

(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
2021 年 2 月 25 日 (25.02.2021)



(10) 国际公布号
WO 2021/031242 A1

- (51) 国际专利分类号:
G06T 3/00 (2006.01) **G06F 21/36** (2013.01)
- (21) 国际申请号: PCT/CN2019/103664
- (22) 国际申请日: 2019 年 8 月 30 日 (30.08.2019)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201910774964.4 2019 年 8 月 21 日 (21.08.2019) CN
- (71) 申请人: 平安科技(深圳)有限公司(PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN];
中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。
- (72) 发明人: 黎立桂(LI, Liguì); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

- (74) 代理人: 北京市立方律师事务所(LIFANG & PARTNERS); 中国北京市东城区香河园街1号院信德京汇中心12层, Beijing 100028 (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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,

(54) Title: CHARACTER VERIFICATION METHOD AND APPARATUS, COMPUTER DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 字符验证方法、装置、计算机设备及存储介质

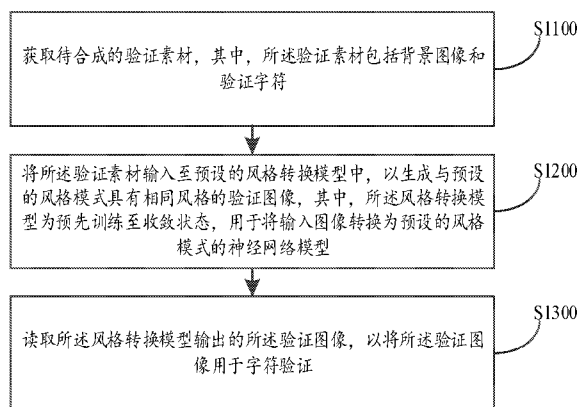


图 1

- S1100 Obtain verification materials to be synthesized, the verification materials comprising a background image and verification characters
- S1200 Input the verification materials into a preset style conversion model to generate a verification image having the same style as a preset style mode, the style conversion model being pre-trained to a convergence state and used for converting the input image into a neural network model in the preset style mode
- S1300 Read the verification image output by the style conversion model so as to use the verification image for character verification

(57) Abstract: A character verification method and apparatus, a computer device, and a storage medium. The method comprises: obtaining verification materials to be synthesized, the verification materials comprising a background image and verification characters (S1100); inputting the verification materials into a preset style conversion model to generate a verification image having the same style as a preset style mode, the style conversion model being pre-trained to a convergence state and used for converting the input image into a neural network model in the preset style mode (S1200); and reading the verification image output by the style conversion model so as to use the verification image for character verification (S1300). The background image and the verification characters are converted into images of a same style, so that grain change in the whole verification image is coherent and smooth; the background image and the verification characters do not have sharp pixel comparison, so that the difficulty in extracting the verification characters by means of an image processing technique is increased, the obfuscation degree between the background image and the verification characters is further improved, the identification difficulty and the error rate are increased, and the security of character verification is effectively guaranteed.

RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则4.17的声明:

- 发明人资格(细则4.17(iv))

本国际公布:

- 包括国际检索报告(条约第21条(3))。

(57) 摘要: 一种字符验证方法、装置、计算机设备及存储介质,包括:获取待合成的验证素材,其中,所述验证素材包括背景图像和验证字符(S1100);将所述验证素材输入至预设的风格转换模型中,以生成与预设的风格模式具有相同风格的验证图像,其中,所述风格转换模型为预先训练至收敛状态,用于将输入图像转换为预设的风格模式的神经网络模型(S1200);读取所述风格转换模型输出的所述验证图像,以将所述验证图像用于字符验证(S1300)。背景图像与验证字符转换为同一种风格图像,使整个验证图像中纹路变化连贯且平滑,背景图像与验证字符之间不具有尖锐的像素比对,提高了通过图像处理技术提取验证字符的难度,进一步地提高了背景图像与验证字符之间的混淆度,增大了识别难度和错误率,有效的保障字符验证的安全性。

字符验证方法、装置、计算机设备及存储介质

本申请要求于 2019 年 8 月 21 日提交中国专利局、申请号为 201910774964.4，发明名称为“字符验证方法、装置、计算机设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请实施例涉及数据安全领域，尤其是一种字符验证方法、装置、计算机设备及存储介质。

背景技术

伴随着科学技术的发展，信息化时代的来临为我们带来了很多的便利，同时，也为人们的生活带来诸多的困扰。例如，通过互联网进行网络购票时，常常有不法商贩通过开发应用程序快速的进行刷票，然后高价进行转卖获得暴利，而真正需要购买的用户却无法通过互联网接口进行购买，且现实生活中，类似的互联网资源抢夺发生在各个领域，通过应用程序快速刷票和领取佣金的行为难以被杜绝。为了限制上述行为的发生，信息验证应用而生。

现有技术中，通常使用验证码进行验证，终端在进行验证操作时，首先向服务器端获取验证码，然后，接收用户根据该验证码输入的验证信息，最终，由终端将采集的用户信息发送至服务器端，服务器端通过比对验证码与验证信息中的文字是否一致，确定验证是否通过。

本申请的发明人在研究中发现，现有技术中验证码技术简单的将验证码设置在背景图像上进行显示，通过图像识别技术能够无障碍的识别出验证码，然后，直接将识别出的验证码发送至服务器端进行验证，无需人工进行输入。因此，现有技术中验证码容易被识别，验证安全级别较低，无法真正保护网络资源被安全使用。

发明内容

本申请实施例提供一种通过风格转换提高验证图像的混淆度，增大图像识别难度的字符验证方法、装置、计算机设备及存储介质。

为解决上述技术问题，本申请创造的实施例采用的一个技术方案是：提供一种字符验证方法，包括：

获取待合成的验证素材，其中，所述验证素材包括背景图像和验证字符；

将所述验证素材输入至预设的风格转换模型中，以生成与预设的风格模式具有相同风格的验证图像，其中，所述风格转换模型为预先训练至收敛状态，用于将输入图像转换为预设的风格模式的神经网络模型；

读取所述风格转换模型输出的所述验证图像，以将所述验证图像用于字符验证。

为解决上述技术问题，本申请实施例还提供一种字符验证装置，包括：

获取模块，用于获取待合成的验证素材，其中，所述验证素材包括背景图像和验证字符；

处理模块，用于将所述验证素材输入至预设的风格转换模型中，以生成与预设的风格模式具有相同风格的验证图像，其中，所述风格转换模型为预先训练至收敛状态，用于将输入图像转换为预设的风格模式的神经网络模型；

读取所述风格转换模型输出的所述验证图像，以将所述验证图像用于字符验证。

为解决上述技术问题，本申请实施例还提供一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行上述所述字符验证方法的步骤，其中，所述字符验证方法的步骤，包括：

获取待合成的验证素材，其中，所述验证素材包括背景图像和验证字符；

将所述验证素材输入至预设的风格转换模型中，以生成与预设的风格模式具有相同风格的验证图像，其中，所述风格转换模型为预先训练至收敛状态，用于将输入图像转换为预设的风格模式的神经网络模型；

读取所述风格转换模型输出的所述验证图像，以将所述验证图像用于字符验证。

为解决上述技术问题，本申请实施例还提供一种存储有计算机可读指令的非易失性存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行上述所述字符验证方法的步骤，其中，所述字符验证方法的步骤，包括：

获取待合成的验证素材，其中，所述验证素材包括背景图像和验证字符；

将所述验证素材输入至预设的风格转换模型中，以生成与预设的风格模式具有相同风格的验证图像，其中，所述风格转换模型为预先训练至收敛状态，用于将输入图像转换为预设的风格模式的神经网络模型；

读取所述风格转换模型输出的所述验证图像，以将所述验证图像用于字符验证。

本申请实施例的有益效果是：将背景图像和验证字符同时输入至风格转换模型中进行风格转换，转换得到的验证图像中背景图像和验证字符均被转换为同一种风格。由于，风格转换过程中能够使验证字符与背景图像之间进行深度融合，提高了背景图像与验证字符的混淆度。同时，背景图像与验证字符转换为同一种风格图像，使整个验证图像中纹路变化连贯且平滑，背景图像与验证字符之间不具有尖锐的像素比对，提高了通过图像处理技术提取验证字符的难度，进一步地提高了背景图像与验证字符之间的混淆度，增大了识别难度和错误率，有效的保障字符验证的安全性。

