性特征损失度小于易失性特征损失度容许阈值时，则商品为正品，否则商品为伪品。

[0110] 实施例6

[0111] 基于上述实施例，本实施例中，提供了一种存储介质，其上存储有指令，指令被处理器执行时实现上述任意方法实施例中的基于标识信息的二维码防伪方法。

[0112] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有程序代码的可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的程序产品的形式。

[0113] 本发明是参照根据本发明实施例的方法、设备(系统)的流程图和/或示意图来描述的。应理解可由程序指令实现流程图和/或示意图中的每一流程和/或示意图、以及流程图和/或示意图中的流程和/或方框的结合。可提供这些程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程中指定的功能的装置。

[0114] 这些程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的可读存储器中，使得存储在该可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程中指定的功能。

[0115] 这些程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程中指定的功能的步骤。

[0116] 上述实施例为本发明较佳的实施方式，但本发明的实施方式并不受上述实施例的限制，其他的任何未背离本发明的精神实质与原理下所作的改变、修饰、替代、组合、简化，均应为等效的置换方式，都包含在本发明的保护范围之内。

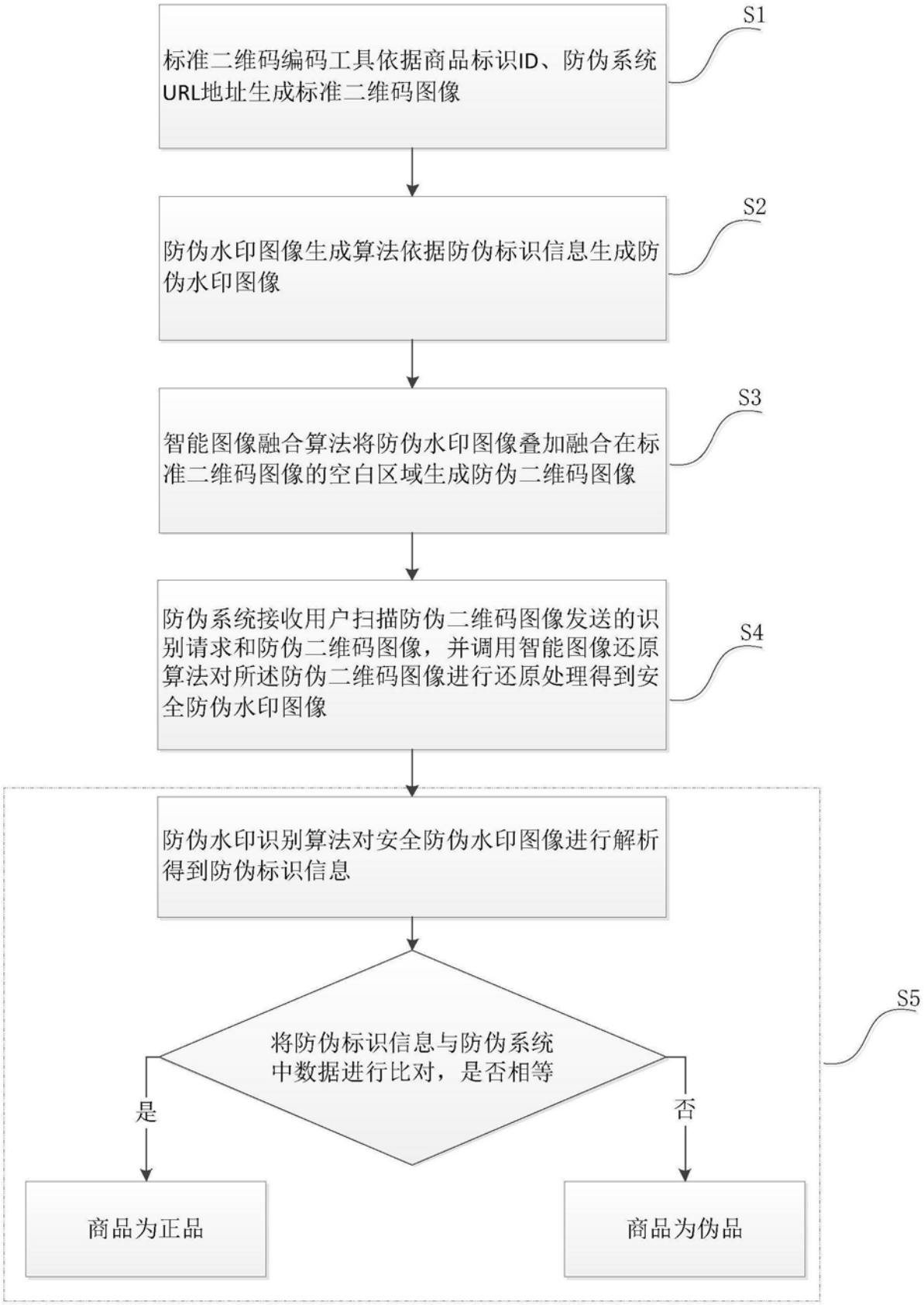

S1
标准二维码编码工具依据商品标识ID、防伪系统URL地址生成标准二维码图像
S2
防伪水印图像生成算法依据防伪标识信息生成防伪水印图像
S3
智能图像融合算法将防伪水印图像叠加融合在标准二维码图像的空白区域生成防伪二维码图像
S4
防伪系统接收用户扫描防伪二维码图像发送的识别请求和防伪二维码图像，并调用智能图像还原算法对所述防伪二维码图像进行还原处理得到安全防伪水印图像
防伪水印识别算法对安全防伪水印图像进行解析得到防伪标识信息
S5
将防伪标识信息与防伪系统中数据进行比对，是否相等
是
否
商品为正品
商品为伪品

