



(12)发明专利申请

(10)申请公布号 CN 109523611 A

(43)申请公布日 2019. 03. 26

(21)申请号 201811433488.1

(22)申请日 2018.11.28

(71)申请人 百度在线网络技术(北京)有限公司

地址 100085 北京市海淀区上地十街10号

百度大厦三层

(72)发明人 王洋 刘焱 郝新

(74)专利代理机构 北京英赛嘉华知识产权代理

有限责任公司 11204

代理人 王达佐 马晓亚

(51)Int.Cl.

G06T 11/60(2006.01)

G06F 21/36(2013.01)

权利要求书3页 说明书13页 附图4页

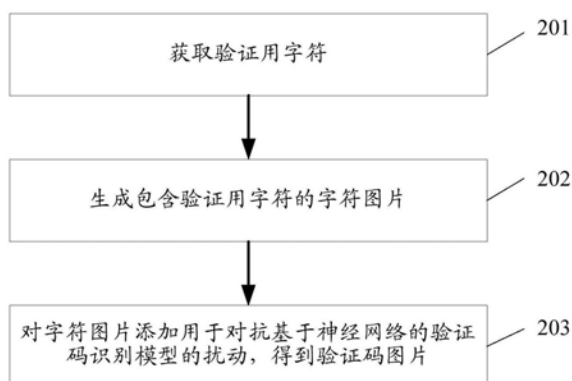
(54)发明名称

验证码图片生成方法和装置

(57)摘要

本申请实施例公开了验证码图片生成方法和装置。该方法的一具体实施方式包括:获取验证用字符;生成包含验证用字符的字符图片;对字符图片添加用于对抗基于神经网络的验证码识别模型的扰动,得到验证码图片,扰动基于差分进化算法得出。该实施方式实现了能够有效防止基于神经网络的图像识别算法破解的验证码图片的快速生成,提升了验证码图片对恶意攻击的安全防护性能。

200



1. 一种验证码图片生成方法,包括:

获取验证用字符;

生成包含所述验证用字符的字符图片;

对所述字符图片添加用于对抗基于神经网络的验证码识别模型的扰动,得到验证码图片,所述扰动基于差分进化算法得出。

2. 根据权利要求1所述的方法,其中,所述验证码图片按照如下方式生成:

在所述字符图片上叠加采用差分进化算法迭代更新得到的扰动向量集合,生成所述验证码图片;

其中,添加更新后的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度强于添加更新前的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度。

3. 根据权利要求2所述的方法,其中,所述在所述字符图片上叠加采用差分进化算法迭代更新得到的扰动向量集合,生成所述验证码图片,包括:

获取基于样本验证码图片集合对图像识别神经网络训练得到的验证码识别模型,以及所述训练得到的验证码识别模型对样本验证码图片集合的第一识别结果;

初始化扰动向量集合,所述扰动向量集合中的扰动向量是对所述样本验证码图片中的随机位置的预设数量个像素赋予随机值生成的;

基于扰动向量集合中的扰动向量的差分向量迭代更新扰动向量集合,使得所述验证码识别模型对添加更新后的扰动向量集合的样本验证码图片集合的识别结果与所述第一识别结果之间的偏离程度满足预设的条件。

4. 根据权利要求3所述的方法,其中,所述基于扰动向量集合中的扰动向量的差分向量迭代更新扰动向量集合,包括:

迭代执行预设次如下搜索操作:

将当前扰动向量集合中的扰动向量添加至所述样本验证码图片集合中,利用训练得到的验证码识别模型对添加扰动向量后的样本验证码图片集合进行识别,得到第二识别结果;

随机选择当前扰动向量集合中的扰动向量进行差分变异,得到差分变异后的扰动向量集合;

将差分变异后的扰动向量集合中的扰动向量添加至所述样本验证码图片集合中,利用训练得到的验证码识别模型对添加差分变异后的后的扰动向量的样本验证码图片集合进行识别,得到第三识别结果;

比对所述第二识别结果偏离所述第一识别结果的置信度以及所述第三识别结果偏离所述第一识别结果的置信度;

若所述第二识别结果偏离所述第一识别结果的置信度小于所述第三识别结果偏离所述第一识别结果的置信度,将所述差分变异后的扰动向量集合作为下一次搜索操作中的当前扰动向量集合;

若所述第二识别结果偏离所述第一识别结果之间的置信度大于所述第三识别结果偏离所述第一识别结果的置信度,将当前搜索操作中的当前扰动向量集合作为下一次搜索操作中的当前扰动向量集合。

5. 根据权利要求1所述的方法, 其中, 所述生成包含所述验证用字符的字符图片, 包括:
从预设的字符图形库中确定出各所述验证用字符的字符图形, 将各所述验证用字符的字符图形组合为所述字符图片。

6. 根据权利要求1所述的方法, 其中, 所述生成包含所述验证用字符的字符图片, 包括:
构建包含验证用字符的图片, 对所述包含验证用字符的图片添加预设的几何噪音后得到所述字符图片。

7. 根据权利要求1-6任一项所述的方法, 其中, 所述方法还包括:
推送所述验证码图片;
获取发出验证请求的对象根据所述验证码图片提供的待验证字符, 并与所述验证用字符进行比对, 根据比对结果判断所述发出验证请求的对象是否通过验证。

8. 一种验证码图片生成装置, 包括:
获取单元, 被配置为获取验证用字符;
生成单元, 被配置为生成包含所述验证用字符的字符图片;
扰动单元, 被配置为对所述字符图片添加用于对抗基于神经网络的验证码识别模型的扰动, 得到验证码图片, 所述扰动基于差分进化算法得出。

9. 根据权利要求8所述的装置, 其中, 所述扰动单元被配置为按照如下方式生成所述验证码图片:

在所述字符图片上叠加采用差分进化算法迭代更新得到的扰动向量集合, 生成所述验证码图片;

其中, 添加更新后的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度强于添加更新前的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度。

10. 根据权利要求9所述的装置, 其中, 所述扰动单元被配置为进一步按照如下方式生成所述验证码图片:

获取基于样本验证码图片集合对图像识别神经网络训练得到的验证码识别模型, 以及所述训练得到的验证码识别模型对样本验证码图片集合的第一识别结果;

初始化扰动向量集合, 所述扰动向量集合中的扰动向量是对所述样本验证码图片中的随机位置的预设数量个像素赋予随机值生成的;

基于扰动向量集合中的扰动向量的差分向量迭代更新扰动向量集合, 使得所述验证码识别模型对添加更新后的扰动向量集合的样本验证码图片集合的识别结果与所述第一识别结果之间的偏离程度满足预设的条件。

11. 根据权利要求10所述的装置, 其中, 所述扰动单元进一步被配置为按照如下方式迭代更新扰动向量集合:

迭代执行预设次如下搜索操作:

将当前扰动向量集合中的扰动向量添加至所述样本验证码图片集合中, 利用训练得到的验证码识别模型对添加扰动向量后的样本验证码图片集合进行识别, 得到第二识别结果;

随机选择当前扰动向量集合中的扰动向量进行差分变异, 得到差分变异后的扰动向量集合;

将差分变异后的扰动向量集合中的扰动向量添加至所述样本验证码图片集合中,利用训练得到的验证码识别模型对添加差分变异后的后的扰动向量的样本验证码图片集合进行识别,得到第三识别结果;