附图说明

图1为本申请实施例字符验证方法的基本流程示意图；

图2为本申请实施例对验证字符进行像素填充的流程示意图；

图3为本申请实施例对背景图像和验证字符进行矢量化处理的流程示意图；

图4为本申请实施例验证用户行为的流程示意图；

图5为本申请实施例通过神经网络模型识别异常行为的流程示意图；

图6为本申请实施例通过神经网络模型筛选验证图像的流程示意图；

图7为本申请实施例获取显示区域中验证图像的流程示意图；

图8为本申请实施例字符验证装置基本结构示意图；

图9为本申请实施例计算机设备基本结构框图。

具体实施方式

为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述。

具体请参阅图1，图1为本实施例字符验证方法的基本流程示意图。

如图 1 所示，一种字符验证方法，包括：

S1100、获取待合成的验证素材，其中，所述验证素材包括背景图像和验证字符；

验证图像中的内容包括背景图像和验证字符，其中，背景图像与验证字符分别存储在对应的数据库中，进行验证时分别在对应的数据库中通过随机抽取的方式获取背景图像与验证字符。但是验证素材的存储方式不局限于此，在一些实施方式中，预先将背景图像与验证字符进行合成存储在数据库中，进行验证时在数据库中抽取一张合成的图像作为验证素材。

在本实施方式中验证字符由有限个字符组成，例如，由 4 个字符组成验证字符，但是验证字符的长度不局限于此，根据具体应用场景的不同，在一些实施方式中，验证字符的长度能够为（不限于）：2 个、3 个、5 个、6 个或者更多个字符。组成验证字符的字符类型能够为已知的具有文字记载的文字字符或者多种文字字符的组合。

本实施方式中字符验证的场景包括（不包括）：用户按照验证字符输入相同的字符进行验证、用户根据验证提示在验证字符中选择部分字符进行输入验证或者用户根据验证提示在验证字符中点选部分字符进行输入验证。

S1200、将所述验证素材输入至预设的风格转换模型中，以生成与预设的风格模式具有相同风格的验证图像，其中，所述风格转换模型为预先训练至收敛状态，用于将输入图像转换为预设的风格模式的神经网络模型；

将获取的验证素材输入至预设的风格转换模型中，风格转换模型为预先训练至收敛状态，用于将输入图像转换为预设的风格模式的神经网络模型。即风格转换模型为已经学习某种或者多种风格模式的神经网络模型，本实施方式中风格转换模型固定的学习一种风格模式，但是风格转换模型学习到的风格模式不局限于此，根据具体应用场景的不同，在一些选择性实施例，风格转换模型学习多套风格模式，根据用户的选择将验证素材转换为对应的风格模式。

其中，预设的风格模式为风格转换模型已经学习到的固有的风格模式，或者用户在多种风格模式中选定的一种风格模式。

风格模式实质上是指读取的当风格转换模型学习到某种风格模式后，对风格转换模型中卷积层的权值进行记录以此保存风格转换模型的风格转换能力。当风格转换模型中风格模式为多种时，对应变换

卷积层的权值就能够调节风格转换模型的风格模式。

将验证素材输入至风格转换模型中，对验证素材进行特征提取，然后对提取的特征进行求导，就能够使验证素材具有对应的风格。

风格转换模型能够为已经训练至收敛状态的卷积神经网络模型（CNN），但是，不局限于此，风格转换模型还能够是：深度神经网络模型（DNN）、循环神经网络模型（RNN）或者上述三种网络模型的变形模型。

S1300、读取所述风格转换模型输出的所述验证图像，以将所述验证图像用于字符验证。

读取风格转换模型输出的验证图像，验证图像中背景图像和验证字符均保持有相同的风格。

本实施方式中，验证图像的生成能够由服务器端进行处理，也能够由终端本地进行处理。服务器端处理时，将生成的验证图像发送至终端进行验证，终端获取用户输入的验证信息，将验证信息上传至服务器端，服务器端根据验证字符与验证信息是否一致判断验证结果。终端本地处理时，在抽取验证字符后，将验证字符上传至服务器端，然后生成验证图像，验证图像生成后采集用户输入的验证信息，并将验证信息发送至服务器端，服务器端根据验证字符与验证信息是否一致判断验证结果。终端本地生成验证图像能够提高验证效率，且验证时不需要传输验证图像，因此，能够有效的节约网络资源。

上述实施方式中，将背景图像和验证字符同时输入至风格转换模型中进行风格转换，转换得到的验证图像中背景图像和验证字符均被转换为同一种风格。由于，风格转换过程中能够使验证字符与背景图像之间进行深度融合，提高了背景图像与验证字符的混淆度。同时，背景图像与验证字符转换为同一种风格图像，使整个验证图像中纹路变化连贯且平滑，背景图像与验证字符之间不具有尖锐的像素比对，提高了通过图像处理技术提取验证字符的难度，进一步地提高了背景图像与验证字符之间的混淆度，增大了识别难度和错误率，有效的保障字符验证的安全性。

在一些实施方式中，为加深背景图像与验证字符的融合深度，进一步地提高图像识别的难度，在进行验证图像生成之前，需要对背景图像和验证字符进行初步融合。请参阅图 2，图 2 为本实施例对验证字符进行像素填充的流程示意图。

如图 2 所示，图 1 所示的 S1200 的步骤之前，包括：

S1111、获取所述背景图像中的背景像素值；

在获取验证素材后，提取背景图像中的背景像素值，其中，背景像素值为背景图相中像素值占比最大的像素值。但是，背景像素值的取值不局限于此，根据具体应用场景的不同，在一些实施方式中，背景像素值为验证字符已覆盖区域中像素值占比最大的像素值。

背景像素值的取值（R、G 和 B），其中，R、G 和 B 均为大于等于 0 小于等于 255 的自然数。

S1112、根据预设的像素计算规则计算所述背景像素值对应的填充像素值，其中，所述填充像素值与所述背景像素值之间的色差值等于预设的第一色差阈值；

获取背景像素值后，根据预设的像素计算规则计算与该背景像素值对应的填充像素值，其中，像素计算规则为：计算与背景像素值之间色差值等于预设的第一色差阈值的填充像素值。第一色差阈值被定义为 2，但是第一色差阈值的取值不局限于此，根据具体应用场景的不同，在一些实施方式中，第一色差阈值的取值能够为：3、4 或 5。

需要指出的时，当背景像素值的通道取值 $(R+G+B)/3 \leq 255$ 时，在背景像素值上加第一色差阈值得到填充像素值；当背景像素值的通道取值 $(R+G+B)/3 > 255$ 时，在背景像素值上减去第一色差阈值得到填充像素值。

S1113、调用与所述填充像素值所映射的图像颜色对所述验证字符进行填充。

计算得到填充像素值后，调用与填充像素值对应的图像颜色对验证字符进行填充。由于填充像素值同样也由（R、G 和 B）三个通道颜色组成，因此，填充像素值所表征的也是一种图像颜色。

通过背景像素值计算得到填充像素值，能够使背景图像与验证字符之间的色差值位于人眼可识别的一个范围内，且该范围被限定的足够小，以使背景图像与验证字符之间融合的更深，进一步地提高图像识别的难度。

在一些实施方式中，为进一步地减少风格转换模型的运算难度，加快风格转换模型的处理速度，对背景图像和验证字符进行图像矢量化处理。请参阅图 3，图 3 为本实施例对背景图像和验证字符进行矢量化处理的流程示意图。

如图 3 所示，图 2 所示的 S1113 的步骤之后，包括：

S1121、将所述验证字符设置在所述背景图像上；

对验证字符进行颜色填充后,根据验证字符中字符之间的空间顺序,将验证字符放置背景图像上。在一些实施方式中,为增加图像识别难度,在进行验证字符设置时对验证字符进行扭曲变形。

S1122、根据所述验证字符与所述背景图像进行图像合成生成合成图像;

将验证字符设置在背景图像上后,验证字符对其所在区域进行像素覆盖,此时,背景图像和验证字符生成合成图像。

S1123、对所述合成图像进行图像矢量化处理生成矢量图像,其中,所述矢量图像替代所述验证素材输入至所述风格转换模型中。

对合成图像进行图像矢量化处理,是将对合成图由位图转化为矢量图,转化后的矢量图像由线段形成外框轮廓,由外框的颜色以及外框所封闭的颜色决定图案显示出的颜色。

在本实施方式中矢量图像将被输入至风格转换模型中进行风格转换。

由于,由于矢量图形可通过公式计算获得,所以矢量图形文件体积一般较小。方便风格转换模型进行运算,提高了运算效率。

在一些实施方式中,除通过验证字符和验证信息比对进行结果验证之外,判断用户是否为人工输入时,还能够通过用户输入验证信息时的行为进行行为验证。请参阅图4,图4为本实施例验证用户行为的流程示意图。

