

(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
2022 年 7 月 28 日 (28.07.2022)



(10) 国际公布号
WO 2022/156552 A1

(51) 国际专利分类号:
G06F 21/36 (2013.01) **G06F 21/60** (2013.01)

(21) 国际申请号: PCT/CN2022/071004

(22) 国际申请日: 2022 年 1 月 10 日 (10.01.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110069620.0 2021 年 1 月 19 日 (19.01.2021) CN

(71) 申请人: 北京嘀嘀无限科技发展有限公司 (BEIJING DIDI INFINITY TECHNOLOGY AND DEVELOPMENT CO., LTD.) [CN/CN]; 中国北京市海淀区东北旺路西路 8 号院 34 号楼, Beijing 100193 (CN)。

(72) 发明人: 汪昊(WANG, Hao); 中国北京市海淀区东北旺路西路 8 号院 34 号楼, Beijing 100193 (CN)。张天明(ZHANG, Tianming); 中国北京市海淀区东北旺路西路 8 号院 34 号楼, Beijing 100193 (CN)。王智恒(WANG, Zhiheng); 中国北京市海淀区东北旺路西路 8 号院 34 号楼, Beijing 100193 (CN)。周士奇(ZHOU, Shiqi); 中国北京市海淀区东北旺路西路 8 号院 34 号楼, Beijing 100193 (CN)。

(74) 代理人: 成都七星天知识产权代理有限公司 (METIS IP (CHENGDU) LLC); 中国四川省成都市中国 (四川) 自由贸易试验区成都市天府新区湖畔路北段 269 号 1 栋 1 单元 4 层 401 号, Sichuan 610213 (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,

(54) Title: METHOD FOR ENCRYPTING VERIFICATION CODE IMAGE, AND DEVICE, STORAGE MEDIUM AND COMPUTER PROGRAM PRODUCT

(54) 发明名称: 验证码图像加密方法、设备、存储介质和计算机程序产品

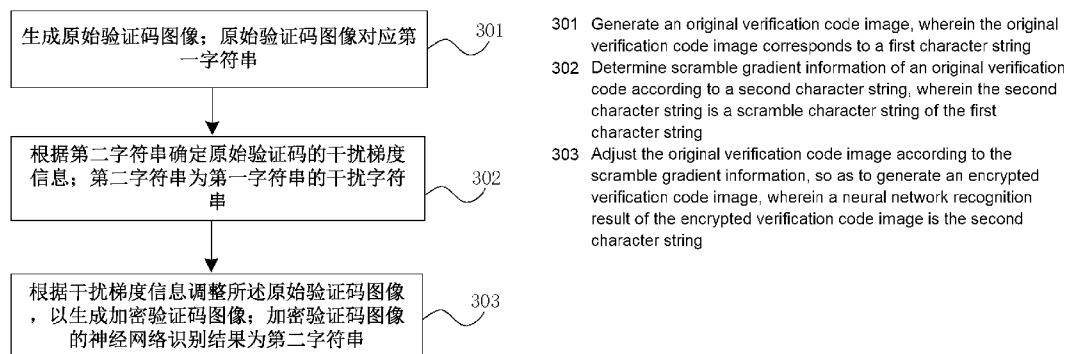


图 3

(57) Abstract: The embodiments of the present disclosure relate to a method for encrypting a verification code image, and a device, a storage medium and a computer program product. The method comprises: generating an original verification code image, wherein the original verification code image corresponds to a first character string; determining scramble gradient information of the original verification code image according to a second character string, wherein the scramble gradient information comprises an adjustment gradient of each pixel in the original verification code image, and the second character string is a scramble character string of the first character string; and adjusting the original verification code image according to the scramble gradient information, so as to generate an encrypted verification code image, wherein a neural network recognition result of the encrypted verification code image is the second character string. By using the method, the security of a verification code image can be improved, thereby effectively preventing malicious registration behavior.

(57) 摘要: 本公开实施例涉及一种验证码图像加密方法、设备、存储介质和计算机程序产品。所述方法包括: 生成原始验证码图像; 所述原始验证码图像对应第一字符串; 根据第二字符串确定所述原始验证码图像的干扰梯度信息; 所述干扰梯度信息包括所述原始验证码图像中每一个像素的调整梯度, 所述第二字符串为所述第一字符串的干扰字符串; 根据所述干扰梯度信息调整所述原始验证码图像, 以生成加密验证码图像; 所述加密验证码图像的神经网络识别结果为所述第二字符串。采用本方法可以提高验证码图像的安全性, 有效阻挡恶意注册行为。

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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, 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)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

验证码图像加密方法、设备、存储介质和计算机程序产品

交叉引用

[0001] 本申请要求于 2021 年 1 月 19 日提交的中国专利申请 No. 202110069620.0 的优先权，其全部内容通过引用结合于此。

技术领域

[0002] 本公开实施例涉及通信技术领域，特别是涉及一种验证码图像加密方法、设备、存储介质和计算机程序产品。

背景技术

[0003] 随着通信电子技术的飞速发展，智能手机得到了广泛应用。智能手机可以安装各种不同的应用程序（application，APP）向用户提供多样的互联网服务，用户注册或登陆 APP 时通常需要识别验证码图片中的字符，准确输入后验证码才能成功注册或登录。

[0004] 但是在实际应用中，恶意黑产往往可以攻破验证码图片，进行恶意注册，干扰企业的正常运营。即便在验证码图像上增加很多干扰图案，黑产仍然能够快速破解验证码，无法有效阻挡恶意注册行为。

发明内容

[0005] 本公开实施例提供一种验证码图像加密方法、设备、存储介质和计算机程序产品，可以提高验证码图像的安全性，有效阻挡恶意注册行为。

[0006] 第一方面，本公开实施例提供一种验证码图像加密方法，方法包括：

[0007] 生成原始验证码图像；原始验证码图像对应第一字符串；

[0008] 根据第二字符串确定原始验证码图像的干扰梯度信息；干扰梯度信息包括原始验证码图像中每一个像素的调整梯度，第二字符串为第一字符串的干扰字符串；

[0009] 根据干扰梯度信息调整原始验证码图像，以生成加密验证码图像；加密验证码图像的神经网络识别结果为第二字符串。

[0010] 第二方面，本公开实施例提供一种计算机设备，计算机设备包括：

[0011] 验证码图像生成单元，用于生成原始验证码图像；原始验证码图像对应第一字符串；

[0012] 干扰梯度信息生成单元，用于根据第二字符串确定原始验证码图像的干扰梯度信息；干扰梯度信息包括原始验证码图像中每一个像素的调整梯度，第二字符串为第一字符串的干扰字符串；

[0013] 加密单元，用于根据干扰梯度信息调整原始验证码图像，以生成加密验证码图像；加密验证码图像的神经网络识别结果为第二字符串。

[0014] 第三方面，本公开实施例提供一种服务器，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行计算机程序时实现上述第一方面的方法。

[0015] 第四方面，本公开实施例提供一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时实现上述第一方面的方法。