比对所述第二识别结果偏离所述第一识别结果的置信度以及所述第三识别结果偏离所述第一识别结果的置信度;

若所述第二识别结果偏离所述第一识别结果的置信度小于所述第三识别结果偏离所述第一识别结果的置信度,将所述差分变异后的扰动向量集合作为下一次搜索操作中的当前扰动向量集合;

若所述第二识别结果偏离所述第一识别结果之间的置信度大于所述第三识别结果偏离所述第一识别结果的置信度,将当前搜索操作中的当前扰动向量集合作为下一次搜索操作中的当前扰动向量集合。

12. 根据权利要求8所述的装置,其中,所述生成单元进一步被配置为按照如下方式生成包含所述验证用字符的字符图片:

从预设的字符图形库中确定出各所述验证用字符的字符图形,将各所述验证用字符的字符图形组合为所述字符图片。

13. 根据权利要求8所述的装置,其中,所述生成单元进一步被配置为按照如下方式生成包含所述验证用字符的字符图片:

构建包含验证用字符的图片,对所述包含验证用字符的图片添加预设的几何噪音后得到所述字符图片。

14. 根据权利要求8-13任一项所述的装置,其中,所述装置还包括:

推送单元,被配置为推送所述验证码图片;

验证单元,被配置为获取发出验证请求的对象根据所述验证码图片提供的待验证字符,并与所述验证用字符进行比对,根据比对结果判断所述发出验证请求的对象是否通过验证。

15. 一种电子设备,包括:

一个或多个处理器;

存储装置,用于存储一个或多个程序,

当所述一个或多个程序被所述一个或多个处理器执行,使得所述一个或多个处理器实现如权利要求1-7中任一所述的方法。

16. 一种计算机可读介质,其上存储有计算机程序,其中,所述程序被处理器执行时实现如权利要求1-7中任一所述的方法。

验证码图片生成方法和装置

技术领域

[0001] 本申请实施例涉及计算机技术领域,具体涉及身份验证技术领域,尤其涉及验证码图片生成方法和装置。

背景技术

[0002] CAPTCHA(验证码)是“Completely Automated Public Turing test to tell Computers and Humans Apart”(全自动区分计算机和人类的图灵测试)的缩写,是一种区分用户是计算机还是人的公共全自动程序。通常验证码以图片形式呈现,由于机器难以自动识别验证码图片的内容,而人类可以容易地识别出验证码图片的内容,因此可以用于验证是否为人工操作。验证码技术可以防止恶意破解密码、刷票、论坛灌水,有效防止某个黑客对某一个特定注册用户用特定程序暴力破解方式进行不断的登陆尝试。

[0003] 基于图像识别的验证码攻击方式可以自动识别验证码图片中的字符,传统的验证码机器识别抵御机制主要采用在图片中增加基于边缘检测等图像检测算法无法准确分割的几何图案、或者对字符进行扭曲变形等方式。随着人工智能技术的发展,出现了采用诸如基于神经网络的图像识别算法识别验证码的方法。基于神经网络的图像识别算法对包含这些几何图案、扭曲变形的字体的验证码图片具有较强的鲁棒性,在经过足够数量的样本训练之后,可以比较准确地识别出验证码图片中的字符。

发明内容

[0004] 本申请实施例提出了验证码图片生成方法和装置。

[0005] 第一方面,本申请实施例提供了一种验证码图片生成方法,包括:获取验证用字符;生成包含验证用字符的字符图片;对字符图片添加用于对抗基于神经网络的验证码识别模型的扰动,得到验证码图片,扰动基于差分进化算法得出。

[0006] 在一些实施例中,上述验证码图片按照如下方式生成:在字符图片上叠加采用差分进化算法迭代更新得到的扰动向量集合,生成验证码图片;其中,添加更新后的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度强于添加更新前的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度。

[0007] 在一些实施例中,上述在字符图片上叠加采用差分进化算法迭代更新得到的扰动向量集合,生成验证码图片,包括:获取基于样本验证码图片集合对图像识别神经网络训练得到的验证码识别模型,以及训练得到的验证码识别模型对样本验证码图片集合的第一识别结果;初始化扰动向量集合,扰动向量集合中的扰动向量是对上述样本验证码图片中的随机位置的预设数量个像素赋予随机值生成的;基于扰动向量集合中的扰动向量的差分向量迭代更新扰动向量集合,使得验证码识别模型对添加更新后的扰动向量集合的样本验证码图片集合的识别结果与第一识别结果之间的偏离程度满足预设的条件。

[0008] 在一些实施例中,上述基于扰动向量集合中的扰动向量的差分向量迭代更新扰动

向量集合,包括:迭代执行预设次如下搜索操作:将当前扰动向量集合中的扰动向量添加至样本验证码图片集合中,利用训练得到的验证码识别模型对添加扰动向量后的样本验证码图片集合进行识别,得到第二识别结果;随机选择当前扰动向量集合中的扰动向量进行差分变异,得到差分变异后的扰动向量集合;将差分变异后的扰动向量集合中的扰动向量添加至样本验证码图片集合中,利用训练得到的验证码识别模型对添加差分变异后的后的扰动向量的样本验证码图片集合进行识别,得到第三识别结果;比对第二识别结果偏离第一识别结果的置信度以及第三识别结果偏离第一识别结果的置信度;若第二识别结果偏离第一识别结果的置信度小于第三识别结果偏离第一识别结果的置信度,将差分变异后的扰动向量集合作为下一次搜索操作中的当前扰动向量集合;若第二识别结果偏离第一识别结果之间的置信度大于第三识别结果偏离第一识别结果的置信度,将当前搜索操作中的当前扰动向量集合作为下一次搜索操作中的当前扰动向量集合。

[0009] 在一些实施例中,上述生成包含验证用字符的字符图片,包括:从预设的字符图形库中确定出各验证用字符的字符图形,将各验证用字符的字符图形组合为字符图片。

[0010] 在一些实施例中,上述生成包含验证用字符的字符图片,包括:构建包含验证用字符的图片,对包含验证用字符的图片添加预设的几何噪音后得到字符图片。

[0011] 在一些实施例中,上述方法还包括:推送验证码图片;获取发出验证请求的对象根据验证码图片提供的待验证字符,并与验证用字符进行比对,根据比对结果判断发出验证请求的对象是否通过验证。

[0012] 第二方面,本申请实施例提供了一种验证码图片生成装置,包括:获取单元,被配置为获取验证用字符;生成单元,被配置为生成包含验证用字符的字符图片;扰动单元,被配置为对字符图片添加用于对抗基于神经网络的验证码识别模型的扰动,得到验证码图片,扰动基于差分进化算法得出。

[0013] 在一些实施例中,上述扰动单元被配置为按照如下方式生成验证码图片:在字符图片上叠加采用差分进化算法迭代更新得到的扰动向量集合,生成验证码图片;其中,添加更新后的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度强于添加更新前的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度。

[0014] 在一些实施例中,上述扰动单元被配置为进一步按照如下方式生成验证码图片:获取基于样本验证码图片集合对图像识别神经网络训练得到的验证码识别模型,以及训练得到的验证码识别模型对样本验证码图片集合的第一识别结果;初始化扰动向量集合,扰动向量集合中的扰动向量是对上述样本验证码图片中的随机位置的预设数量个像素赋予随机值生成的;基于扰动向量集合中的扰动向量的差分向量迭代更新扰动向量集合,使得验证码识别模型对添加更新后的扰动向量集合的样本验证码图片集合的识别结果与第一识别结果之间的偏离程度满足预设的条件。