如图4所示,图1所示的S1300步骤之后,包括:

S1310、获取用户根据所述验证图像输入验证信息时的输入节点信息,其中,所述输入节点信息包括用户输入各个字符时的输入时间;

用户参照验证图像中的验证字符输入验证信息时,需要通过在终端的键盘上进行依次输入。本实施方式所指的键盘为与终端连接的外设键盘或者在终端显示区域虚拟显示的软键盘。

定义用户输入每个字符时的时刻为输入时间,则用户进行验证时输入的所有字符的输入时间的集合为输入节点信息。

S1320、根据所述输入节点信息判断所述用户的输入行为是否为异常输入行为;

根据收集得到的输入节点信息判断用户的输入行为是否为异常输入行为,判断的方式为计算两个相邻输入时间之间的时间差是否一致。但是判断方法不局限于此,为应对一些更为复杂的模拟真人输入的验证破解方案,还能够采用神经网络模型对用户行为进行判断。

S1330、当所述用户的输入行为判定为异常输入行为时，确认验证结果为验证失败。

当两个相邻输入时间之间的时间差均为同一个数值时，判断用户输入为异常输入，否则，则用户的输入为正常输入。使用神经网络模型进行异常判断时，则根据神经网络模型的分类结果判断用户行为是否异常。

当确认用户行为验证为异常行为时，则无论验证字符与验证信息的比对是否一致，均确定此次字符验证的验证结果为验证失败。

通过采集用户输入验证信息时的时间信息，判断输入字符的时间是否为具有非人为输入的痕迹，如果存在则判定验证行为异常，有效的防止采用图像识别技术进行图像验证。

在一些实施方式中，为应对复杂的图像识别技术对用户行为进行针对性破解，例如，修改输入各个字符的输入时间间隔，以防止输入间隔一致被确定为异常行为的破解方案。需要掌握更多的识别非人为的操作的方法，或者从更深的维度识别非人为操作痕迹的方法。请参阅图 5，图 5 为本实施例通过神经网络模型识别异常行为的流程示意图。

如图 5 所示，图 4 所示的 S1320 步骤包括：

S1321、将所述输入时间按时序排列生成时间矩阵；

将获取的输入时间按照时序的先后顺序排列生成时间矩阵。

S1322、将所述时间矩阵输入至预设的第一验证模型中，以判断所述用户的输入行为是否为异常输入行为，其中，所述第一验证模型为预先训练至收敛状态，用于根据所述输入时间判断用户输入行为是否异常的神经网络模型；

将时间矩阵输入至第一验证模型中进行特征提取与分类。第一验证模型能够为已经训练至收敛状态的卷积神经网络模型（CNN），但是，不局限于此，第一验证模型还能够是：深度神经网络模型（DNN）、循环神经网络模型（RNN）或者上述三种网络模型的变形模型。

作为第一验证模型的初始神经网络模型在训练时，通过收集大量的输入时间信息转换后的时间矩阵作为训练样本，通过人工在观察了数据的输入时的主体后（人为输入或者非人为输入），对各个训练样本进行标定（标定各个训练样本的分类结果）。然后将训练样本输入到初始的神经网络模型中，神经网络模型提取该训练样本的特征向量，并将该特征向量与分类层的分类类目进行比对，得到特征向量与各个

分类类目之间的置信度，置信度最高的分类类目即为分类结果。

获取模型输出的分类结果(分类结果为模型计算得到的输入时间信息的分类结果)，并通过神经网络模型的损失函数计算该分类结果与标定结果之间的距离(例如：欧氏距离、马氏距离或余弦距离等)，将计算结果与设定的距离阈值(距离阈值的取值与对言交互模型的准确率成反比，即准确率要求越高，距离阈值的取值越低)进行比对，若计算结果小于等于距离阈值则通过验证，继续进行下一个训练样本的训练，若计算结果大于距离阈值则通过损失函数计算二者之间的差值，并通过反向传播校正神经网络模型内的权值，使神经网络模型能够提高训练样本中准确表达输入主体的元素的权重，以此，增大提取的准确率和全面性。通过循环执行上述方案和大量的训练样本训练后，训练得到的神经网络模型对时间矩阵分类的准确率大于一定数值的，例如，95%，则该神经网络模型训练至收敛状态，则该训练至收敛的神经网络即为第一验证模型。

训练至收敛状态的第一验证模型能够准确的对时间矩阵进行分类。

S1323、读取所述第一验证模型输出的判断结果。

读取第一验证模型输出的分类结果，分类结果中记载的信息即为第一验证模型对时间矩阵所表征的用户行为的判断结果。当判断结果为异常时，则用户行为为异常行为；否则，则用户行为为正常行为。

通过神经网络模型能够快速的对用户行为进行准确判断，也能够对有意模拟人为输入的非人为操作行为进行辨识，提高了验证的便捷性和安全性。

在一些实施方式中，为防止验证图像被恶意者采用深度学习的方法进行破解，验证图像生成后采用现有技术中已经训练至收敛的用于字符识别的第二验证模型对验证图像进行识别，根据识别结果判断是否需要对验证图像进行替换。请参阅图6，图6为本实施例通过神经网络模型筛选验证图像的流程示意图。

如图6所示，图1所示的S1300步骤之后，包括：

S1410、将所述验证图像输入至预设的第二验证模型中，其中，所述第二验证模型为预先训练至收敛状态，用于提取所述验证图像中字符信息的神经网络模型；

将获取得到的验证图像输入至预设的第二验证模型中，其中，第二验证模型为预先训练至收敛状态，用于提取验证图像中字符信息的

神经网络模型。第二验证模型现有技术中已经训练至收敛的用于字符识别的第二验证模型。

S1420、获取所述第二验证模型输出的分类结果，其中，所述分类结果中包括所述第二验证模型提取的所述验证图像中的字符信息；

获取第二验证模型输出的分类结果，分类结果中包括第二验证模型提取的验证图像中的字符信息。

S1430、将所述字符信息与所述验证字符进行比对，当所述字符信息与所述验证字符一致时，对所述验证图像进行刷新。

将字符信息与验证字符进行比对，比对的方式为采用汉明距离或者海明距离进行比对，具体地，计算字符信息与验证字符之间的海明距离或汉明距离，当二者之间的海明距离或汉明距离为0时，表明字符信息与验证字符一致，否则，则表明字符信息与验证字符不一致。当字符信息与验证字符一致时，表明验证图像中的验证字符能够被现有技术中的AI模型识别并提取，该验证图像不符合验证的需求，需要被替换，因此，当字符信息与验证字符一致时对验证图像进行刷新，重新生成验证图像。

通过神经网络模型对验证图像进行筛选，降低了验证图像被AI图像识别的几率，有效的保证了验证的安全性。

在一些实施方式中，部分非人工验证的验证方式直接提取后台的验证图像，经过计算后将验证参数进行上传，完成验证。为限制该模拟验证的行为，需要通过图像分类的方法对验证完成时的验证画面进行判断，以确定是否进行了真实的字符验证。请参阅图7，图7为本实施例获取显示区域中验证图像的流程图示意图。

S1401、获取帧缓冲存储器内的显示数据；

终端对验证图像进行显示时，需要将包括验证图像的验证页面存储在帧缓冲存储器内，即帧缓冲存储器内是屏幕所显示画面的一个直接映像，又称为位映射图(Bit Map)，也即显示数据。

S1402、根据所述验证图像在验证页面中预设的显示位置，在所述显示数据内提取表征所述验证图像的目标数据；

由于，验证图像在位映射图中的具有设定的区域，根据设定区域的信息，在位映射图提取表征验证区域内容的数据区域生成局部位映射图，即表征验证图像显示内容的目标数据。

S1403、将所述目标数据转换为图片格式生成所述验证图像。

最后将目标数据转换为常规的图片格式，例如（不限于）JPG、

PNG 或者 TIF 等格式，生成验证图像。

在一些实施方式中，在帧缓冲存储器内无法获取到验证图像时，则表明该验证方式为虚拟验证。

通过对验证页面中验证图像进行验证，能够有效地防止通过虚拟验证的进行数据上传的验证漏洞，大大地提高了验证的安全性。

为解决上述技术问题，本申请实施例还提供一种字符验证装置。

具体请参阅图 8, 图 8 为本实施例字符验证装置基本结构示意图。

如图 8 所示，一种字符验证装置，包括：获取模块 2100、处理模块 2200 和执行模块 2300。其中，获取模块 2100 用于获取待合成的验证素材，其中，验证素材包括背景图像和验证字符；处理模块 2200 用于将验证素材输入至预设的风格转换模型中，以生成与预设的风格模式具有相同风格的验证图像，其中，风格转换模型为预先训练至收敛状态，用于将输入图像转换为预设的风格模式的神经网络模型；执行模块 2300 用于读取风格转换模型输出的验证图像，以将验证图像用于字符验证。