[0016] 第五方面，本公开实施例提供一种计算机程序产品，包括计算机程序，其特征在于，该计算机程序被处理器执行时实现上述第一方面所述的方法的步骤。

[0017] 本公开实施例提供的验证码图像加密方法、计算机设备和存储介质，生成原始验证码图像后，指定一个与原始验证码图像真实对应字符串相似的干扰字符串（例如，前文的第二字符串），还可以根据该干扰字符串确定干扰梯度信息调整原始验证码图像，以干扰攻击方神经网络模型的识别结果，提高验证码图像的安全性，有效抵抗恶意注册行为。

附图说明

[0018] 图1为本公开实施例提供的验证码图像加密方法的应用环境图；

[0019] 图2为本公开实施例提供的验证码图像应用示意图；

[0020] 图3为本公开实施例提供的验证码图像加密方法的流程示意图；

[0021] 图4为本公开实施例提供的确定干扰梯度信息的流程示意图；

[0022] 图5为本公开实施例提供的像素调整示意图；

[0023] 图6为本公开实施例提供的训练数据集的示意图；

[0024] 图7为本公开实施例提供的模型训练示意图；

[0025] 图8为本公开实施例提供的损失值梯度示意图；

[0026] 图 9 为本公开实施例提供的确定干扰梯度信息的迭代示意图；

[0027] 图 10 为本公开实施例提供的验证码图像加密过程示意图；

[0028] 图 11 为本公开实施例提供的加密效果示意图；

[0029] 图 12 为本公开实施例提供的计算机设备的结构框图；

[0030] 图 13 为本公开实施例提供的计算机设备的内部结构图。

具体实施方式

[0031] 为了使本公开实施例的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本公开实施例进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本公开实施例，并不用于限定本公开实施例。

[0032] 首先，在具体介绍本公开实施例的技术方案之前，先对本公开实施例基于的技术背景或者技术演进脉络进行介绍。通常情况下，用户注册或登陆 APP 时通常需要输入用户名、密码和验证码，以帮助服务器识别机器行为，从而阻挡基于机器行为的恶意注册。基于该背景，申请人发现即使使用在验证码图像增加大量干扰元素，也无法抵抗恶意注册行为。攻击方还是可以利用神经网络学习算法识别出验证码图像中的字符，进行恶意注册。此外，在验证码图像中添加过多的干扰元素可能导致用户无法辨认出验证码中的文字，影响用户注册成功率。可见，如何抵抗恶意注册行为，成为目前亟待解决的难题。为解决这一问题，申请人付出了大量的创造性劳动，提出了下述实施例介绍的技术方案。

[0033] 下面结合本公开实施例所应用的场景，对本公开实施例涉及的技术方案进行介绍。

[0034] 本公开实施例提供的验证码图像加密方法，可以应用于如图 1 所示的应用环境中。其中，电子设备 10 通过网络与服务器 20 进行通信。电子设备可以安装 APP 向用户提供各种互联网服务，例如，提供网约车服务、网上购物服务等。服务器 20 可以是 APP 的应用服务器，用于支持 APP 所提供服务的后台实现。

[0035] 具体实现中，电子设备 10 可以但不限于各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备，服务器 20 可以用独立的

服务器或者是多个服务器组成的服务器集群来实现。

[0036] 参考图 2，用户在 APP 或网页进行注册时，可以通过电子设备 10 输入用户名、密码后，还需要识别验证码图像中的验证码，根据识别结果输入验证码。电子设备 10 可以向服务器 20 发送用户输入的用户名、密码和验证码，服务器 20 可以根据接收到的用户名、密码和验证码完成用户注册。

[0037] 目前，攻击方可以利用神经网络模型识别验证码图像，进行恶意注册。为了提高验证码图像的安全性，有效抵抗恶意注册行为，本公开实施例提供一种验证码图像加密方法。所述方法适用于图 1 所示系统，执行主体可以是图 1 所示系统中的服务器 20。如图 3 所示，所述方法包括以下步骤：

[0038] 步骤 301、生成原始验证码图像；原始验证码图像对应第一字符串。

[0039] 具体实现中，服务器可以在空白图像上添加字符串来生成验证码图像，还可以在验证码图像上添加干扰。验证码图像中的字符可以是任意数字、任意字母，也可以是数字和字母的组合，本公开实施例对此不做限制。

[0040] 示例性的，根据第一字符串生成原始验证码图像，第一字符串为原始验证码图像对应的字符串，即人眼识别原始验证码图像的结果为第一字符串。第一字符串包括数字、字母。

[0041] 步骤 302、根据第二字符串确定原始验证码的干扰梯度信息；第二字符串为第一字符串的干扰字符串。

[0042] 需要说明的是，改变验证码图像中各个像素的值可能影响神经模型对验证码图像的识别结果，黑产攻击方通常使用神经网络模型识别验证码图像中的字符，为了干扰黑产攻击方的对验证码图像的识别，可以对原始验证码图像中各个像素的值进行调整。

[0043] 本公开实施例中，干扰梯度信息包括原始验证码图像中每一个像素的调整梯度，调整梯度用于指示像素值的调整幅度。示例性的，可以是像素值的调整数值。利用干扰梯度信息调整原始验证码图像的像素，以干扰神经网络模型的识别结果。具体地，可以指定一个干扰字符串，根据该干扰字符串确定干扰梯度信息，利用干扰梯度信息处理原始验证码图像，使得神经网络模型对原始验证码图像的识别结果为干扰字符串。其中，干扰字符串可以是与原始验证码图像真实对应的字符串相似的字符串，与原始

验证码图像真实对应的字符串不完全相同，其中某些字符相似度较高。

[0044] 示例性的，在对包含第一字符串的原始验证码图像进行加密时，可以根据与第一字符串相似的第二字符串确定干扰梯度信息，以干扰神经网络模型的识别结果。例如，第一字符串、第二字符串均包括 N 个字符，第一字符串的前 (N-1) 个字符与第二字符串的前 (N-1) 个字符相同，第一字符串的第 N 个字符与第二字符串的第 N 个字符相似。例如，第一字符串为“32E8”，用于干扰的第二字符串为“32E3”。

[0045] 步骤 303、根据干扰梯度信息调整所述原始验证码图像，以生成加密验证码图像；加密验证码图像的神经网络识别结果为第二字符串。

[0046] 具体实现中，针对原始验证码图像中的每一个像素，根据干扰梯度信息中该像素的调整梯度调整所述像素的值，调整后的图像为加密验证码图像。

[0047] 示例性的，以下表 1 为本公开实施例提供的干扰梯度信息的一种可能实现，假设原始验证图像包括的像素为 a1~a9，其中，a1~a9 的像素值的调整梯度为 $\nabla 1$ 、 $\nabla 2$ 、 $\nabla 3$ 、 $\nabla 4$ 、 $\nabla 5$ 、 $\nabla 6$ 、 $\nabla 7$ 、 $\nabla 8$ 、 $\nabla 9$ 。