[0015] 在一些实施例中,上述扰动单元进一步被配置为按照如下方式迭代更新扰动向量集合:迭代执行预设次如下搜索操作:将当前扰动向量集合中的扰动向量添加至样本验证码图片集合中,利用训练得到的验证码识别模型对添加扰动向量后的样本验证码图片集合进行识别,得到第二识别结果;随机选择当前扰动向量集合中的扰动向量进行差分变异,得到差分变异后的扰动向量集合;将差分变异后的扰动向量集合中的扰动向量添加至样本验

验证码图片集合中,利用训练得到的验证码识别模型对添加差分变异后的后的扰动向量的样本验证码图片集合进行识别,得到第三识别结果;比对第二识别结果偏离第一识别结果的置信度以及第三识别结果偏离第一识别结果的置信度;若第二识别结果偏离第一识别结果的置信度小于第三识别结果偏离第一识别结果的置信度,将差分变异后的扰动向量集合作为下一次搜索操作中的当前扰动向量集合;若第二识别结果偏离第一识别结果之间的置信度大于第三识别结果偏离第一识别结果的置信度,将当前搜索操作中的当前扰动向量集合作为下一次搜索操作中的当前扰动向量集合。

[0016] 在一些实施例中,上述生成单元进一步被配置为按照如下方式生成包含验证用字符的字符图片:从预设的字符图形库中确定出各验证用字符的字符图形,将各验证用字符的字符图形组合为字符图片。

[0017] 在一些实施例中,上述生成单元进一步被配置为按照如下方式生成包含验证用字符的字符图片:构建包含验证用字符的图片,对包含验证用字符的图片添加预设的几何噪音后得到字符图片。

[0018] 在一些实施例中,上述装置还包括:推送单元,被配置为推送验证码图片;验证单元,被配置为获取发出验证请求的对象根据验证码图片提供的待验证字符,并与验证用字符进行比对,根据比对结果判断发出验证请求的对象是否通过验证。

[0019] 第三方面,本申请实施例提供了一种电子设备,包括:一个或多个处理器;存储装置,用于存储一个或多个程序,当一个或多个程序被一个或多个处理器执行,使得一个或多个处理器实现如第一方面提供的验证码图片生成方法。

[0020] 第四方面,本申请实施例提供了一种计算机可读介质,其上存储有计算机程序,其中,程序被处理器执行时实现第一方面提供的验证码图片生成方法。

[0021] 本申请上述实施例的验证码图片生成方法和装置,通过获取验证用字符,生成包含验证用字符的字符图片,对字符图片添加用于对抗基于神经网络的验证码识别模型的扰动,得到验证码图片,扰动基于差分进化算法得出,实现了能有效防止基于神经网络的图像识别算法破解的验证码图片的快速生成,提升了验证码图片对恶意攻击的安全防护性能。

附图说明

[0022] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述,本申请的其它特征、目的和优点将会变得更明显:

[0023] 图1是本申请实施例可以应用于其中的示例性系统架构图;

[0024] 图2是根据本申请的验证码图片生成方法的一个实施例的流程图;

[0025] 图3是根据本申请的验证码图片生成方法的另一个实施例的流程图;

[0026] 图4是本申请的验证码图片生成装置的一个实施例的结构示意图;

[0027] 图5是适于用来实现本申请实施例的电子设备的计算机系统的结构示意图。

具体实施方式

[0028] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是,此处所描述的具体实施例仅仅用于解释相关发明,而非对该发明的限定。另外还需要说明的是,为了便于描述,附图中仅示出了与有关发明相关的部分。

[0029] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0030] 图1示出了可以应用本申请的验证码图片生成方法或验证码图片生成装置的示例性系统架构100。

[0031] 如图1所示,系统架构100可以包括终端设备101、102、103,网络104以及服务器105。网络104用以在终端设备101、102、103和服务器105之间提供通信链路的介质。网络可以包括各种连接类型,例如有线、无线通信链路或者光纤电缆等等。

[0032] 用户110可以使用终端设备101、102、103通过网络104与服务器105交互,以接收或发送消息等。终端设备101、102、103上可以安装有各种数据访问应用,例如文件管理应用、搜索应用、电商应用、邮件客户端、社交平台应用等。

[0033] 终端设备101、102、103可以是具有显示屏并支持互联网访问的各种电子设备,包括但不限于台式电脑、智能手机、平板电脑、智能手表、笔记本电脑、膝上便携型电脑、电子书阅读器等。

[0034] 服务器105可以是提供各类数据访问服务的服务器,例如文件管理服务器或邮件服务器。服务器105可以接收终端设备101、102、103发送的数据访问请求,对发出数据访问请求的对象的身份进行验证,例如可以生成验证码图片,通过网络104发送至终端设备101、102、103。终端设备101、102、103可以将用户输入的验证码、或者从其他设备获取的验证码发送给服务器105,服务器105可以将终端设备101、102、103发送的验证码与后台存储的验证码序列进行比对,若一致,则服务器105可以确认发出数据访问请求的对象的身份合法,根据数据访问请求查询数据并反馈给终端设备101、102、103;否则可以确认发出数据访问请求的对象的身份不合法,拒绝向发出数据访问请求的对象提供所请求访问的数据。

[0035] 终端设备101、102、103可以包含用于执行物理运算的部件(例如GPU等处理器),终端设备101、102、103也可以生成验证码图片,对发出数据访问请求的对象的身份进行验证。这时,上述系统架构中可以不包含网络104和服务器105。

[0036] 本申请实施例所提供的验证码图片生成方法可以由终端设备101、102、103或服务器105执行,相应地,验证码图片生成装置可以设置于终端设备101、102、103或服务器105中。

[0037] 应该理解,图1中的终端设备、网络、服务器的数目仅仅是示意性的。根据实现需要,可以具有任意数目的终端设备、网络、服务器。

[0038] 继续参考图2,其示出了根据本申请的验证码图片生成方法的一个实施例的流程200。该验证码图片生成方法,包括以下步骤:

[0039] 步骤201,获取验证用字符。

[0040] 在本实施例中,验证码图片生成方法的执行主体可以从已存储的字符库中获取验证用字符,该验证用字符可以用于验证发出验证请求的对象的身份。已存储的字符库可以包括各种类别的字符库,例如英文字符库、中文字符库、符号库等。上述执行主体可以从字符库中随机、或按照预先制定的规则选取一些字符作为验证用字符。

[0041] 可选地,在选择验证用字符时,可以在一个类别的字符库中选择预设数量的字符,例如可以在中文字符库中选择3个汉字作为验证用字符;也可以从不同类别的字符库中分别选择一个或多个字符,例如可以分别从中文字符库、英文字符库、符号库中各选择一个字

符形成验证用字符。

[0042] 在本实施例中,在获取验证用字符时还可以记录各验证用字符的排列顺序。在实践中,基于验证码图片的身份验证方法中还可以验证输入的验证码的顺序是否与获取的验证用字符的排列顺序一致。