字符验证装置将背景图像和验证字符同时输入至风格转换模型中进行风格转换，转换得到的验证图像中背景图像和验证字符均被转换为同一种风格。由于，风格转换过程中能够使验证字符与背景图像之间进行深度融合，提高了背景图像与验证字符的混淆度。同时，背景图像与验证字符转换为同一种风格图像，使整个验证图像中纹路变化连贯且平滑，背景图像与验证字符之间不具有尖锐的像素比对，提高了通过图像处理技术提取验证字符的难度，进一步地提高了背景图像与验证字符之间的混淆度，增大了识别难度和错误率，有效的保障字符验证的安全性。

在一些实施方式中，字符验证装置还包括：第一获取子模块、第一处理子模块和第一执行子模块。其中，第一获取子模块用于获取背景图像中的背景像素值；第一处理子模块用于根据预设的像素计算规则计算背景像素值对应的填充像素值，其中，填充像素值与背景像素值之间的色差值等于预设的第一色差阈值；第一执行子模块用于调用与填充像素值所映射的图像颜色对验证字符进行填充。

在一些实施方式中，字符验证装置还包括：第二处理子模块、第一合成子模块和第二执行子模块。其中，第二处理子模块用于将验证字符设置在背景图像上；第一合成子模块用于根据验证字符与背景图像进行图像合成生成合成图像；第二执行子模块用于对合成图像进行

图像矢量化处理生成矢量图像，其中，矢量图像替代验证素材输入至风格转换模型中。

在一些实施方式中，字符验证装置还包括：第二获取子模块、第三处理子模块和第三执行子模块。第二获取子模块用于获取用户根据验证图像输入验证信息时的输入节点信息，其中，输入节点信息包括用户输入各个字符时的输入时间；第三处理子模块用于根据输入节点信息判断用户的输入行为是否为异常输入行为；第三执行子模块用于当用户的输入行为判定为异常输入行为时，确认验证结果为验证失败。

在一些实施方式中，字符验证装置还包括：第一生成子模块、第四处理子模块和第四执行子模块。其中，第一生成子模块用于将输入时间按时序排列生成时间矩阵；第四处理子模块用于将时间矩阵输入至预设的第一验证模型中，以判断用户的输入行为是否为异常输入行为，其中，第一验证模型为预先训练至收敛状态，用于根据输入时间判断用户输入行为是否异常的神经网络模型；第四执行子模块用于读取第一验证模型输出的判断结果。

在一些实施方式中，字符验证装置还包括：第五处理子模块、第三获取子模块和第五执行子模块。其中，第五处理子模块用于将验证图像输入至预设的第二验证模型中，其中，第二验证模型为预先训练至收敛状态，用于提取验证图像中字符信息的神经网络模型；第三获取子模块用于获取第二验证模型输出的分类结果，其中，分类结果中包括第二验证模型提取的验证图像中的字符信息；第五执行子模块用于将字符信息与验证字符进行比对，当字符信息与验证字符一致时，对验证图像进行刷新。

在一些实施方式中，字符验证装置还包括：第四获取子模块、第六处理子模块和第六执行子模块。其中，第四获取子模块用于获取帧缓冲存储器内的显示数据；第六处理子模块用于根据验证图像在验证页面中预设的显示位置，在显示数据内提取表征验证图像的目标数据；第六执行子模块用于将目标数据转换为图片格式生成验证图像。

为解决上述技术问题，本申请实施例还提供计算机设备。具体请参阅图9，图9为本实施例计算机设备基本结构框图。

如图9所示，计算机设备的内部结构示意图。该计算机设备包括通过系统总线连接的处理器、非易失性存储介质、存储器和网络接口。其中，该计算机设备的非易失性存储介质存储有操作系统、数据库和计算机可读指令，数据库中可存储有控件信息序列，该计算机可读指

令被处理器执行时，可使得处理器实现一种字符验证方法。该计算机设备的处理器用于提供计算和控制能力，支撑整个计算机设备的运行。该计算机设备的存储器中可存储有计算机可读指令，该计算机可读指令被处理器执行时，可使得处理器执行一种字符验证方法。该计算机设备的网络接口用于与终端连接通信。本领域技术人员可以理解，图 9 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

本实施方式中处理器用于执行图 8 中获取模块 2100、处理模块 2200 和执行模块 2300 的具体功能，存储器存储有执行上述模块所需的程序代码和各类数据。网络接口用于向用户终端或服务器之间的数据传输。本实施方式中的存储器存储有人脸图像关键点检测装置中执行所有子模块所需的程序代码及数据，服务器能够调用服务器的程序代码及数据执行所有子模块的功能。

计算机设备将背景图像和验证字符同时输入至风格转换模型中进行风格转换，转换得到的验证图像中背景图像和验证字符均被转换为同一种风格。由于，风格转换过程中能够使验证字符与背景图像之间进行深度融合，提高了背景图像与验证字符的混淆度。同时，背景图像与验证字符转换为同一种风格图像，使整个验证图像中纹路变化连贯且平滑，背景图像与验证字符之间不具有尖锐的像素比对，提高了通过图像处理技术提取验证字符的难度，进一步地提高了背景图像与验证字符之间的混淆度，增大了识别难度和错误率，有效的保障字符验证的安全性。

本申请还提供一种存储有计算机可读指令的非易失性存储介质，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行上述任一实施例字符验证方法的步骤。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，该计算机程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，前述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory, ROM）等非易失性存储介质，或随机存储记忆体（Random Access Memory, RAM）等。

应该理解的是，虽然附图的流程图中的各个步骤按照箭头的指示

依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，其可以以其他的顺序执行。而且，附图的流程图中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，其执行顺序也不必然是依次进行，而是可以与其他步骤或者其他步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

权 利 要 求 书

1.一种字符验证方法，包括：

获取待合成的验证素材，其中，所述验证素材包括背景图像和验证字符；

将所述验证素材输入至预设的风格转换模型中，以生成与预设的风格模式具有相同风格的验证图像，其中，所述风格转换模型为预先训练至收敛状态，用于将输入图像转换为预设的风格模式的神经网络模型；

读取所述风格转换模型输出的所述验证图像，以将所述验证图像用于字符验证。

2.根据权利要求1所述的字符验证方法，所述将所述验证素材输入至预设的风格转换模型中，以生成与预设的风格模式具有相同风格的验证图像之前，包括：

获取所述背景图像中的背景像素值；

根据预设的像素计算规则计算所述背景像素值对应的填充像素值，其中，所述填充像素值与所述背景像素值之间的色差值等于预设的第一色差阈值；

调用与所述填充像素值所映射的图像颜色对所述验证字符进行填充。

3.根据权利要求2所述的字符验证方法，所述调用与所述填充像素值所映射的图像颜色对所述验证字符进行填充之后，包括：

将所述验证字符设置在所述背景图像上；

根据所述验证字符与所述背景图像进行图像合成生成合成图像；

对所述合成图像进行图像矢量化处理生成矢量图像，其中，所述矢量图像替代所述验证素材输入至所述风格转换模型中。

4.根据权利要求1所述的字符验证方法，所述读取所述风格转换模型输出的所述验证图像，以将所述验证图像用于字符验证之后，包括：

获取用户根据所述验证图像输入验证信息时的输入节点信息，其中，所述输入节点信息包括用户输入各个字符时的输入时间；

根据所述输入节点信息判断所述用户的输入行为是否为异常输入行为；

当所述用户的输入行为判定为异常输入行为时，确认验证结果为验证失败。

5.根据权利要求4所述的字符验证方法,所述根据所述输入节点信息判断所述用户的输入行为是否为异常输入行为包括:

将所述输入时间按时序排列生成时间矩阵;