表 1

像素 信息	a1	a2	a3	a4	a5	a6	a7	a8	a9
调整 梯度	$\nabla 1$	$\nabla 2$	$\nabla 3$	$\nabla 4$	$\nabla 5$	$\nabla 6$	$\nabla 7$	$\nabla 8$	$\nabla 9$

[0048] a1~a9 的排列 $\nabla 1$ a1 的值进行调整，根据 $\nabla 2$ a2 的值进行调整，以此类推，获得加密后的验证码图像。

[0049] 需要说明的是，加密验证码图像中各个像素的值较原始验证码有所改变，这会导致神经网络模型对加密验证码图像的识别结果不再是第一字符串，而是第二字符串，由此实现对黑产攻击方的干扰，提高验证码图像的安全性，有效抵抗恶意注册行为。

[0050] 此外，针对原始验证码图像中各个像素的调整梯度往往较小，因此通过干扰梯度信息改变原始验证码图像中各个像素的值对原始验证码图像的视觉效果影响不大，因此不会对用户识别造成明显的干扰。

[0051] 一种可能的实现方式中，为了避免通过干扰梯度信息改变原始验证码图像的边缘后对用户识别造成干扰，加密验证码图像和原始验证码图像的视觉识别结果相同。具体地，干扰梯度信息中的调整梯度的绝对值往往较小，可以保证加密验证码图像和原始验证码图像在视觉上不会存在明显差别，二者的视觉识别结果相同。

[0052] 图 3 所示的方法中，生成原始验证码图像后，指定一个与原始验证码图像真实对应字符串相似的字符串，还可以根据该字符串确定干扰梯度信息调整原始验证码图像，以干扰攻击方神经网络模型的识别结果，提高验证码图像的安全性，有效抵抗恶意注册行为。

[0053] 本公开实施例中，服务器 20 还可以根据神经网络模型的识别结果与干扰字符串的差异来确定最终用于加密的干扰梯度信息。参考图 5，具体包括以下步骤：

[0054] 步骤 501、训练神经网络模型，该神经网络模型用于识别验证码图像。

[0055] 需要说明的是，上述神经网络模型还可以称为验证码图像识别模型，用于识别验证码图像，其输入可以是验证码图像，输出为验证码（例如，字符串）。示例性的，用于训练验证码图像识别模型的样本数据集包括验证码图像和验证码图像的标签，其中，验证码图像的标签可以是验证码图像包括的字符串。示例的，参考图 6，验证码图像 1 对应的标签为“32E8”，验证码图像 2 对应的标签为“Trdk”。

[0056] 一种可能的实现方式中，服务器在生成验证码图像（例如，前文所述的原始验证码图像）时，还可以生成标签信息，标签信息用于记录验证码图像与字符串的对应关系。在训练验证码图像识别模型时，可以根据标签信息获取大量的训练样本。

[0057] 具体实现中，参考图 7，将验证码图像输入初始的神经网络模型，将神经网络模型的输出（识别结果）与真实标签进行比较，获得损失值 Loss。损失值 Loss 用于表征神经网络模型的输出相比于真实标签的差异。还可以以最小化 Loss 为优化目标，对神经网络模型的参数进行更新。当损失值

Loss 取得最小值，获得稳定的验证码图像识别模型。

[0058] 步骤 502、根据神经网络模型对原始验证码图像的识别结果与第二字符串的差异确定干扰梯度信息。

[0059] 其中，确定干扰梯度信息需要满足的准则是：利用干扰梯度信息和原始验证码图像生成的加密验证码图像的神经网络识别结果为第二字符串。

[0060] 具体实现中，根据神经网络模型对原始验证码图像的识别结果与第二字符串的差异确定干扰梯度信息，具体包括以下步骤：

[0061] S1、将原始验证码图像输入上述神经网络模型模型，确定第二字符串相比于神经网络模型的输出的损失值。

[0062] 其中，损失值用于表征第二字符串相比于神经网络模型的输出的差异。

[0063] S2、根据上述损失值确定梯度信息，包括原始验证码图像中每一个像素的调整梯度。

[0064] 需要说明的是，损失值可以表征第二字符串相比于神经网络模型的输出的差异，神经网络模型的输出为神经网络模型对原始验证码图像的识别结果，为了保证神经网络模型对原始验证码图像的识别结果更接近第二字符串，可以根据上述损失值来确定梯度信息。一种可能的实现方式中，神经网络模型的输入可以认为是原始验证码图像包括的所有像素，对损失值求导可以获得每一个像素的调整梯度。

[0065] S3、利用上述梯度信息更新原始验证码图像，直至上述损失值取得最小值，确定当前的梯度信息为干扰梯度信息。

[0066] 具体实现中，针对原始验证码图像中的每一个像素，根据上述梯度信息中与该像素对应的调整梯度，对该像素的值进行调整。当对原始验证码图像中各个像素的值逐一进行调整后，完成了对原始验证码图像的更新。

[0067] 需要说明的是，输入验证图像码识别模型的图像发生变化，验证码图像识别模型的输出结果也会发生变化，第二字符串相比于验证码图像识别模型的输出结果的损失值也会发生变化。为了使得神经网络模型对调整像素后的原始验证码图像的识别结果尽可能接近第二字符串，可以不断地迭代更新梯度信息，以更新原始验证码图像，直至上述损失值取得最小值。将使得上述损失值取得最小值的梯度信息确定为最终用于生成加密验证码

图像的干扰梯度信息。

[0068] 一种可能的实现方式中，利用梯度信息中的调整梯度对原始验证码中各个像素的值进行调整，将调整后的图像输入神经网络模型，如果神经网络模型对输入图像的识别结果为上述第二字符串，则确定损失值取得最小值。本公开实施例中，确定干扰梯度信息的过程中对神经网络模型的参数不做调整，调整神经网络模型的输入，随着输入的变化，神经网络模型的输出与指定标签（例如前文所述的第二字符串）之间的损失值也会发生变化。当神经网络模型对输入图像的识别结果为上述第二字符串，神经网络模型的输出与指定标签之间的损失值最小。

[0069] 示例性的，图 8 为损失值的示意图。参考图 8，随着神经网络输入的改变，神经网络的输出与指定标签（例如，第二字符串）的损失值也会随之变化。当神经网络的输出为指定标签，神经网络模型的输出与指定标签之间的损失值最小。

[0070] 示例性的，参考图 9，将包括验证码“32E3”的原始验证码图像输入神经网络模型，计算神经网络模型的输出结果 1 和干扰字符串“32E8”（即前文所述的第二字符串）的损失值 Loss1，根据损失值 Loss1 确定梯度信息 1，包括原始验证码图像中各个像素的值的调整梯度。根据梯度信息 1 对原始验证码图像进行更新。

[0071] 将更新后的验证码图像输入神经网络模型，如果神经网络模型的输出不是“32E8”，则继续迭代，根据当前的损失值确定新的梯度信息对原始验证码图像进行调整后输入神经网络模型，直至神经网络的输出为“32E8”。