[0043] 步骤202,生成包含验证用字符的字符图片。

[0044] 在本实施例中,可以将获取到的验证用字符组合在一张图片中,生成字符图片。可以预先生成图片模板,图片模板包括预先设定的各字符的字体、尺寸、位置等信息,在字体库中查找到验证用字符的与图片模板中匹配的字体后,进行相应的缩放之后填充至图片模板中生成字符图片。

[0045] 在本实施例的一些可选的实现方式中,可以按照如下方式生成包含验证用字符的字符图片:从预设的字符图形库中确定出各验证用字符的字符图形,将各验证用字符的字符图形组合为字符图片。预设的字符图形库中包含了预设字符库中的各字符对应的字符图形,其中每个字符对应的字符图形可以有多个,例如每个字符可以具有不同文字样式的字符图形(例如带有纹理填充的字符图形、带有阴影的字符图形)。并且,每个字符图形具有相应字符的标识。可以从预设的字符图像库中确定出步骤201获取的各验证用字符的字符图形,然后将各验证用字符的字符图形组合起来,进行图片填充后生成字符图片。

[0046] 在本实施例的另一些可选的实现方式中,可以按照如下方式生成包含验证用字符的字符图片:构建包含验证用字符的图片,对包含验证用字符的图片添加预设的几何噪音后得到字符图片。

[0047] 具体来说,可以基于诸如上述利用字符图形组合的方式构建出包含验证用字符的图片,然后可以在构建的图片上添加预设的几何噪音。在这里,添加预设的几何噪音的方式可以包括但不限于添加以下至少一项:干扰线噪音、背景噪音、噪点、镂空图案。添加预设的几何噪音的方式也可以是对构建的图片进行几何变形使得其中的字符扭曲、黏连、字体变化等的处理。

[0048] 在添加预设的几何噪音后,生成的字符图片中包含了用于干扰基于图像分割等的验证码机器识别结果的因素,使得机器识别的准确率下降,而人眼可以准确辨识验证码,从而实现了人机鉴别。

[0049] 步骤203,对字符图片添加用于对抗基于神经网络的验证码识别模型的扰动,得到验证码图片。

[0050] 为了对抗基于神经网络的验证码机器识别方法,可以利用差分进化算法确定用于对抗基于神经网络的验证码识别模型的扰动,并添加至步骤202生成的字符图片上。具体可以采用差分进化算法确定添加的扰动因子,将扰动因子添加至生成的字符图片中,生成验证码图片。

[0051] 扰动因子可以是与验证码图片的像素矩阵维度相同的矩阵,确定扰动因子即确定该矩阵中各元素的参数。在本实施例中,可以首先生成初始的扰动因子集合作为种群,该种群中的每个个体可以是与验证码图片的像素矩阵维度相同的矩阵。在实践中,可以随机选择验证码图片的像素矩阵中的一些像素赋予随机的值,将其他像素赋值为0,形成一个扰动因子。选择不同的像素赋予随机的值、其他像素赋值为0之后,得到多个各不相同的扰动因子,从而形成包含多个扰动因子的扰动因子集合。

[0052] 随后可以执行如下进化操作:基于扰动因子集合进行差分进化运算,具体可以选出扰动因子集合中的两个目标扰动因子进行差分运算得到差分扰动因子,将差分扰动因子叠加至扰动因子集合中的除目标扰动因子之外的任意一个扰动因子上得到进化后的扰动因子集合。利用进化前的扰动因子集合和进化后的扰动因子集合分别对所搜集的样本验证码图片进行扰动,然后判断所添加的进化后的扰动因子集合是否提升了验证码图片对抗基于神经网络的验证码识别模型的能力(例如判断基于神经网络的验证码识别模型是否对添加进化后的扰动因子集合的验证码图片的识别准确率下降和/或识别速率下降),若是,则可以将进化后的扰动因子添加至上述字符图片中,来生成验证码图片。这样,通过在字符图片中添加基于差分进化算法得出的扰动因子,可以提升验证码图片对抗基于神经网络的验证码识别模型的能力。

[0053] 本申请上述实施例的验证码图片生成方法,通过获取验证用字符,验证用字符用于验证发出验证请求的对象的身份;生成包含验证用字符的字符图片;采用差分进化算法对字符图片添加对抗基于神经网络的验证码识别模型的扰动,得到验证码图片,能够快速、高效地生成对抗基于神经网络的验证码识别模型的验证码图片,能够更准确地进行人机鉴别,提升了验证码图片对于恶意攻击的安全防护能力。同时,采用差分进化算法得出的图像扰动在视觉上的扰动较小,提升了用户友好性。

[0054] 在本实施例的一些可选的实现方式中,验证码图片可以是按照如下方式的:在字符图片上叠加采用差分进化算法迭代更新得到的扰动向量集合,生成验证码图片;其中,添加更新后的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度强于添加更新前的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度。

[0055] 即可以构建包含多个扰动向量的扰动向量集合,并对扰动向量集合采用差分进化算法执行多次迭代更新操作,在每次迭代过程中,可以基于扰动向量集合进行差分进化运算,将两个扰动向量的差分扰动向量叠加至当前扰动向量集合中的其他扰动向量上得到更新后的扰动向量集合。利用更新后的扰动向量集合和更新前的扰动向量集合分别对所搜集的样本验证码图片进行扰动,然后判断添加更新后的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度是否强于添加更新前的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度。即判断基于神经网络的验证码识别模型对添加更新后的扰动向量集合的字符图片的识别准确性是否低于对添加更新前的扰动向量集合的字符图片的识别准确性。若是,则将更新后的扰动向量集合作为新的扰动向量集合,否则将更新前的扰动向量集合作为新的扰动向量集合,继续执行上述迭代更新操作。在这里,识别准确性可以由识别准确率表示,也可以由错误识别率、错误拒绝率、错误接受率等的倒数来表示。

[0056] 这样,在多次执行扰动向量集合的进化操作后,更新后的扰动向量集合不断提升对抗基于神经网络的验证码识别模型的能力,使基于神经网络的验证码识别模型对添加扰动后的验证码图片的识别准确性逐渐降低。可以获得多次进化操作后的扰动向量集合,将其叠加至步骤202生成的字符图片上,得到包含上述验证用字符的验证码图片。

[0057] 在进一步的实现方式中,上述在字符图片上叠加采用差分进化算法迭代更新得到的扰动向量集合,生成验证码图片的步骤可以包括:获取基于样本验证码图片集合对图像

识别神经网络训练得到的验证码识别模型,以及训练得到的验证码识别模型对样本验证码图片集合的第一识别结果;初始化扰动向量集合,扰动向量集合中的扰动向量是对样本验证码图片中随机位置的预设数量个像素赋予随机值生成的;基于扰动向量集合中的扰动向量的差分向量迭代更新扰动向量集合,使得验证码识别模型对添加更新后的扰动向量集合的样本验证码图片集合的识别结果与第一识别结果之间的偏离程度满足预设的条件。

[0058] 具体来说,首先可以选择一个图像识别神经网络,该图像识别神经网络可以是深度神经网络,例如ResNet、VGG等,使用验证码生成器生成样本验证码图片的集合,或者从互联网收集验证码图片生成样本验证码图片的集合。其中验证码生成器可以采用例如步骤201和步骤202的方法生成样本验证码图片。利用样本验证码图片对图像识别神经网络进行训练得到验证码识别模型。还可以获取利用该训练得到的验证码识别模型对样本验证码图片进行识别得到的第一识别结果。