将所述时间矩阵输入至预设的第一验证模型中,以判断所述用户的输入行为是否为异常输入行为,其中,所述第一验证模型为预先训练至收敛状态,用于根据所述输入时间判断用户输入行为是否异常的神经网络模型;

读取所述第一验证模型输出的判断结果。

6.根据权利要求1所述的字符验证方法,所述读取所述风格转换模型输出的所述验证图像,以将所述验证图像用于字符验证之后,包括:

将所述验证图像输入至预设的第二验证模型中,其中,所述第二验证模型为预先训练至收敛状态,用于提取所述验证图像中字符信息的神经网络模型;

获取所述第二验证模型输出的分类结果,其中,所述分类结果中包括所述第二验证模型提取的所述验证图像中的字符信息;

将所述字符信息与所述验证字符进行比对,当所述字符信息与所述验证字符一致时,对所述验证图像进行刷新。

7.根据权利要求6所述的字符验证方法,所述将所述验证图像输入至预设的第二验证模型中之前,包括:

获取帧缓冲存储器内的显示数据;

根据所述验证图像在验证页面中预设的显示位置,在所述显示数据内提取表征所述验证图像的目标数据;

将所述目标数据转换为图片格式生成所述验证图像。

8.一种字符验证装置,包括:

获取模块,用于获取待合成的验证素材,其中,所述验证素材包括背景图像和验证字符;

处理模块,用于将所述验证素材输入至预设的风格转换模型中,以生成与预设的风格模式具有相同风格的验证图像,其中,所述风格转换模型为预先训练至收敛状态,用于将输入图像转换为预设的风格模式的神经网络模型;

执行模块,用于读取所述风格转换模型输出的所述验证图像,以将所述验证图像用于字符验证。

9.一种计算机设备,包括存储器和处理器,所述存储器中存储有

计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行上述权利要求所述字符验证方法的步骤。

10.根据权利要求 9 所述的计算机设备，所述将所述验证素材输入至预设的风格转换模型中，以生成与预设的风格模式具有相同风格的验证图像之前，包括：

获取所述背景图像中的背景像素值；

根据预设的像素计算规则计算所述背景像素值对应的填充像素值，其中，所述填充像素值与所述背景像素值之间的色差值等于预设的第一色差阈值；

调用与所述填充像素值所映射的图像颜色对所述验证字符进行填充。

11.根据权利要求 10 所述的计算机设备，所述调用与所述填充像素值所映射的图像颜色对所述验证字符进行填充之后，包括：

将所述验证字符设置在所述背景图像上；

根据所述验证字符与所述背景图像进行图像合成生成合成图像；

对所述合成图像进行图像矢量化处理生成矢量图像，其中，所述矢量图像替代所述验证素材输入至所述风格转换模型中。

12.根据权利要求 9 所述的计算机设备，所述读取所述风格转换模型输出的所述验证图像，以将所述验证图像用于字符验证之后，包括：

获取用户根据所述验证图像输入验证信息时的输入节点信息，其中，所述输入节点信息包括用户输入各个字符时的输入时间；

根据所述输入节点信息判断所述用户的输入行为是否为异常输入行为；

当所述用户的输入行为判定为异常输入行为时，确认验证结果为验证失败。

13.根据权利要求 12 所述的计算机设备，所述根据所述输入节点信息判断所述用户的输入行为是否为异常输入行为包括：

将所述输入时间按时序排列生成时间矩阵；

将所述时间矩阵输入至预设的第一验证模型中，以判断所述用户的输入行为是否为异常输入行为，其中，所述第一验证模型为预先训练至收敛状态，用于根据所述输入时间判断用户输入行为是否异常的神经网络模型；

读取所述第一验证模型输出的判断结果。

14.根据权利要求 9 所述的计算机设备,所述读取所述风格转换模型输出的所述验证图像,以将所述验证图像用于字符验证之后,包括:

将所述验证图像输入至预设的第二验证模型中,其中,所述第二验证模型为预先训练至收敛状态,用于提取所述验证图像中字符信息的神经网络模型;

获取所述第二验证模型输出的分类结果,其中,所述分类结果中包括所述第二验证模型提取的所述验证图像中的字符信息;

将所述字符信息与所述验证字符进行比对,当所述字符信息与所述验证字符一致时,对所述验证图像进行刷新。

15.一种存储有计算机可读指令的非易失性存储介质,所述计算机可读指令被一个或多个处理器执行时,使得一个或多个处理器执行上述权利要求所述字符验证方法的步骤。

16.根据权利要求 15 所述的非易失性存储介质,所述将所述验证素材输入至预设的风格转换模型中,以生成与预设的风格模式具有相同风格的验证图像之前,包括:

获取所述背景图像中的背景像素值;

根据预设的像素计算规则计算所述背景像素值对应的填充像素值,其中,所述填充像素值与所述背景像素值之间的色差值等于预设的第一色差阈值;

调用与所述填充像素值所映射的图像颜色对所述验证字符进行填充。

17.根据权利要求 16 所述的非易失性存储介质,所述调用与所述填充像素值所映射的图像颜色对所述验证字符进行填充之后,包括:

将所述验证字符设置在所述背景图像上;

根据所述验证字符与所述背景图像进行图像合成生成合成图像;

对所述合成图像进行图像矢量化处理生成矢量图像,其中,所述矢量图像替代所述验证素材输入至所述风格转换模型中。

18.根据权利要求 15 所述的非易失性存储介质,所述读取所述风格转换模型输出的所述验证图像,以将所述验证图像用于字符验证之后,包括:

获取用户根据所述验证图像输入验证信息时的输入节点信息,其中,所述输入节点信息包括用户输入各个字符时的输入时间;

根据所述输入节点信息判断所述用户的输入行为是否为异常输

入行为；

当所述用户的输入行为判定为异常输入行为时，确认验证结果为验证失败。

19.根据权利要求 18 所述的非易失性存储介质，所述根据所述输入节点信息判断所述用户的输入行为是否为异常输入行为包括：

将所述输入时间按时序排列生成时间矩阵；

将所述时间矩阵输入至预设的第一验证模型中，以判断所述用户的输入行为是否为异常输入行为，其中，所述第一验证模型为预先训练至收敛状态，用于根据所述输入时间判断用户输入行为是否异常的神经网络模型；