[0072] 示例性的，参考图 9，根据梯度信息 1 对原始验证码图像进行更新后输入神经网络模型，神经网络模型的输出为输出结果 2。计算神经网络模型的输出结果 2 和干扰字符串“32E8”的损失值 Loss2，根据损失值 Loss2 确定梯度信息 2，包括原始验证码图像中各个像素的值的调整梯度。

[0073] 根据梯度信息 2 对原始验证码图像进行更新后输入神经网络模型，神经网络模型的输出为“32E8”，即损失值取得最小值。可以将梯度信息 2 确定为干扰梯度信息，利用干扰梯度信息对原始验证码图像进行处理，获得加密验证码图像。

[0074] 本公开图 5 所示的实施例中，利用梯度信息更新原始验证码图像，为了保证神经网络模型对更新后的原始验证码图像的识别结果尽可能靠近干扰字符串，可以将最小化神经网络对作为优化目标迭代梯度信息。在此过程中，识别网络的参数是保持不变的，仅对梯度信息做调整。

[0075] 示例的，参考图 10，利用干扰梯度信息调整“原始验证码图像 32E3”中各个像素的值，生成加密验证码图像。加密验证码图像人眼看上去仍然是字符“32E3”，但采用深度学习方法对其识别，识别结果就是“32E8”，这就导致攻击方的自动识别算法识别错误，从而达到加密的效果。

[0076] 示例性的，参考图 11，服务器生成的原始验证码图像包括“32E3”，利用“32E8”确定干扰梯度信息，例如干扰梯度信息调整原始验证码图像中各个像素的值，生成加密验证码图像，向电子设备发送加密验证码图像的图像信息。电子设备显示的是加密验证码图像，用户可以准确识别验证码“32E3”，准确输入验证码“32E3”。但如果当前注册行为是黑产的注册行为，黑产所使用神经网络模型（例如，前文所述的验证码图像模型）无法识别真实的验证码“32E3”，对验证码图像的识别结果为“32E8”，黑产控制点击器输入的验证码为“32E8”，无法成功注册，可见本公开能够有效阻挡恶意注册行为。

[0077] 应该理解的是，虽然图 3、图 5 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，这些步骤可以以其它的顺序执行。而且，图 3、图 5 的至少一部分步骤可以包括多个步骤或者多个阶段，这些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，这些步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

[0078] 本公开实施例提供了一种计算机设备，可以是本公开实施例所述的服务器。如图 11 所示，该计算机设备包括：验证码图像生成单元 1201、梯度信息生成单元 1202 以及加密单元 1203。

[0079] 验证码图像生成单元 1201，用于生成原始验证码图像；原始验证码图像对应第一字符串；

[0080] 干扰梯度信息生成单元 1202，用于根据第二字符串确定原始验证码图像的干扰梯度信息；干扰梯度信息包括原始验证码图像中每一个像素的调整梯度，第二字符串为第一字符串的干扰字符串；

[0081] 加密单元 1203，用于根据干扰梯度信息调整原始验证码图像，以生成加密验证码图像；加密验证码图像的神经网络识别结果为第二字符串。

[0082] 一种可能的实现方式中，干扰梯度信息生成单元 1202 用于，根据神经网络模型对原始验证码图像的识别结果与第二字符串的差异确定干扰梯度信息，使得根据干扰梯度信息和原始验证码图像生成的加密验证码图像的神经网络识别结果为第二字符串；神经网络模型的输入为验证码图像，输出为字符串。

[0083] 一种可能的实现方式中，干扰梯度信息生成单元 1202 具体用于，将原始验证码图像输入神经网络模型，确定第二字符串相比于神经网络模型的输出的损失值；

[0084] 根据损失值确定梯度信息，梯度信息包括原始验证码图像中每一个像素的调整梯度；

[0085] 利用梯度信息更新原始验证码图像，直至损失值取得最小值，确定当前的梯度信息为干扰梯度信息。

[0086] 一种可能的实现方式中，干扰梯度信息生成单元 1202 用于，针对原始验证码图像中的每一个像素，根据梯度信息中像素的调整梯度调整像素的值，以对原始验证码图像进行更新。

[0087] 一种可能的实现方式中，加密单元 1203 具体用于，针对原始验证码图像中的每一个像素，根据干扰梯度信息中像素的调整梯度调整像素的值，调整后的图像为加密验证码图像。

[0088] 一种可能的实现方式中，干扰梯度信息中的调整梯度用于保证加密验证码图像和原始验证码图像视觉识别结果相同。

[0089] 关于上述计算机设备的具体限定可以参见上文中对于验证码图像加密方法的限定，在此不再赘述。上述计算机设备中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于电子设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[0090] 图 13 是根据一示例性实施例示出的一种服务器 1300 的框图。参照图 13, 服务器 1300 包括处理组件 1320, 其进一步包括一个或多个处理器, 以及由存储器 1322 所代表的存储器资源, 用于存储可由处理组件 1320 执行的指令或者计算机程序, 例如应用程序。存储器 1322 中存储的应用程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外, 处理组件 1320 被配置为执行指令, 以执行上述验证码图像加密方法。

[0091] 服务器 1300 还可以包括一个电源组件 1324 被配置为执行设备 1300 的电源管理, 一个有线或无线网络接口 1326 被配置为将设备 1300 连接到网络, 和一个输入输出 (I/O) 接口 1328。服务器 1300 可以操作基于存储在存储器 1322 的操作系统, 例如 Window13 13erverTM, Mac O13 XTM, UnixTM, LinuxTM, FreeB13DTM 或类似。

[0092] 本公开实施例还提供了一种包括指令的非临时性计算机可读存储介质, 例如包括指令的存储器, 上述指令可由计算机设备 (例如, 前文所述的服务器) 的处理器执行以完成上述方法。例如, 所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器 (RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0093] 本公开实施例还提供了一种包括指令的存储介质, 例如包括指令的存储器, 上述指令可由服务器的处理器执行以完成上述方法。存储介质可以是非临时性计算机可读存储介质, 例如, 所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器 (RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0094] 在示例性实施例中, 还提供了一种计算机程序产品, 该计算机程序被处理器执行时, 可以实现上述方法。该计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行这些计算机指令时, 可以全部或部分地按照本公开实施例所述的流程或功能实现上述方法中的部分或者全部。

[0095] 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, 所述的计算机程序可存储于一非易失性计算机可读取存储介质中, 该计算机程序在执行时, 可包括如上述各方法的实施例的流程。其中, 本公开实施例所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用, 均可包

括非易失性和易失性存储器中的至少一种。非易失性存储器可包括只读存储器（Read-Only Memory, ROM）、磁带、软盘、闪存或光存储器等。易失性存储器可包括随机存取存储器（Random Access Memory, RAM）或外部高速缓冲存储器。作为说明而非局限，RAM可以是多种形式，比如静态随机存取存储器（Static Random Access Memory, SRAM）或动态随机存取存储器（Dynamic Random Access Memory, DRAM）等。