[0059] 然后,初始化一个扰动向量集合,该扰动向量集合中的每个扰动向量可以通过选择样本验证码图片中预设数量、位置随机的像素,赋予随机的值生成的,例如样本验证码图片的分辨率为 $M \times N$,其包含 $M \times N$ 个像素, M 、 N 均为正整数。初始的扰动向量集合中的扰动向量可以是包含 $M \times N$ 个元素的一维向量,每个元素对应样本验证码图片的一个像素。可以在该一维向量中随机选择一些元素赋值为随机的非零数,并且将其他元素赋值为0。初始的扰动向量集合中各扰动向量互不相同。

[0060] 之后,可以从扰动向量集合中随机选择两个扰动向量做差分运算,得到差分向量,利用该差分向量更新扰动向量集合。具体可以将该差分向量叠加至扰动向量集合中的至少一个扰动向量,得到更新后的扰动向量集合。然后将更新后的扰动向量集合中的扰动向量与样本验证码图片集合中的样本验证码图片随机地组合叠加,得到扰动后的样本验证码图片。

[0061] 接着,可以利用上述已训练的验证码识别模型对扰动后的样本验证码图片进行识别,判断识别准确率是否小于上述第一识别结果所表征的识别准确率。若该验证码识别模型对扰动后的样本验证码图片的识别准确率小于验证码识别模型对本次扰动前的样本验证码图片的识别准确率,则表明添加扰动后样本验证码图片对基于神经网络的验证码识别模型的对抗能力增强,这时,可以在更新后的扰动向量集合的基础上,继续计算差分向量并更新扰动向量集合。若该验证码识别模型对扰动后的样本验证码图片的识别准确率大于验证码识别模型对本次扰动前的样本验证码图片的识别准确率,则表明添加扰动后样本验证码图片对基于神经网络的验证码识别模型的对抗能力减弱,这时,可以在更新前的扰动向量集合的基础上,重新随机选择两个扰动向量计算差分向量并更新扰动向量集合。

[0062] 可以重复执行上述更新扰动向量集合的操作,直到验证码识别模型对添加更新后的扰动向量集合的样本验证码图片集合的识别结果与第一识别结果之间的偏离程度满足预设的条件。在这里,预设的条件可以是识别准确率的偏移达到预设的偏移值。

[0063] 通过获取训练得到的验证码识别模型,并利用差分向量迭代更新扰动向量集合,可以快速地确定出能够干扰基于神经网络的验证码识别模型的扰动向量。

[0064] 可选地,上述基于扰动向量集合中的扰动向量的差分向量迭代更新扰动向量集合的操作可以包括迭代执行预设次(例如100次)搜索操作。在这里,搜索操作是搜索最优扰动向量集合的操作,该搜索操作具体可以按照如下方式执行:

[0065] 首先,将当前扰动向量集合中的扰动向量添加至样本验证码图片集合中,利用训练得到的验证码识别模型对添加扰动向量后的样本验证码图片集合进行识别,得到第二识别结果。在迭代过程的每次搜索操作中,首先可以将当前搜索操作的扰动向量集合添加至样本验证码图片集合得到第一扰动图片集合,并获取验证码识别模型对第一扰动图片的第二识别结果。

[0066] 接着,随机选择当前扰动向量集合中的扰动向量进行差分变异,得到差分变异后的扰动向量集合。

[0067] 具体地,可以从当前扰动向量集合 $\{x_1(g), x_2(g), x_3(g), \dots\}$ 中随机选择三个扰动向量 $x_{r1}(g)$ 、 $x_{r2}(g)$ 、 $x_{r3}(g)$,对 $x_{r2}(g)$ 、 $x_{r3}(g)$ 做差分运算得到差分向量 $x_{r2}(g) - x_{r3}(g)$,然后对差分向量加权后与 $x_{r1}(g)$ 相加得到差分变异向量 $h_i(g)$:

$$[0068] \quad h_i(g) = x_{r1}(g) + F(x_{r2}(g) - x_{r3}(g)) \quad (1)$$

[0069] 其中, $x_i(g)$ 、 $x_{r1}(g)$ 、 $x_{r2}(g)$ 、 $x_{r3}(g)$ 分别为第 g 次迭代(即第 g 次搜索操作)中扰动向量集合的第 i 个、第 $r1$ 个、第 $r2$ 个、第 $r3$ 个扰动向量, $i, r1, r2, r3$ 均为正整数, $r1 \neq r2 \neq r3$; F 为权重,可以预先设定,例如为 0.5、0.3 等。

[0070] 可以将差分变异向量 $h_i(g)$ 与当前扰动向量集合中的第 i 个扰动向量 $x_i(g)$ 叠加来替换 $x_i(g)$,得到差分变异后的扰动向量,即将当前扰动向量集合中的 $x_i(g)$ 替换为 $x_i(g) + h_i(g)$,其他扰动向量不做变换,得到差分变异后的扰动向量集合 $\{x_1(g), x_2(g), \dots, x_{i-1}(g), x_i(g) + h_i(g), x_{i+1}(g), \dots\}$ 。

[0071] 然后,将差分变异后的扰动向量集合中的扰动向量添加至样本验证码图片集合中,利用训练得到的验证码识别模型对添加差分变异后的后的扰动向量的样本验证码图片集合进行识别,得到第三识别结果。具体可以将差分变异后的扰动向量集合中的扰动向量转换为对应的扰动图像矩阵,将样本验证码图片与扰动图像矩阵叠加得到添加了差分变异后的扰动向量的验证码图片,然后利用上述验证码识别模型对添加了差分变异后的扰动向量的验证码图片进行识别得到第三识别结果。

[0072] 最后,比对第二识别结果偏离第一识别结果的置信度以及第三识别结果偏离第一识别结果的置信度。若第二识别结果偏离第一识别结果的置信度小于第三识别结果偏离第一识别结果的置信度,将差分变异后的扰动向量集合作为下一次搜索操作中的当前扰动向量集合;若第二识别结果偏离第一识别结果的置信度大于第三识别结果偏离第一识别结果的置信度,将当前搜索操作中的当前扰动向量集合作为下一次搜索操作中的当前扰动向量集合。

[0073] 如果第二识别结果偏离第一识别结果的置信度小于第三识别结果偏离第一识别结果的置信度,也就是说第三识别结果相较于第二识别结果偏离第一识别结果更多,表明添加了差分变异后的扰动向量的验证码图片对于验证码识别模型的对抗能力强于添加了差分变异前的扰动向量的验证码图片对于验证码识别模型的对抗能力,这时,可以将变异后的扰动向量作为下一次搜索操作的当前扰动向量,执行下一次搜索操作。反之,如果第二识别结果偏离第一识别结果的置信度大于第三识别结果偏离第一识别结果的置信度,也就是说第二识别结果相较于第三识别结果偏离第一识别结果更多,表明添加了差分变异前的扰动向量的验证码图片对于验证码识别模型的对抗能力强于添加了差分变异后的扰动向量的验证码图片对于验证码识别模型的对抗能力,这时,可以将变异前的扰动向量作为下

一次搜索操作的当前扰动向量,执行下一次搜索操作。

[0074] 这样,每次搜索操作可以确定出使得添加扰动向量后的样本验证码图片对基于神经网络的验证码识别模型具有较强的对抗能力的扰动向量集合。通过多次执行搜索操作,可以进一步提升扰动向量集合的优化速度。