图1

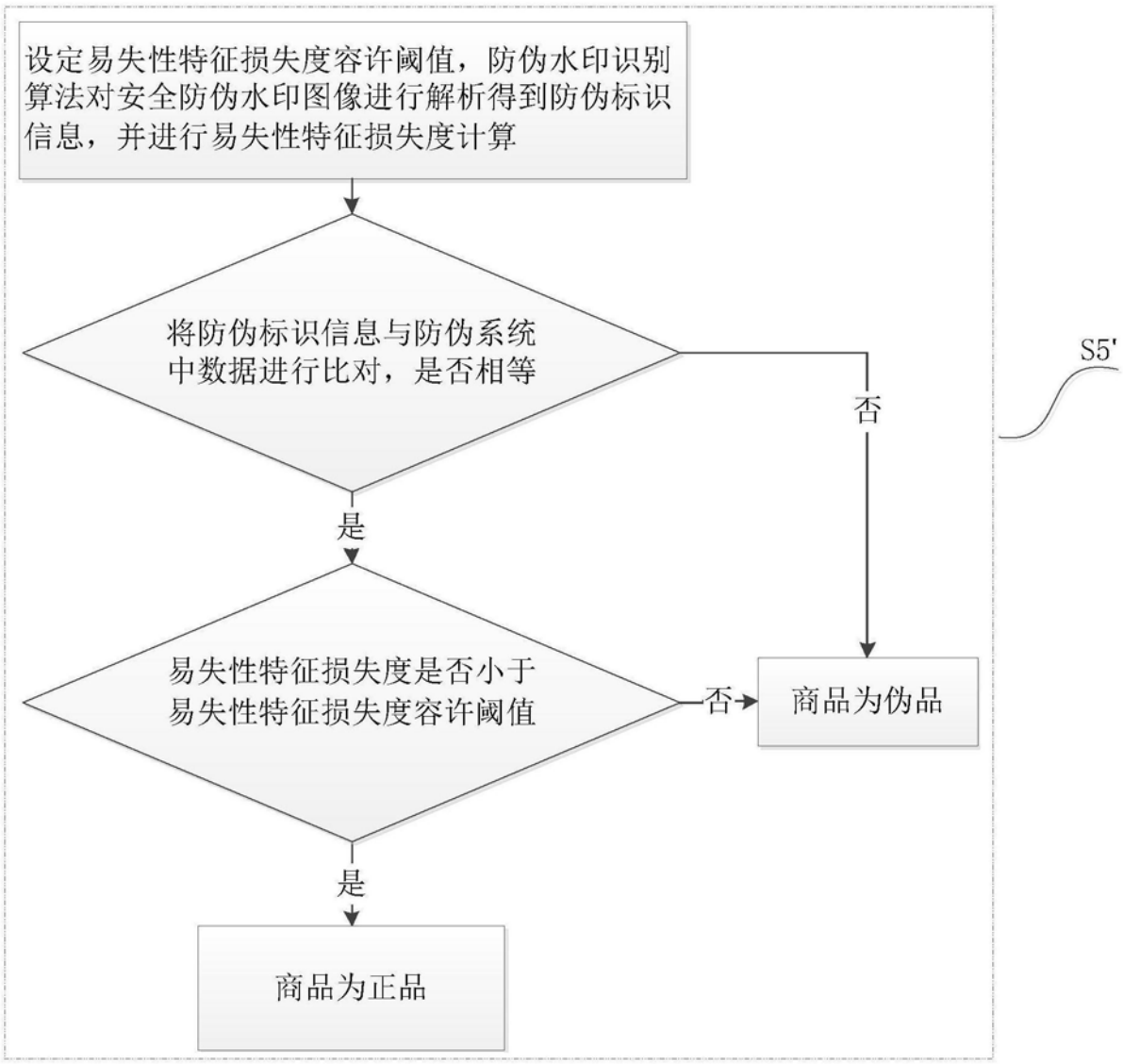

设定易失性特征损失度容许阈值，防伪水印识别算法对安全防伪水印图像进行解析得到防伪标识信息，并进行易失性特征损失度计算
将防伪标识信息与防伪系统中数据进行比对，是否相等
否
S5'
是
易失性特征损失度是否小于易失性特征损失度容许阈值