[0096] 以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0097] 以上所述实施例仅表达了本公开实施例的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本公开实施例构思的前提下，还可以做出若干变形和改进，这些都属于本公开实施例的保护范围。因此，本公开实施例专利的保护范围应以所附权利要求为准。

权利要求书

1、一种验证码图像加密方法，其特征在于，所述方法包括：

生成原始验证码图像；所述原始验证码图像对应第一字符串；

根据第二字符串确定所述原始验证码图像的干扰梯度信息；所述干扰梯度信息包括所述原始验证码图像中每一个像素的调整梯度，所述第二字符串为所述第一字符串的干扰字符串；

根据所述干扰梯度信息调整所述原始验证码图像，以生成加密验证码图像；所述加密验证码图像的神经网络识别结果为所述第二字符串。

2、根据权利要求1所述的方法，其特征在于，所述根据第二字符串确定所述原始验证码的干扰梯度信息，包括：

根据神经网络模型对所述原始验证码图像的识别结果与所述第二字符串的差异确定所述干扰梯度信息，使得根据所述干扰梯度信息和所述原始验证码图像生成的加密验证码图像的神经网络识别结果为所述第二字符串；所述神经网络模型的输入为验证码图像，输出为字符串。

3、根据权利要求2所述的方法，其特征在于，所述根据神经网络模型对所述原始验证码图像的识别结果与所述第二字符串的差异确定所述干扰梯度信息，包括：

将所述原始验证码图像输入所述神经网络模型，确定所述第二字符串相比于所述神经网络模型的输出的损失值；

根据所述损失值确定梯度信息，所述梯度信息包括所述原始验证码图像中每一个像素的调整梯度；

利用所述梯度信息更新所述原始验证码图像，直至所述损失值取得最小值，确定当前的梯度信息为所述干扰梯度信息。

4、根据权利要求3所述的方法，其特征在于，所述利用所述梯度

信息更新所述原始验证码图像，包括：

针对所述原始验证码图像中的每一个像素，根据所述梯度信息中所述像素的调整梯度调整所述像素的值，以对所述原始验证码图像进行更新。

5、根据权利要求 1-4 任一项所述的方法，其特征在于，所述根据所述干扰梯度信息调整所述原始验证码图像，以生成加密验证码图像，包括：

针对所述原始验证码图像中的每一个像素，根据所述干扰梯度信息中所述像素的调整梯度调整所述像素的值，调整后的图像为所述加密验证码图像。

6、根据权利要求 1-4 任一项所述的方法，其特征在于，所述干扰梯度信息中的调整梯度用于保证所述加密验证码图像和所述原始验证码图像视觉识别结果相同。

7、一种计算机设备，其特征在于，包括：

验证码图像生成单元，用于生成原始验证码图像；所述原始验证码图像对应第一字符串；

干扰梯度信息生成单元，用于根据第二字符串确定所述原始验证码图像的干扰梯度信息；所述干扰梯度信息包括所述原始验证码图像中每一个像素的调整梯度，所述第二字符串为所述第一字符串的干扰字符串；

加密单元，用于根据所述干扰梯度信息调整所述原始验证码图像，以生成加密验证码图像；所述加密验证码图像的神经网络识别结果为所述第二字符串。

8、根据权利要求 7 所述的计算机设备，其特征在于，所述干扰梯度信息生成单元用于，根据神经网络模型对所述原始验证码图像的识别结果与所述第二字符串的差异确定所述干扰梯度信息，使得根据所

述干扰梯度信息和所述原始验证码图像生成的加密验证码图像的神经网络识别结果为所述第二字符串；所述神经网络模型的输入为验证码图像，输出为字符串。

9、根据权利要求8所述的计算机设备，其特征在于，所述干扰梯度信息生成单元具体用于，将所述原始验证码图像输入所述神经网络模型，确定所述第二字符串相比于所述神经网络模型的输出的损失值；

根据所述损失值确定梯度信息，所述梯度信息包括所述原始验证码图像中每一个像素的调整梯度；

利用所述梯度信息更新所述原始验证码图像，直至所述损失值取得最小值，确定当前的梯度信息为所述干扰梯度信息。

10、根据权利要求9所述的计算机设备，其特征在于，所述干扰梯度信息生成单元用于，针对所述原始验证码图像中的每一个像素，根据所述梯度信息中所述像素的调整梯度调整所述像素的值，以对所述原始验证码图像进行更新。

11、根据权利要求7-10任一项所述的计算机设备，其特征在于，所述加密单元具体用于，针对所述原始验证码图像中的每一个像素，根据所述干扰梯度信息中所述像素的调整梯度调整所述像素的值，调整后的图像为所述加密验证码图像。