[0075] 继续参考图3,其示出了根据本申请的验证码图片生成方法的另一个实施例的流程图。如图3所示,本实施例的验证码图片生成方法,包括以下步骤:

[0076] 步骤301,获取验证用字符。

[0077] 在本实施例中,验证码图片生成方法的执行主体可以从已存储的字符库中获取验证用字符,该验证用字符可以用于验证发出验证请求的对象的身份。已存储的字符库可以包括各种类别的字符库,例如英文字符库、中文字符库、符号库等。上述执行主体可以从字符库中随机、或按照预先制定的规则选取一些字符作为验证用字符。

[0078] 步骤302,生成包含验证用字符的字符图片。

[0079] 在本实施例中,可以将获取到的验证用字符组合在一张图片中,生成字符图片。可以预先生成图片模板,图片模板包括预先设定的各字符的字体、尺寸、位置等信息,在字体库中查找到验证用字符的与图片模板中匹配的字体后,进行相应的缩放之后填充至图片模板中生成字符图片。

[0080] 在本实施例的一些可选的实现方式中,可以按照如下方式生成包含验证用字符的字符图片:从预设的字符图形库中确定出各验证用字符的字符图形,将各验证用字符的字符图形组合为字符图片。预设的字符图形库中包含了预设字符库中的各字符对应的字符图形,并且,每个字符图形具有相应字符的标识。可以从预设的字符图像库中确定出步骤301获取的各验证用字符的字符图形,然后将各验证用字符的字符图形组合起来,进行图片填充后生成字符图片。

[0081] 在本实施例的另一些可选的实现方式中,可以按照如下方式生成包含验证用字符的字符图片:构建包含验证用字符的图片,对包含验证用字符的图片添加预设的几何噪音后得到字符图片。

[0082] 步骤303,对字符图片添加用于对抗基于神经网络的验证码识别模型的扰动,得到验证码图片。

[0083] 为了对抗基于神经网络的验证码机器识别方法,可以利用差分进化算法确定用于对抗基于神经网络的验证码识别模型的扰动,并添加至步骤302生成的字符图片上。具体可以采用差分进化算法确定添加的扰动因子,将扰动因子添加至生成的字符图片中,生成验证码图片。

[0084] 扰动因子可以是与验证码图片的像素矩阵维度相同的矩阵,确定扰动因子即确定该矩阵中各元素的参数。在本实施例中,可以首先生成初始的扰动因子集合作为种群,该种群中的每个个体可以是与验证码图片的像素矩阵维度相同的矩阵。在实践中,可以随机选择验证码图片的像素矩阵中的一些像素赋予随机的值,将其他像素赋值为0,形成一个扰动因子。选择不同的像素赋予随机的值、其他像素赋值为0之后,得到多个各不相同的扰动因子,从而形成包含多个扰动因子的扰动因子集合。之后采用差分进化算法优化扰动因子集合,将优化的扰动因子添加到字符图片中生成验证码图片。

[0085] 上述步骤301、步骤302、步骤303分别与前述实施例的步骤201、步骤202、步骤203

一致,上文针对步骤201、步骤202、步骤203的具体实现方式及可选实现方式的描述也适用于步骤301、步骤302、步骤303,此处不再赘述。

[0086] 步骤304,推送验证码图片。

[0087] 在本实施例中,可以向用户推送生成的验证码图片。例如当验证码图片生成方法的执行主体是服务器时,该执行主体可以将步骤303得到的验证码图片推送至用户的终端设备。当验证码图片生成方法的执行主体为发出验证请求的终端设备时,可以将验证码图片推送至终端设备的显示器件进行展示。

[0088] 步骤305,获取发出验证请求的对象根据验证码图片提供的待验证字符,并与验证用字符进行比对,根据比对结果判断发出验证请求的对象是否通过验证。

[0089] 在终端设备接收并展示验证码图片之后,上述执行主体可以获取由发出验证请求的对象提供的待验证字符,进而根据待验证字符与上述步骤301获取的待验证字符的比对结果鉴别发出验证请求的对象的身份是否合法。具体可以鉴别发出验证请求的对象是人还是机器。当待验证字符与验证用字符一致时,可以确定发出验证请求的对象是人,而当待验证字符与验证用字符不一致时,确定发出验证请求的对象是机器。

[0090] 在这里,由于验证码图片中添加了用于对抗基于神经网络的验证码识别模型的扰动,则当机器采用基于神经网络的验证码识别模型进行识别时,无法准确获得验证码图片中的字符,因此提供的待验证字符与验证用字符不一致。而验证码图片中添加的用于对抗基于神经网络的验证码识别模型的扰动在视觉上的扰动很小,人可以容易地从验证码图片中辨识出字符,因此可以基于验证码图片进行人机鉴别。并且,能够抵御基于神经网络的验证码机器识别,提升了采用验证码方式进行身份鉴别的安全防护性能。

[0091] 图3所示的实施例通过增加推送验证码图片、并基于发出验证请求的对象根据验证码图片提供的待验证字符是否与验证用字符匹配来鉴别发出验证请求的对象的身份的步骤,能够通过验证码图片可靠地识别请求者的身份,在基于用户权限的信息获取场景中有效防止不合法的用户获取信息。

[0092] 进一步参考图4,作为对上述各图所示方法的实现,本申请提供了一种验证码图片生成装置的一个实施例,该装置实施例与图2和图3所示的方法实施例相对应,该装置具体可以应用于各种电子设备中。

[0093] 如图4所示,本实施例的验证码图片生成装置400包括:获取单元401、生成单元402以及扰动单元403。其中,获取单元401被配置为获取验证用字符;生成单元402被配置为生成包含验证用字符的字符图片;扰动单元403被配置为对字符图片添加用于对抗基于神经网络的验证码识别模型的扰动,得到验证码图片,扰动基于差分进化算法得出。

[0094] 在一些实施例中,上述扰动单元403可以被配置为按照如下方式生成验证码图片:在字符图片上叠加采用差分进化算法迭代更新得到的扰动向量集合,生成验证码图片;其中,添加更新后的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度强于添加更新前的扰动向量集合的字符图片对基于神经网络的验证码识别模型的识别准确性的干扰程度。

[0095] 在一些实施例中,上述扰动单元403可以被配置为进一步按照如下方式生成验证码图片:获取基于样本验证码图片集合对图像识别神经网络训练得到的验证码识别模型,以及训练得到的验证码识别模型对样本验证码图片集合的第一识别结果;初始化扰动向量

集合,扰动向量集合中的扰动向量是对上述样本验证码图片中的随机位置的预设数量个像素赋予随机值生成的;基于扰动向量集合中的扰动向量的差分向量迭代更新扰动向量集合,使得验证码识别模型对添加更新后的扰动向量集合的样本验证码图片集合的识别结果与第一识别结果之间的偏离程度满足预设的条件。