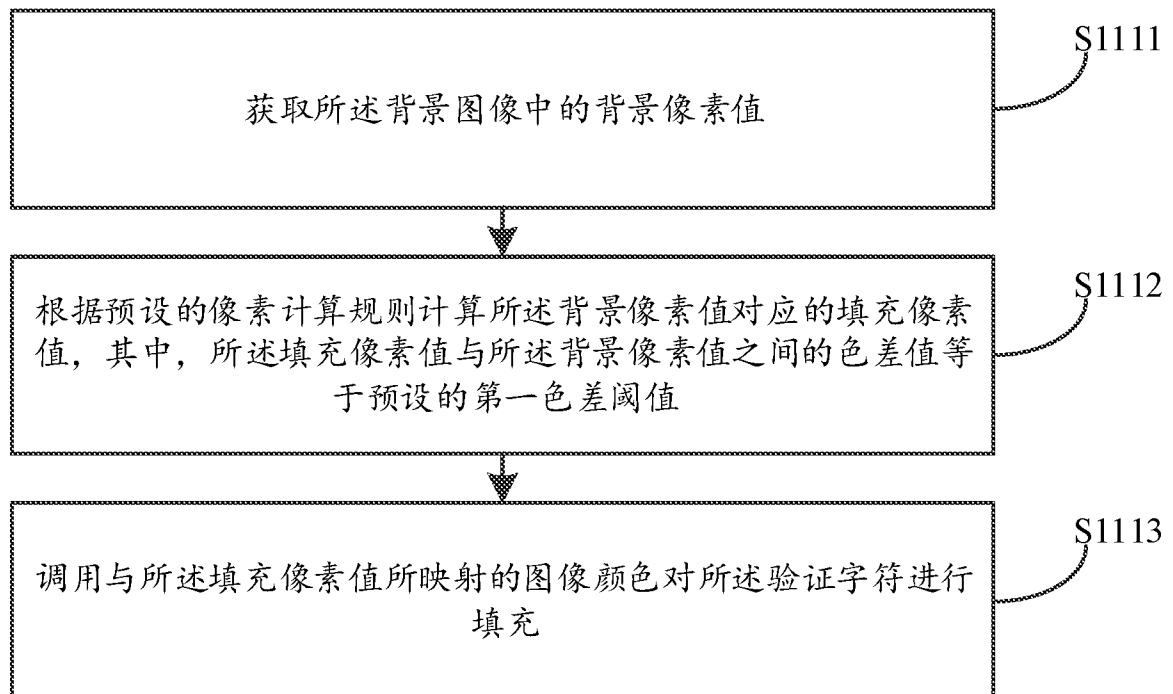
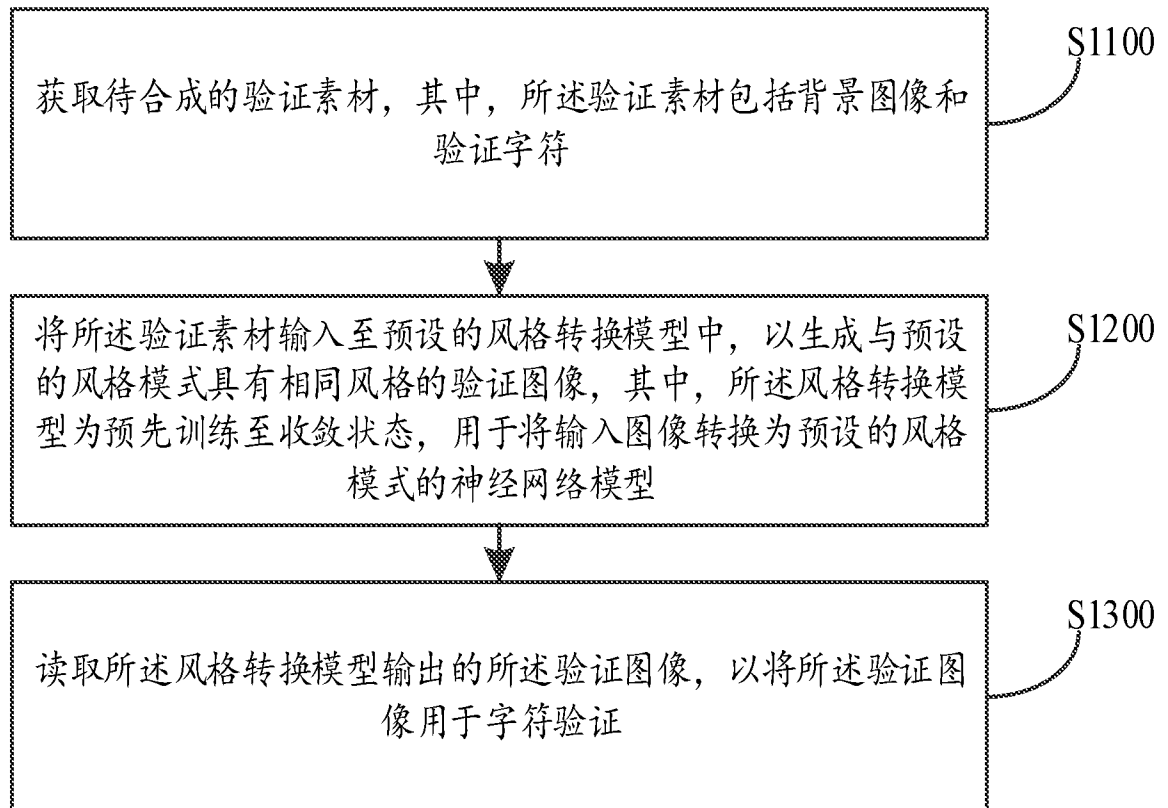
读取所述第一验证模型输出的判断结果。