12、根据权利要求7-10任一项所述的计算机设备，其特征在于，所述干扰梯度信息中的调整梯度用于保证所述加密验证码图像和所述原始验证码图像视觉识别结果相同。

13、一种服务器，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至6中任一项所述的方法的步骤。

14、一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求 1-6 中任一项所述的方法的步骤。

15、一种计算机程序产品，包括计算机程序，其特征在于，该计算机程序被处理器执行时实现权利要求 1-6 中任一项所述的方法的步骤。

1/7

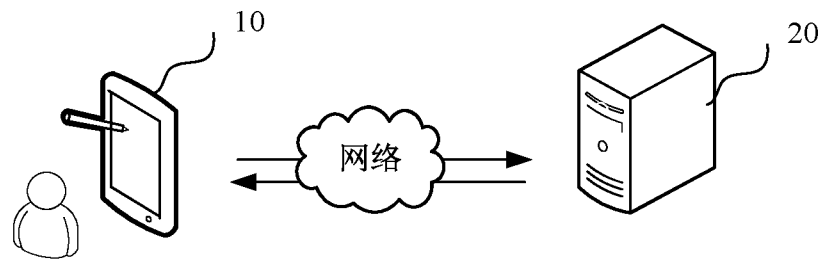


图 1

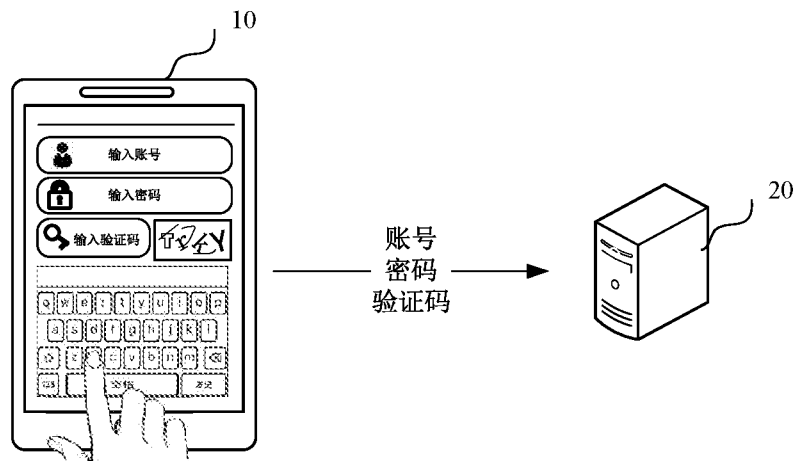


图 2

2/7

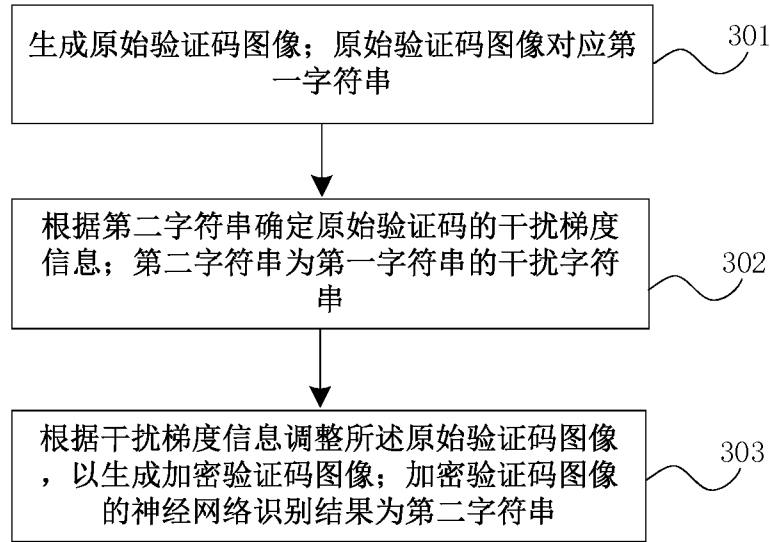


图 3

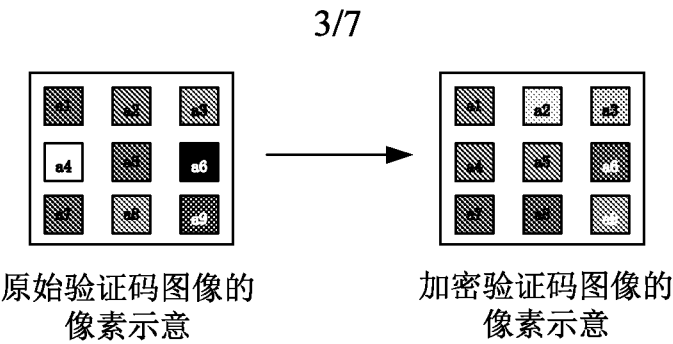


图 4

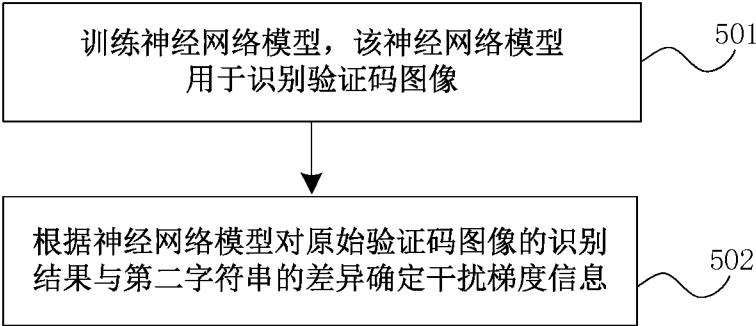


图 5

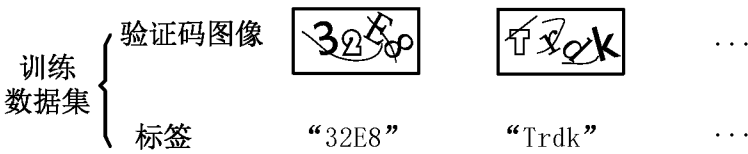


图 6

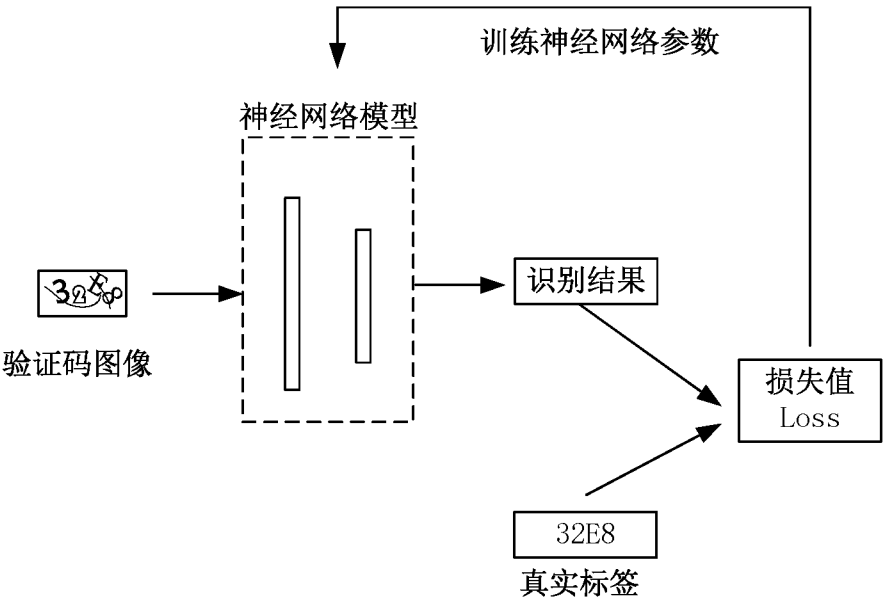


图 7

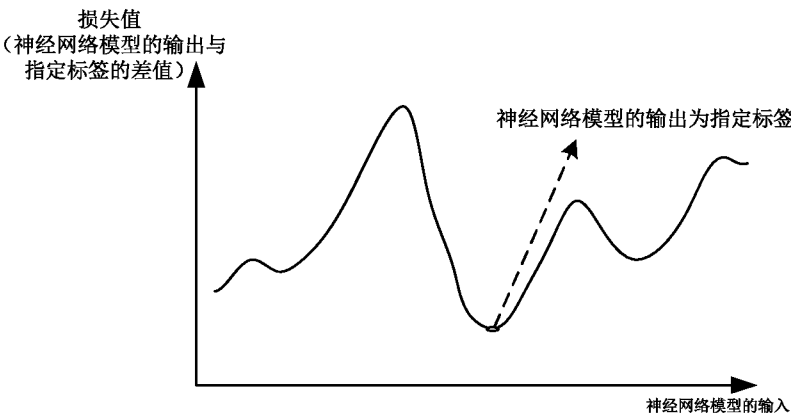


图 8

5/7

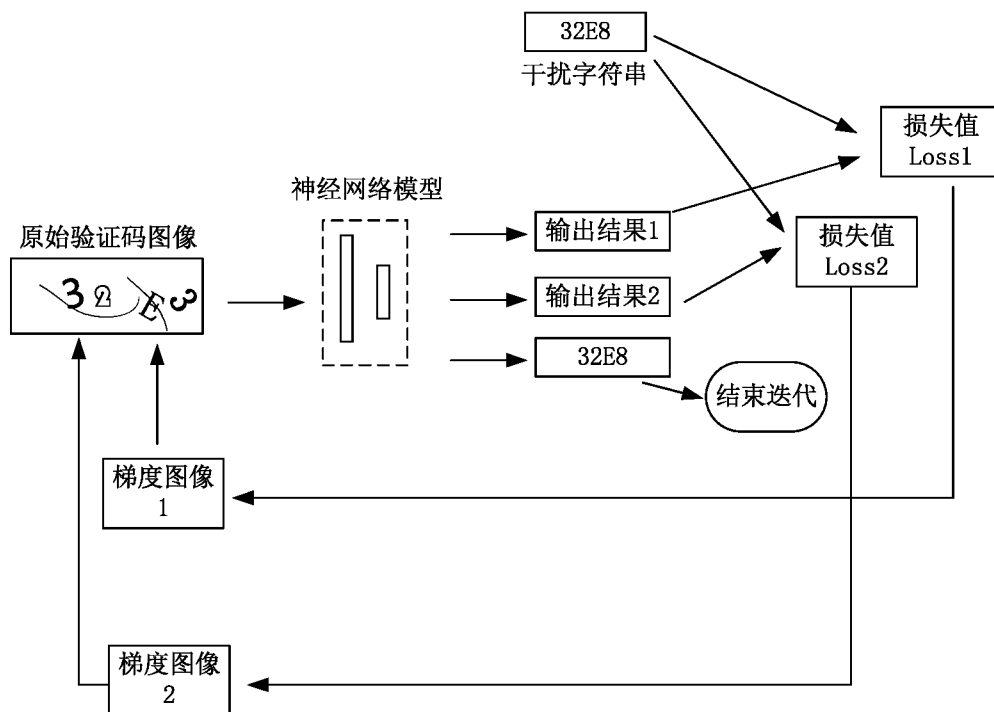


图 9

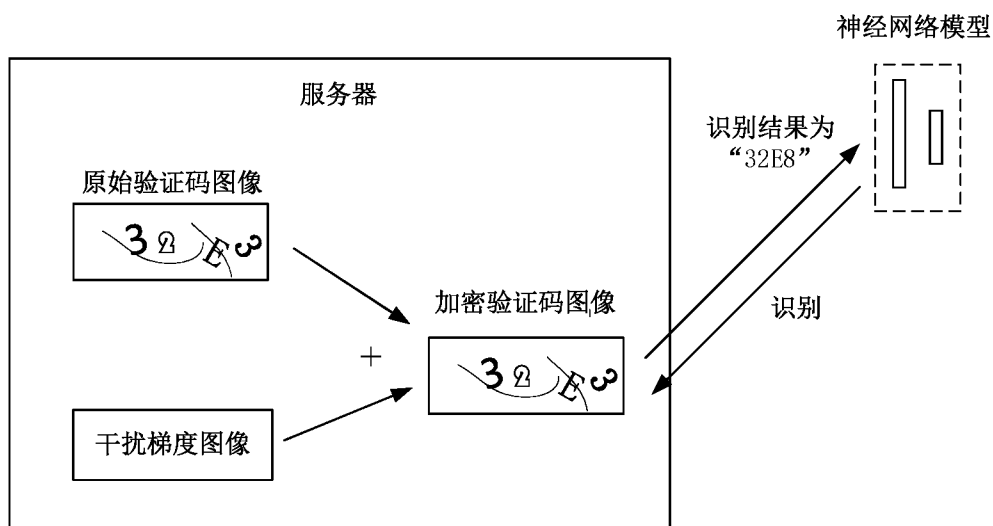


图 10

6/7

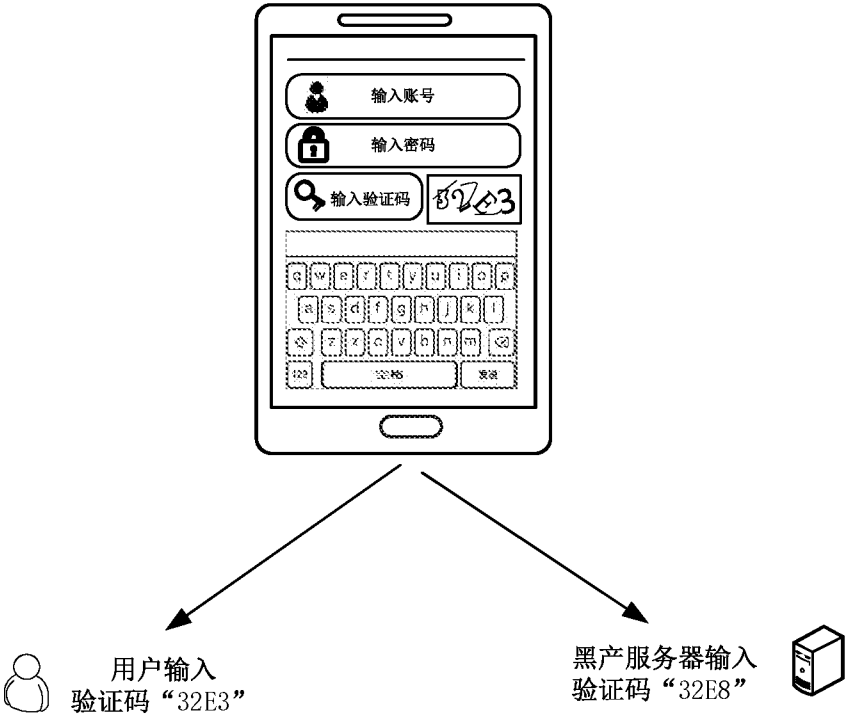


图 11

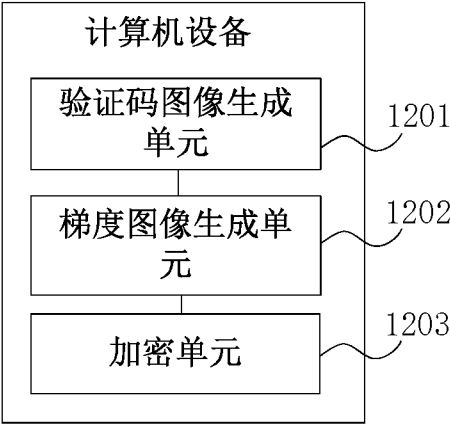


图 12

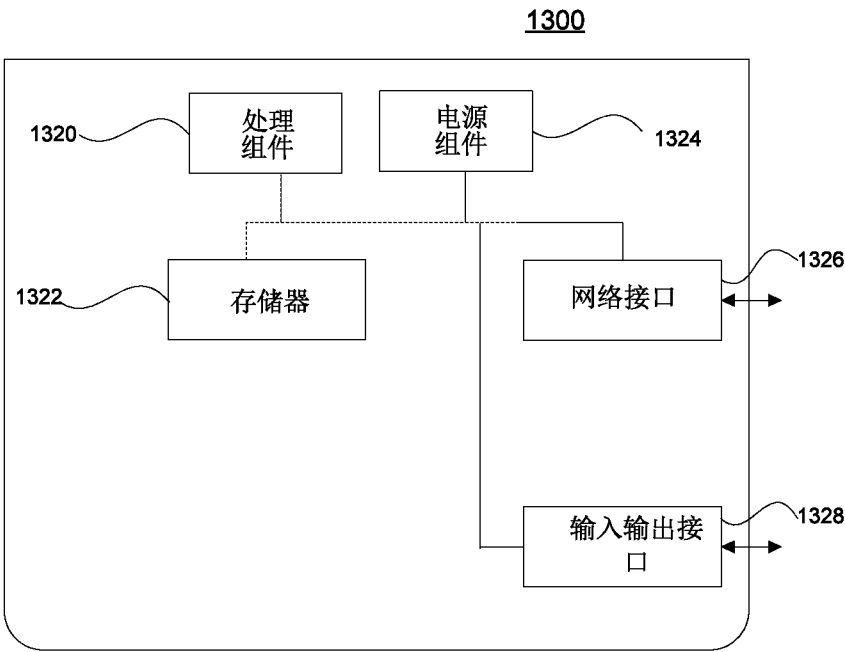


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/071004

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/36(2013.01)i; G06F 21/60(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)

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)

CNABS; CNTXT; CNKI; SIPOABS; DWPI; USTXT; WOTXT; EPTXT: 验证码, 图像, 字符串, 梯度, 损失, 神经网络, 识别, 干扰, 更新, 差, verification code, image, string, gradient, loss, neural network, recognition, interference, update, difference

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 111967592 A (THE 36TH RESEARCH INSTITUTE OF CETC et al.) 20 November 2020 (2020-11-20) description, paragraphs [0006]-[0079], and figure 4	1-15
X	CN 110895691 A (ALIBABA GROUP HOLDING LIMITED) 20 March 2020 (2020-03-20) description, paragraphs [0046]-[0111]	1-15
A	CN 109977980 A (AISINO CORPORATION INC.) 05 July 2019 (2019-07-05) entire document	1-15
A	CN 110555298 A (ALIBABA (CHINA) CO., LTD.) 10 December 2019 (2019-12-10) entire document	1-15