[0096] 在一些实施例中,上述扰动单元403可以进一步被配置为按照如下方式迭代更新扰动向量集合:迭代执行预设次如下搜索操作:将当前扰动向量集合中的扰动向量添加至样本验证码图片集合中,利用训练得到的验证码识别模型对添加扰动向量后的样本验证码图片集合进行识别,得到第二识别结果;随机选择当前扰动向量集合中的扰动向量进行差分变异,得到差分变异后的扰动向量集合;将差分变异后的扰动向量集合中的扰动向量添加至样本验证码图片集合中,利用训练得到的验证码识别模型对添加差分变异后的后的扰动向量的样本验证码图片集合进行识别,得到第三识别结果;比对第二识别结果偏离第一识别结果的置信度以及第三识别结果偏离第一识别结果的置信度;若第二识别结果偏离第一识别结果的置信度小于第三识别结果偏离第一识别结果的置信度,将差分变异后的扰动向量集合作为下一次搜索操作中的当前扰动向量集合;若第二识别结果偏离第一识别结果之间的置信度大于第三识别结果偏离第一识别结果的置信度,将当前搜索操作中的当前扰动向量集合作为下一次搜索操作中的当前扰动向量集合。

[0097] 在一些实施例中,上述生成单元402可以进一步被配置为按照如下方式生成包含验证用字符的字符图片:从预设的字符图形库中确定出各验证用字符的字符图形,将各验证用字符的字符图形组合为字符图片。

[0098] 在一些实施例中,上述生成单元402可以进一步被配置为按照如下方式生成包含验证用字符的字符图片:构建包含验证用字符的图片,对包含验证用字符的图片添加预设的几何噪音后得到字符图片。

[0099] 在一些实施例中,装置400还可以包括:推送单元,被配置为推送验证码图片;验证单元,被配置为获取发出验证请求的对象根据验证码图片提供的待验证字符,并与验证用字符进行比对,根据比对结果判断发出验证请求的对象是否通过验证。

[0100] 应当理解,装置400中记载的诸单元与参考图2和图3描述的方法中的各个步骤相对应。由此,上文针对方法描述的操作和特征同样适用于装置400及其中包含的单元,在此不再赘述。

[0101] 本申请上述实施例的验证码图片生成装置400,通过在字符图片中添加对抗基于神经网络的验证码识别模型的扰动,得到验证码图片,能够快速获得防止基于神经网络的图像识别算法破解的验证码图片,提升了验证码图片对恶意攻击的安全防护性能。

[0102] 下面参考图5,其示出了适于用来实现本申请实施例的电子设备的计算机系统500的结构示意图。图5示出的电子设备仅仅是一个示例,不应对本申请实施例的功能和使用范围带来任何限制。

[0103] 如图5所示,计算机系统500包括中央处理单元(CPU) 501,其可以根据存储在只读存储器(ROM) 502中的程序或者从存储部分508加载到随机访问存储器(RAM) 503中的程序而执行各种适当的动作和处理。在RAM 503中,还存储有系统500操作所需的各种程序和数据。CPU 501、ROM 502以及RAM 503通过总线504彼此相连。输入/输出(I/O)接口505也连接至总线504。

[0104] 以下部件连接至I/O接口505:包括键盘、鼠标等的输入部分506;包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分507;包括硬盘等的存储部分508;以及包括诸如LAN卡、调制解调器等网络接口卡的通信部分509。通信部分509经由诸如因特网的网络执行通信处理。驱动器510也根据需要连接至I/O接口505。可拆卸介质511,诸如磁盘、光盘、磁光盘、半导体存储器等等,根据需要安装在驱动器510上,以便于从其上读出的计算机程序根据需要被安装入存储部分508。

[0105] 特别地,根据本公开的实施例,上文参考流程图描述的过程可以被实现为计算机软件程序。例如,本公开的实施例包括一种计算机程序产品,其包括承载在计算机可读介质上的计算机程序,该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中,该计算机程序可以通过通信部分509从网络上被下载和安装,和/或从可拆卸介质511被安装。在该计算机程序被中央处理单元(CPU) 501执行时,执行本申请的方法中限定的上述功能。需要说明的是,本申请的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是一——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于:具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中,计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输,包括但不限于:无线、电线、光缆、RF等等,或者上述的任意合适的组合。

[0106] 可以以一种或多种程序设计语言或其组合来编写用于执行本申请的操作的计算机程序代码,程序设计语言包括面向对象的程序设计语言——诸如Java、Smalltalk、C++,还包括常规的过程式程序设计语言——诸如“C”语言或类似的设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)——连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0107] 附图中的流程图和框图,图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分,该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个接连地表示的方框实际上

可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或操作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0108] 描述于本申请实施例中所涉及到的单元可以通过软件的方式实现,也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中,例如,可以描述为:一种处理器包括获取单元、生成单元和扰动单元。其中,这些单元的名称在某种情况下并不构成对该单元本身的限定,例如,获取单元还可以被描述为“获取验证用字符的单元”。

[0109] 作为另一方面,本申请还提供了一种计算机可读介质,该计算机可读介质可以是上述实施例中描述的装置中所包含的;也可以是单独存在,而未装配入该装置中。上述计算机可读介质承载有一个或者多个程序,当上述一个或者多个程序被该装置执行时,使得该装置:获取验证用字符;生成包含验证用字符的字符图片;对字符图片添加用于对抗基于神经网络的验证码识别模型的扰动,得到验证码图片,扰动基于差分进化算法得出。

[0110] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解,本申请中所涉及的发明范围,并不限于上述技术特征的特定组合而成的技术方案,同时也应涵盖在不脱离上述发明构思的情况下,由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