20.根据权利要求 15 所述的非易失性存储介质，所述读取所述风格转换模型输出的所述验证图像，以将所述验证图像用于字符验证之后，包括：

将所述验证图像输入至预设的第二验证模型中，其中，所述第二验证模型为预先训练至收敛状态，用于提取所述验证图像中字符信息的神经网络模型；

获取所述第二验证模型输出的分类结果，其中，所述分类结果中包括所述第二验证模型提取的所述验证图像中的字符信息；

将所述字符信息与所述验证字符进行比对，当所述字符信息与所述验证字符一致时，对所述验证图像进行刷新。



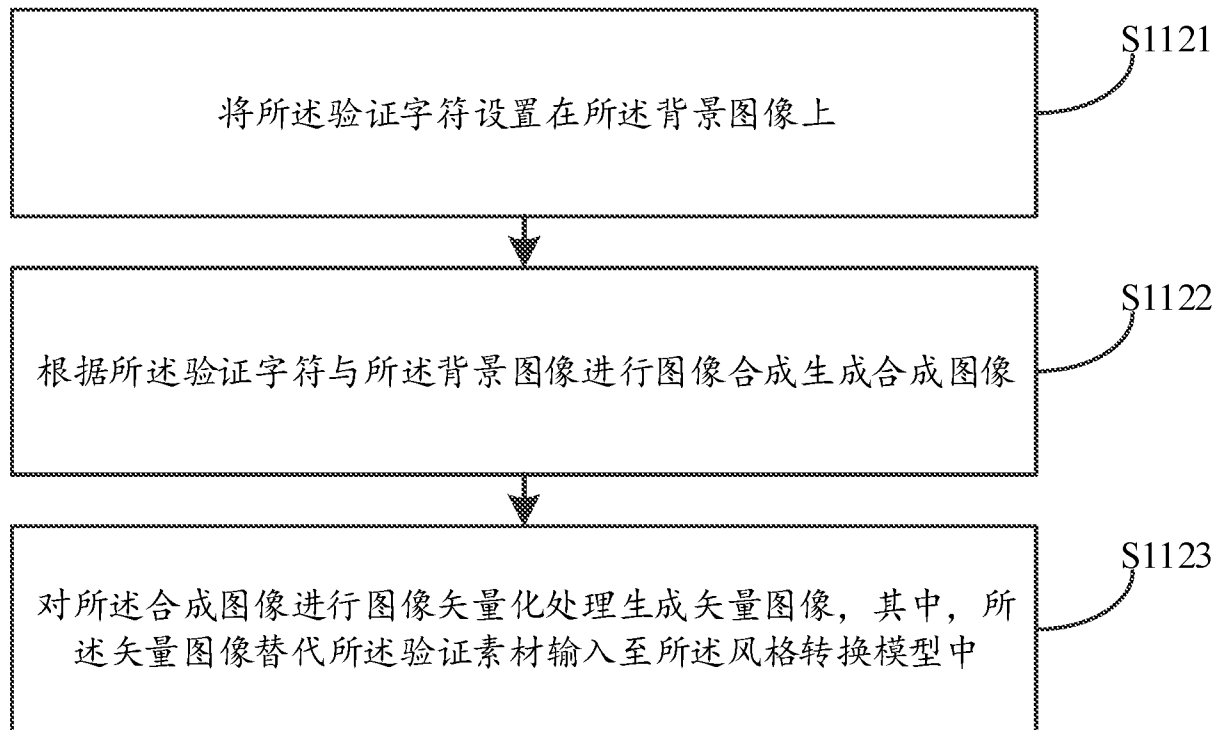


图 3

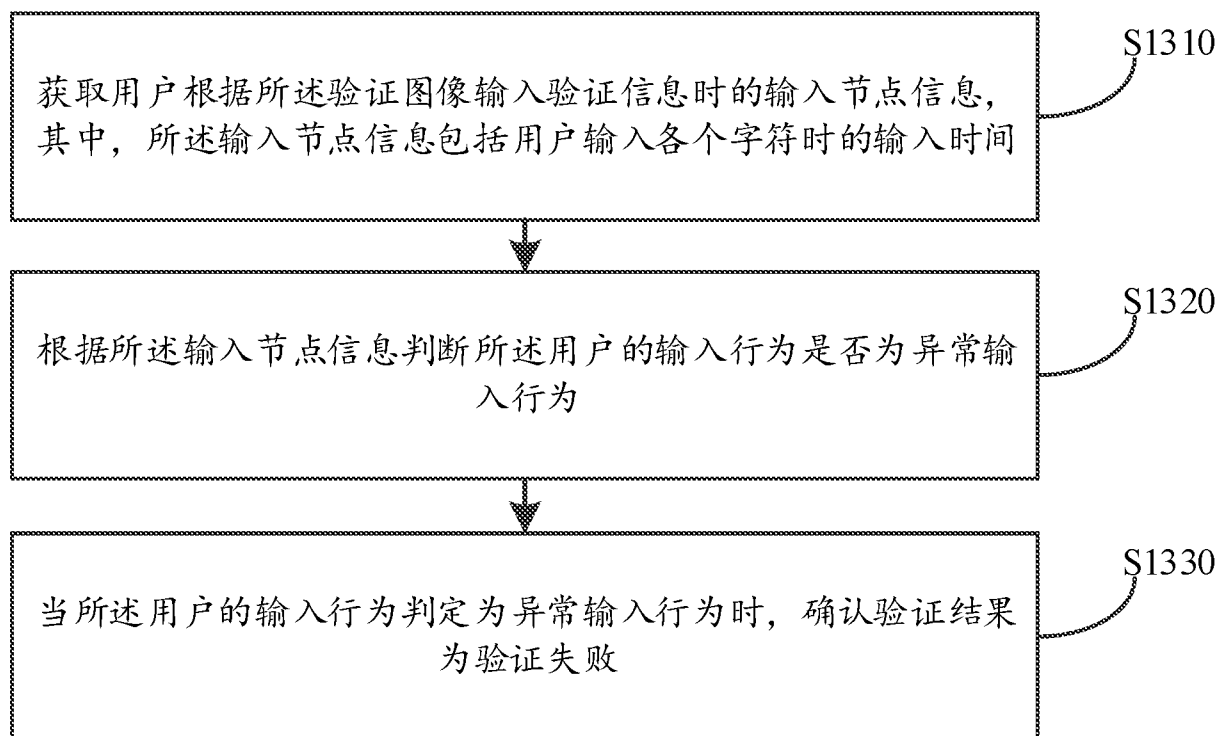


图 4

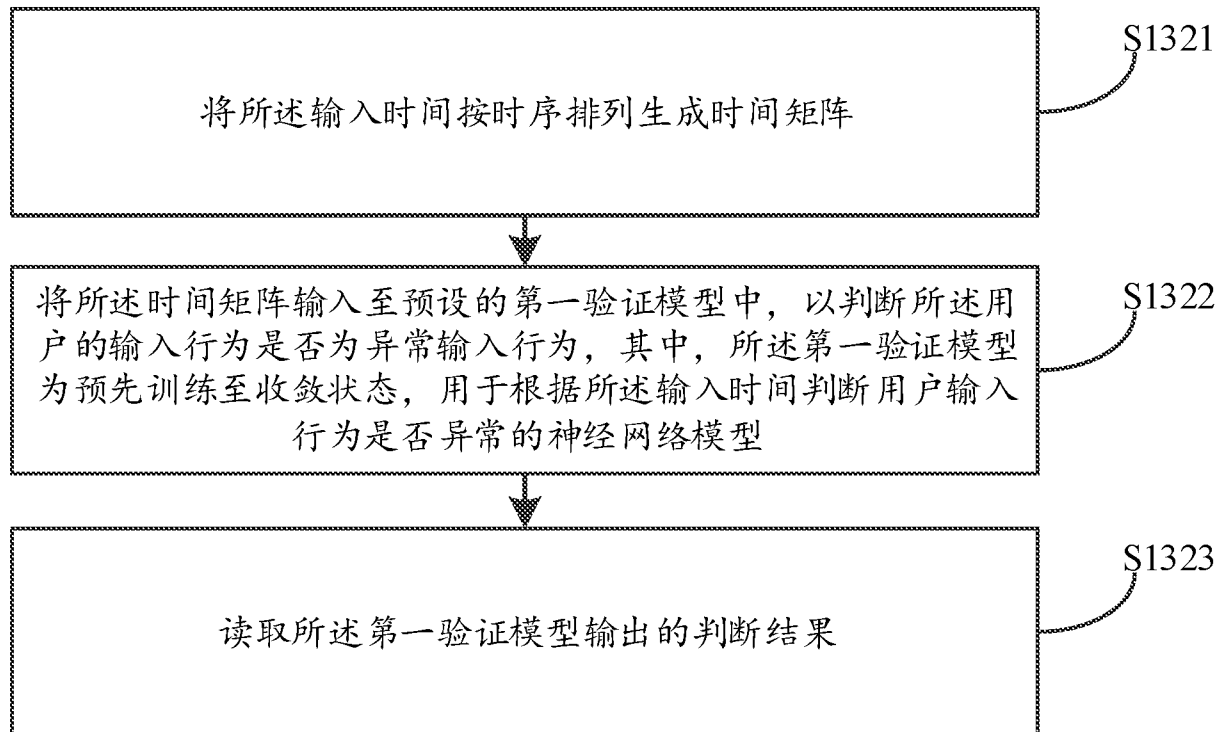


图 5

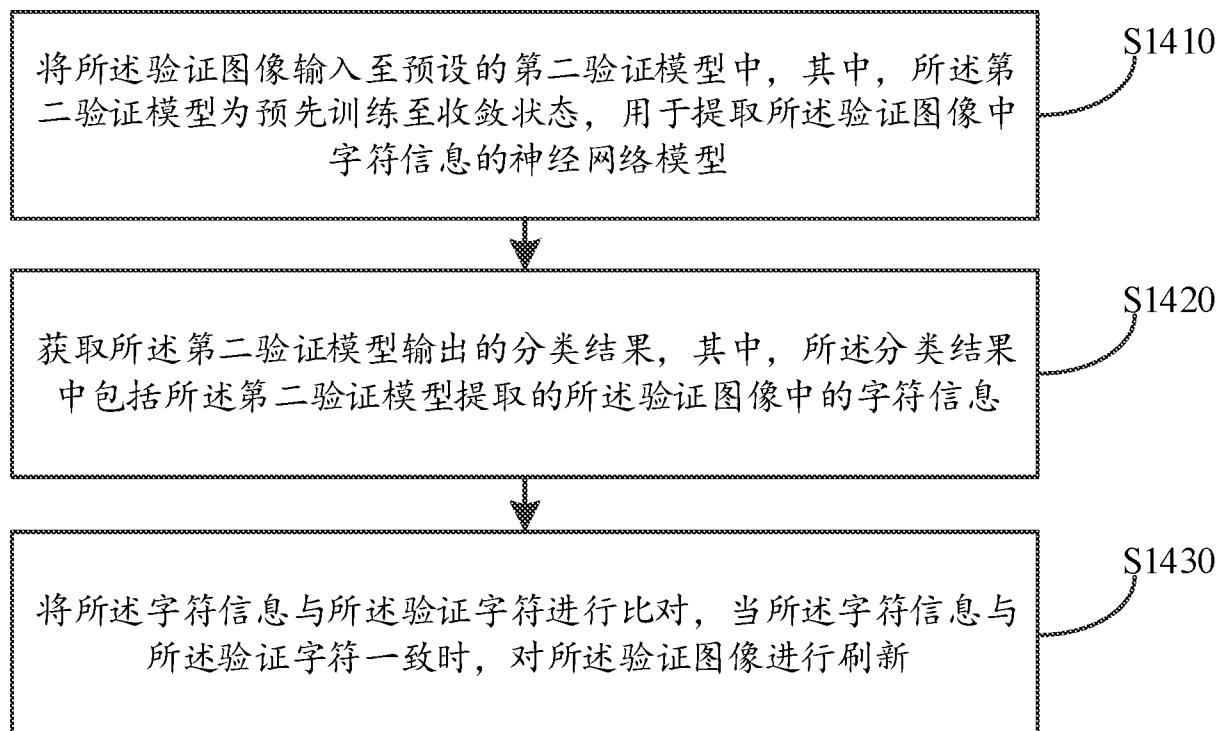


图 6

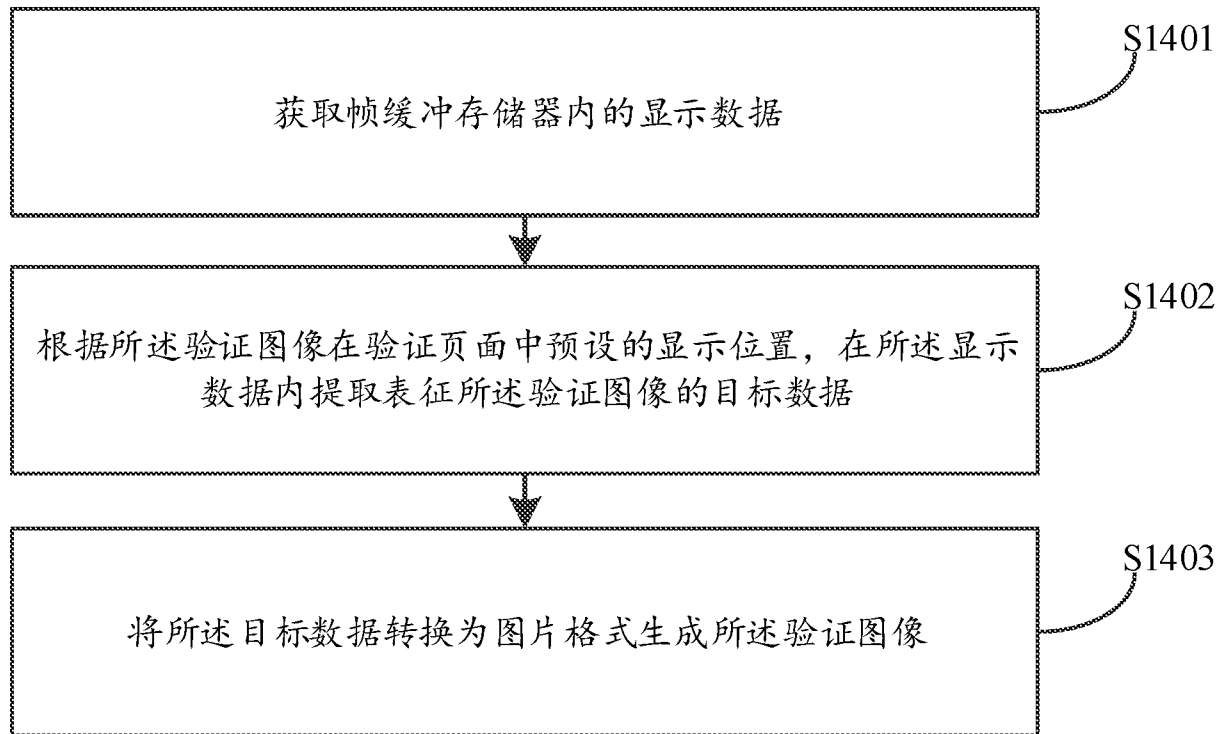


图 7

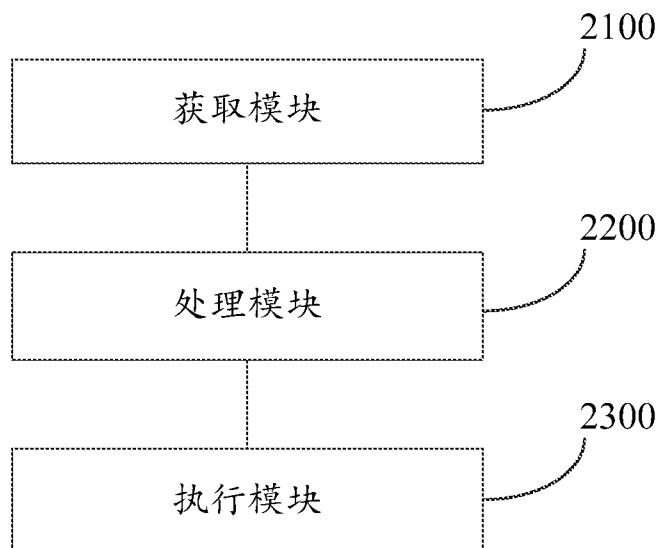


图 8

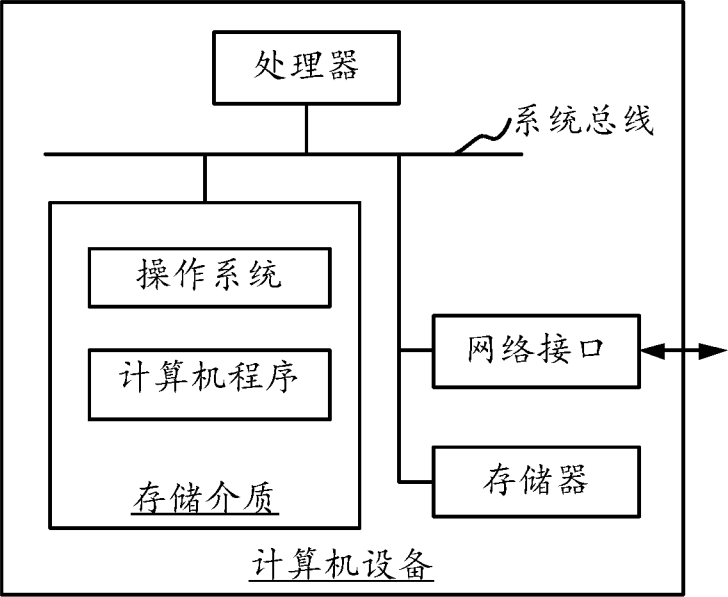


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/103664

A. CLASSIFICATION OF SUBJECT MATTER

G06T 3/00(2006.01)i; G06F 21/36(2013.01)i

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)

G06T G06F

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, CNKI, IEEE: 验证, 码, 图像, 图片, 字符, 背景, 风格, 种类, 类型, 类别, 转换, 转化, 迁移, verify, code, CAPTCHA, image, picture, character, background, style, type, category, transfer, transform, change

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 109918893 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 21 June 2019 (2019-06-21) description, paragraphs [0046]-[0110], and figure 2	1-3, 6-11, 14-17, 20
Y	CN 109918893 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 21 June 2019 (2019-06-21) description, paragraphs [0046]-[0110], and figure 2	4-5, 12-13, 18-19
Y	CN 108229130 A (CHINA UNIONPAY CO., LTD.) 29 June 2018 (2018-06-29) description, paragraphs [0009]-[0020]	4-5, 12-13, 18-19
A	CN 109711136 A (WUHAN JIYI NETWORK TECHNOLOGY CO., LTD.) 03 May 2019 (2019-05-03) entire document	1-20
A	CN 108846274 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 20 November 2018 (2018-11-20) entire document	1-20
A	US 2017310653 A1 (SONY CORPORATION) 26 October 2017 (2017-10-26) entire document	1-20



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

28 April 2020

Date of mailing of the international search report