A	CN 109523611 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 26 March 2019 (2019-03-26) entire document	1-15
A	CN 111783064 A (PING AN INTERNATIONAL SMART CITY TECHNOLOGY CO., LTD.) 16 October 2020 (2020-10-16) entire document	1-15



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

14 March 2022

Date of mailing of the international search report

25 March 2022

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/CN2022/071004

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	111967592	A	20 November 2020	None	
CN	110895691	A	20 March 2020	None	
CN	109977980	A	05 July 2019	None	
CN	110555298	A	10 December 2019	CN 110555298	B 26 October 2021
CN	109523611	A	26 March 2019	None	
CN	111783064	A	16 October 2020	None	

国际检索报告

国际申请号

PCT/CN2022/071004

A. 主题的分类 G06F 21/36(2013.01)i; G06F 21/60(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) 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)) CNABS;CNTXT;CNKI;SIPOABS;DWPI;USTXT;WOTXT;EPTXT: 验证码, 图像, 字符串, 梯度, 损失, 神经网络, 识别, 干扰, 更新, 差, verification code, image, string, gradient, loss, neural network, recognition, interference, update, difference																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 111967592 A (中国电子科技集团公司第三十六研究所 等) 2020年11月20日 (2020 - 11 - 20) 说明书第[0006]-[0079]段、图4</td> <td>1-15</td> </tr> <tr> <td>X</td> <td>CN 110895691 A (阿里巴巴集团控股有限公司) 2020年3月20日 (2020 - 03 - 20) 说明书第[0046]-[0111]段</td> <td>1-15</td> </tr> <tr> <td>A</td> <td>CN 109977980 A (航天信息股份有限公司) 2019年7月5日 (2019 - 07 - 05) 全文</td> <td>1-15</td> </tr> <tr> <td>A</td> <td>CN 110555298 A (阿里巴巴中国有限公司) 2019年12月10日 (2019 - 12 - 10) 全文</td> <td>1-15</td> </tr> <tr> <td>A</td> <td>CN 109523611 A (百度在线网络技术北京有限公司) 2019年3月26日 (2019 - 03 - 26) 全文</td> <td>1-15</td> </tr> <tr> <td>A</td> <td>CN 111783064 A (平安国际智慧城市科技股份有限公司) 2020年10月16日 (2020 - 10 - 16) 全文</td> <td>1-15</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 