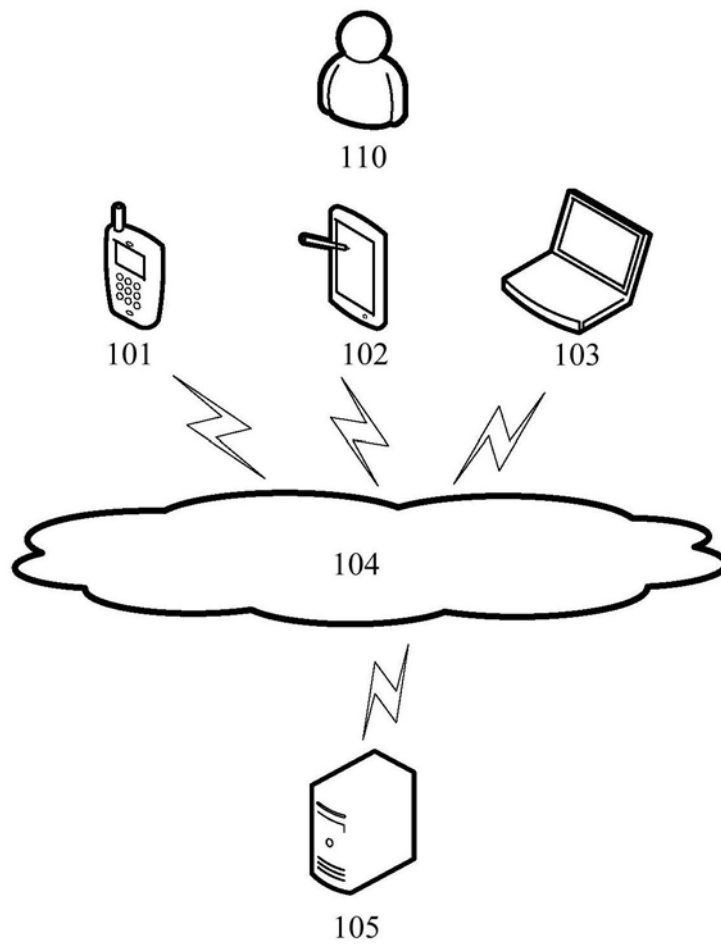
100

图1

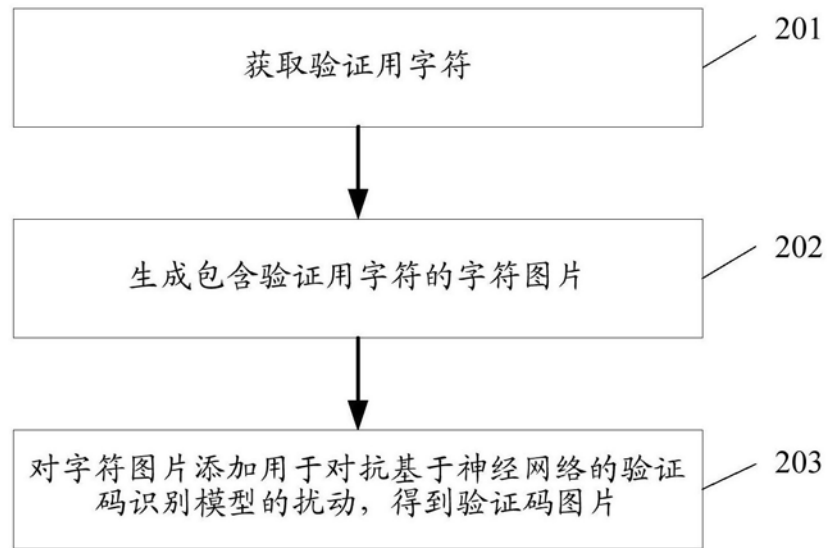
200

图2

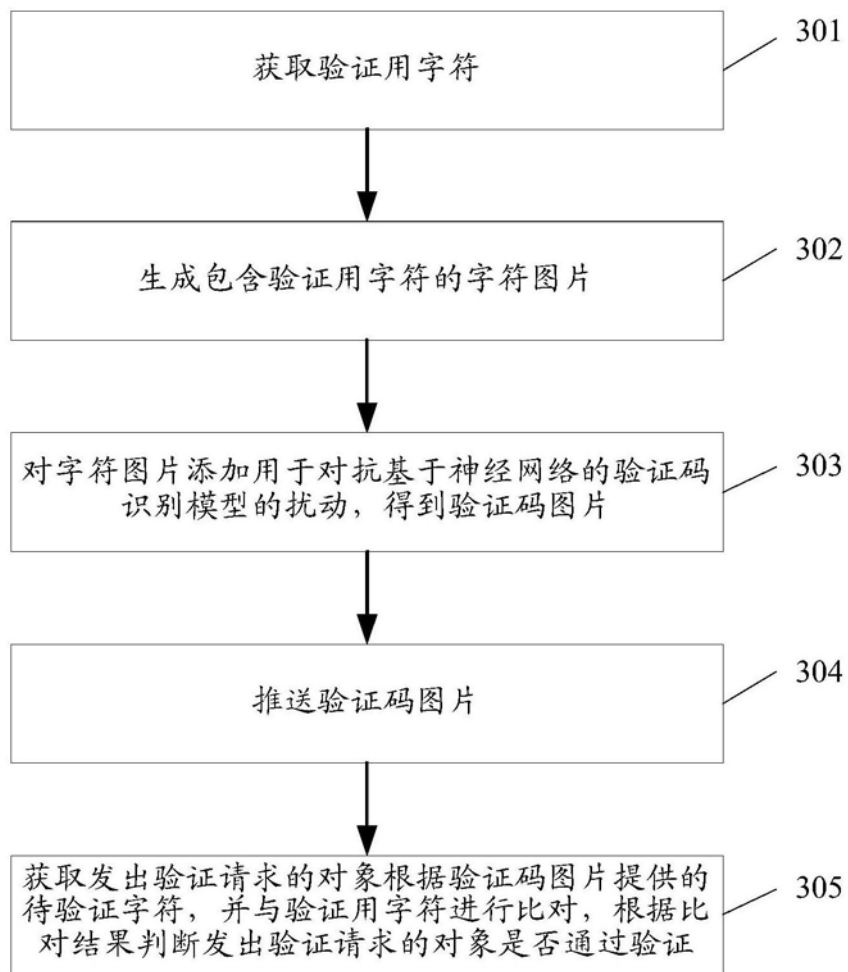
300

图3

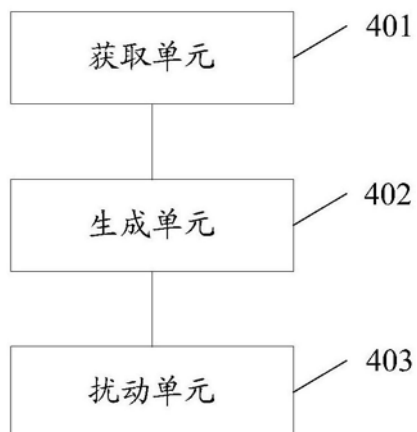
400

图4

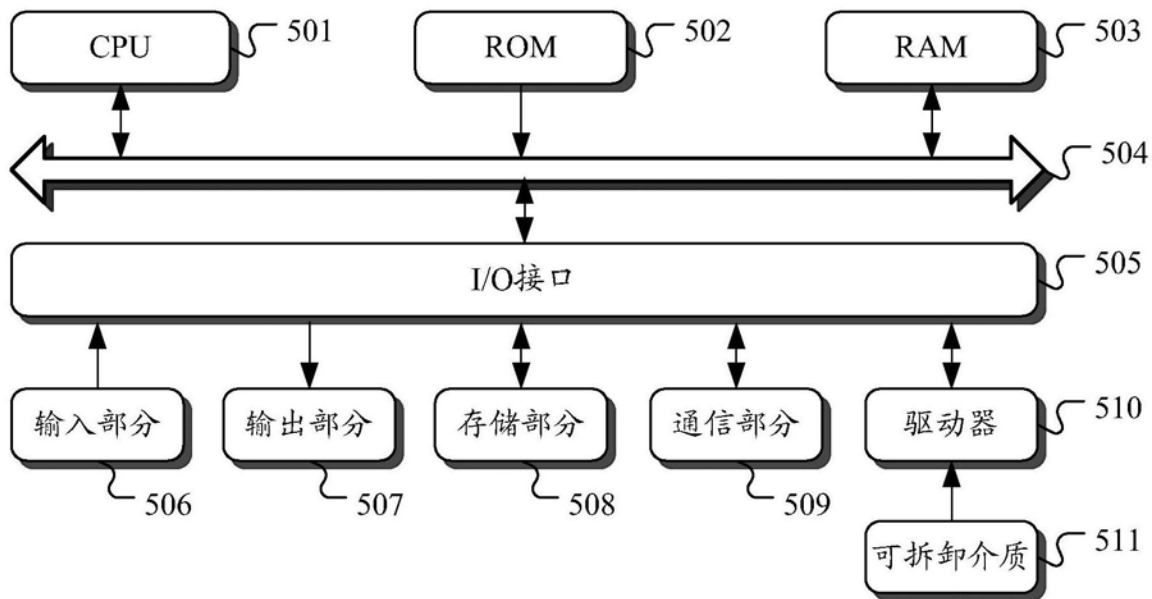
500

图5