22 May 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/103664

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109918893	A	21 June 2019	None			
CN	108229130	A	29 June 2018	None			
CN	109711136	A	03 May 2019	None			
CN	108846274	A	20 November 2018	None			
US	2017310653	A1	26 October 2017	CN	107306183	A	31 October 2017
				EP	3236403	A2	25 October 2017

国际检索报告

国际申请号

PCT/CN2019/103664

A. 主题的分类

G06T 3/00 (2006.01) i; G06F 21/36 (2013.01) i

按照国际专利分类(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)

G06T G06F

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, EPDOC, CNKI, IEEE: 验证, 码, 图像, 图片, 字符, 背景, 风格, 种类, 类型, 类别, 转换, 转化, 迁移, verify, code, CAPTCHA, image, picture, character, background, style, type, category, transfer, transform, change

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
X	CN 109918893 A (平安科技深圳有限公司) 2019年 6月 21日 (2019 - 06 - 21) 说明书[0046]-[0110]段, 图2	1-3, 6-11, 14-17, 20
Y	CN 109918893 A (平安科技深圳有限公司) 2019年 6月 21日 (2019 - 06 - 21) 说明书[0046]-[0110]段, 图2	4-5, 12-13, 18-19
Y	CN 108229130 A (中国银联股份有限公司) 2018年 6月 29日 (2018 - 06 - 29) 说明书[0009]-[0020]段	4-5, 12-13, 18-19
A	CN 109711136 A (武汉极意网络科技有限公司) 2019年 5月 3日 (2019 - 05 - 03) 全文	1-20
A	CN 108846274 A (腾讯科技深圳有限公司) 2018年 11月 20日 (2018 - 11 - 20) 全文	1-20
A	US 2017310653 A1 (SONY CORPORATION) 2017年 10月 26日 (2017 - 10 - 26) 全文	1-20

☐ 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(如具体说明的)

“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

2020年 4月 28日

国际检索报告邮寄日期

2020年 5月 22日

ISA/CN的名称和邮寄地址

中国国家知识产权局(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

授权官员

杨继爽

电话号码 86-(10)-53961357

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/103664

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	109918893	A	2019年 6月 21日	无	
CN	108229130	A	2018年 6月 29日	无	
CN	109711136	A	2019年 5月 3日	无	
CN	108846274	A	2018年 11月 20日	无	
US	2017310653	A1	2017年 10月 26日	CN 107306183 A	2017年 10月 31日
				EP 3236403 A2	2017年 10月 25日