否
商品为伪品
是
商品为正品

图2

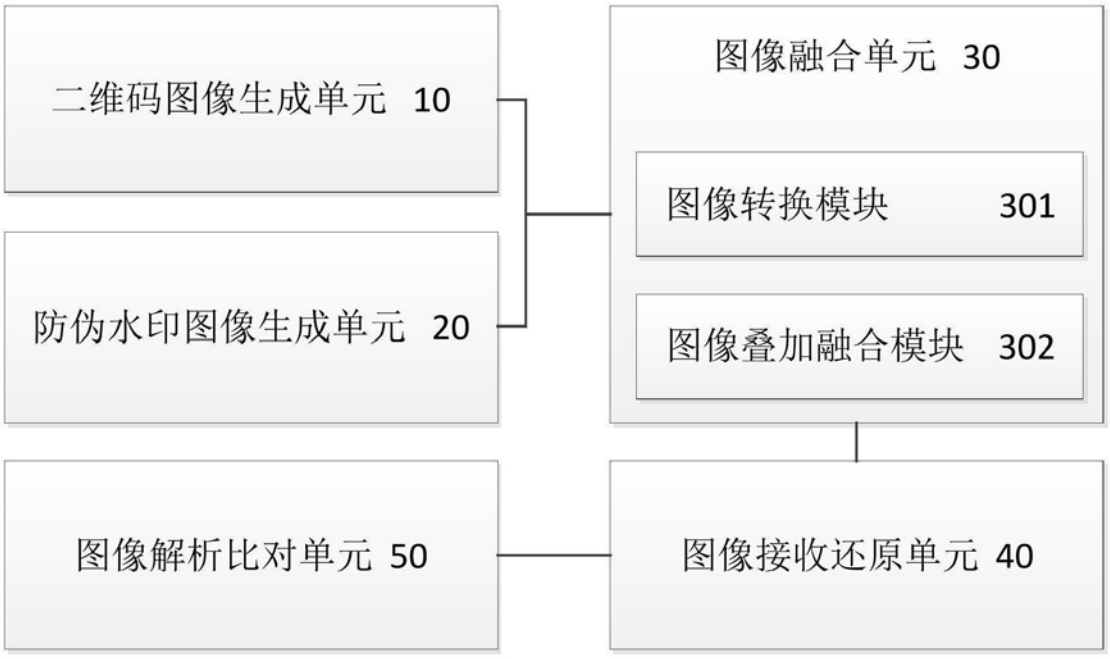

二维码图像生成单元 10
防伪水印图像生成单元 20
图像融合单元 30
图像转换模块 301
图像叠加融合模块 302
图像接收还原单元 40
图像解析比对单元 50