111967592 A (中国电子科技集团公司第三十六研究所 等) 2020年11月20日 (2020 - 11 - 20) 说明书第[0006]-[0079]段、图4	1-15	X	CN 110895691 A (阿里巴巴集团控股有限公司) 2020年3月20日 (2020 - 03 - 20) 说明书第[0046]-[0111]段	1-15	A	CN 109977980 A (航天信息股份有限公司) 2019年7月5日 (2019 - 07 - 05) 全文	1-15	A	CN 110555298 A (阿里巴巴中国有限公司) 2019年12月10日 (2019 - 12 - 10) 全文	1-15	A	CN 109523611 A (百度在线网络技术北京有限公司) 2019年3月26日 (2019 - 03 - 26) 全文	1-15	A	CN 111783064 A (平安国际智慧城市科技股份有限公司) 2020年10月16日 (2020 - 10 - 16) 全文	1-15
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
X	CN 111967592 A (中国电子科技集团公司第三十六研究所 等) 2020年11月20日 (2020 - 11 - 20) 说明书第[0006]-[0079]段、图4	1-15																					
X	CN 110895691 A (阿里巴巴集团控股有限公司) 2020年3月20日 (2020 - 03 - 20) 说明书第[0046]-[0111]段	1-15																					
A	CN 109977980 A (航天信息股份有限公司) 2019年7月5日 (2019 - 07 - 05) 全文	1-15																					
A	CN 110555298 A (阿里巴巴中国有限公司) 2019年12月10日 (2019 - 12 - 10) 全文	1-15																					
A	CN 109523611 A (百度在线网络技术北京有限公司) 2019年3月26日 (2019 - 03 - 26) 全文	1-15																					
A	CN 111783064 A (平安国际智慧城市科技股份有限公司) 2020年10月16日 (2020 - 10 - 16) 全文	1-15																					
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																							
<table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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																			
* 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		国际检索报告邮寄日期																					
2022年3月14日		2022年3月25日																					
ISA/CN的名称和邮寄地址		受权官员																					
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		石蒙蒙 电话号码 (86-512) 88995856																					

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/071004

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	111967592	A	2020年11月20日	无	
CN	110895691	A	2020年3月20日	无	
CN	109977980	A	2019年7月5日	无	
CN	110555298	A	2019年12月10日	CN 110555298	B 2021年10月26日
CN	109523611	A	2019年3月26日	无	
CN	111783064	A	2020年10月16日	无	