图3

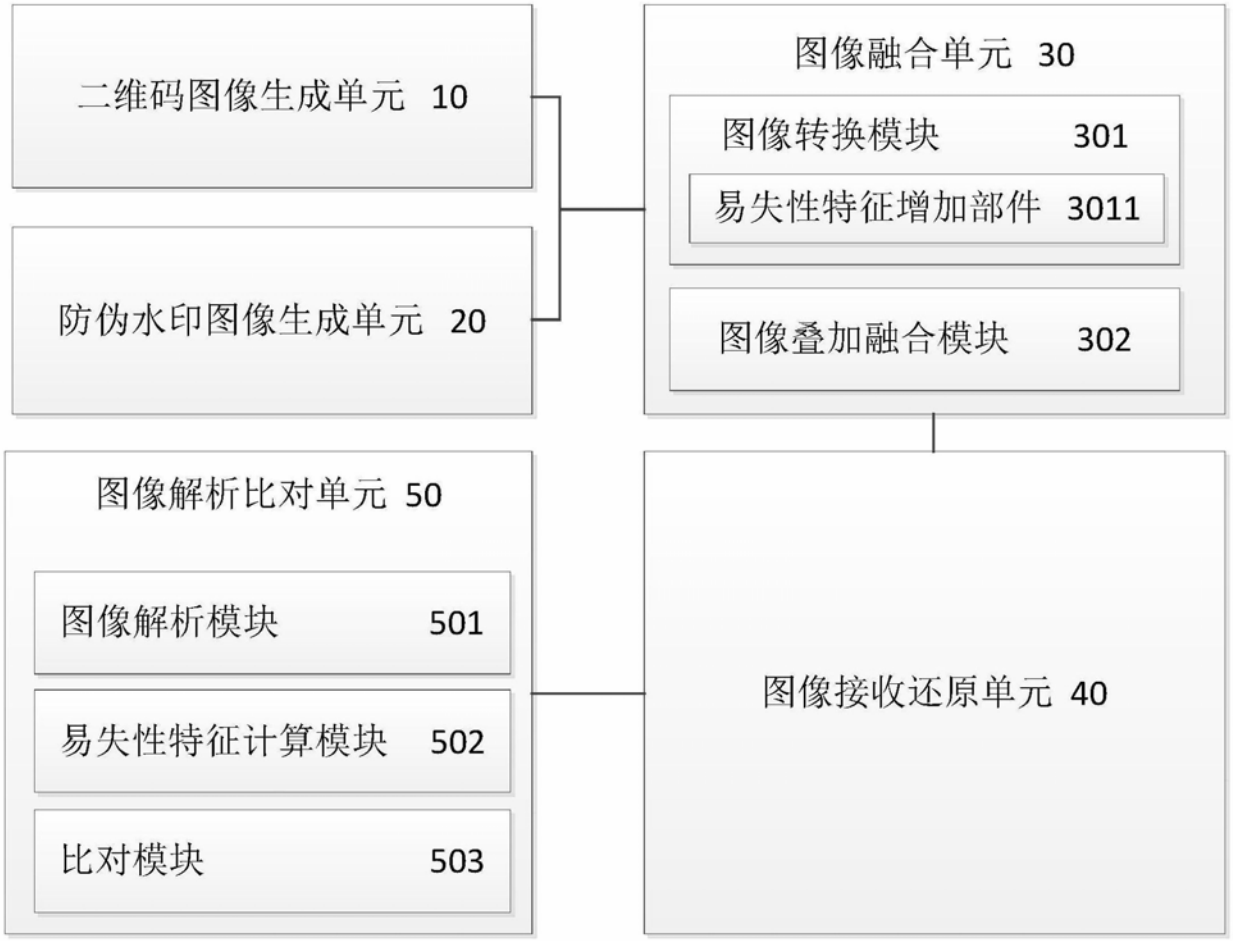

二维码图像生成单元 10
防伪水印图像生成单元 20
图像融合单元 30
图像转换模块 301
易失性特征增加部件 3011
图像叠加融合模块 302
图像解析比对单元 50
图像解析模块 501
易失性特征计算模块 502
比对模块 503
图像接收还原单元 40

图4