

(19) 国家知识产权局



(12) 发明专利



(10) 授权公告号 CN 114117514 B

(45) 授权公告日 2022.09.13

(21) 申请号 202111273688.7

审查员 于萍

(22) 申请日 2021.10.29

(65) 同一申请的已公布的文献号

申请公布号 CN 114117514 A

(43) 申请公布日 2022.03.01

(73) 专利权人 香港理工大学深圳研究院

地址 518057 广东省深圳市南山区粤海街道高新技术产业园南区粤兴一道18号香港理工大学产学研大楼205室

(72) 发明人 赖溥祥 赵麒 李焕浩 余志鹏

(74) 专利代理机构 深圳市君胜知识产权代理事务所(普通合伙) 44268

专利代理人 秦胜军 王永文

(51) Int.Cl.

G06F 21/62 (2013.01)

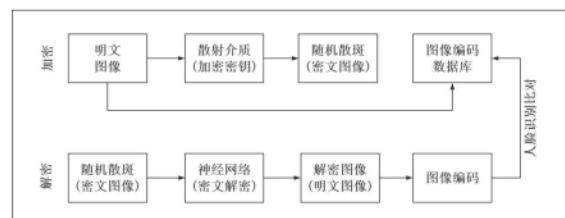
权利要求书2页 说明书8页 附图2页

(54) 发明名称

一种基于光学散斑的加密人脸识别方法和系统

(57) 摘要

本发明公开了一种基于光学散斑的加密人脸识别方法和系统，所述系统包括：人脸图像加密模块，用于基于光学散斑对原始人脸图像进行加密，得到加密人脸图像；人脸图像解密模块，用于将所述加密人脸图像输入已训练的密文图像解密神经网络，得到与所述加密人脸图像对应的解密人脸图像；人脸识别模块，用于将所述解密人脸图像进行识别，得到人脸识别结果。本发明通过人脸图像加密模块基于光学散斑对人脸图像进行加密，可以提升加密的密钥维度，然后通过人脸图像解密模块中的神经网络对加密人脸图像进行解密，最后通过人脸识别模块将解密图像应用于人脸识别，从而提高加密人脸识别系统的安全性，保护人脸照片隐私数据。



1. 一种基于光学散斑的加密人脸识别系统，其特征在于，所述系统包括：

人脸图像加密模块，用于基于光学散斑对原始人脸图像进行加密，得到加密人脸图像；其中，所述加密人脸图像为被调制过的激光经过散射介质后形成；所述散射介质为唯一的高纬度密钥，具有唯一性和不可复制性；

所述人脸图像加密模块包括激光源、空间光调制器、散射介质、相机和透镜；其中，所述激光源用于提供照明；所述空间光调制器用于加载明文图像；所述散射介质用于将所述原始人脸图像变成随机光学散斑图案；所述相机用于记录与所述原始人脸图像对应的随机光学散斑图案；所述透镜包括第一透镜、第二透镜、第三透镜和第四透镜；所述透镜用于对光路中的光束大小进行调整；

人脸图像解密模块，用于将所述加密人脸图像输入已训练的密文图像解密神经网络，得到与所述加密人脸图像对应的用于后续人脸识别的解密人脸图像；

所述人脸图像解密模块为密文图像解密神经网络，其中，所述密文图像解密神经网络由UNet网络和一层基于复数的全连接层组成；

人脸识别模块，用于将所述解密人脸图像进行识别，得到人脸识别结果；

所述人脸识别模块包括图像编码数据库、人脸识别神经网络和匹配模块；其中，所述图像编码数据库用于存储若干人脸图像编码数据；所述人脸识别神经网络用于对人脸图像进行编码；所述匹配模块用于将图像编码数据库中的编码数据和通过所述人脸识别神经网络输出的编码数据进行匹配。

2. 一种如权利要求1所述的基于光学散斑的加密人脸识别系统的方法，其特征在于，所述方法包括：

获取原始人脸图像，并基于光学散斑对所述原始人脸图像进行加密，得到加密人脸图像；

将所述加密人脸图像输入已训练的密文图像解密神经网络，得到与所述加密人脸图像对应的解密人脸图像；

将所述解密人脸图像进行识别，得到人脸识别结果。

3. 根据权利要求2所述的基于光学散斑的加密人脸识别系统的方法，其特征在于，所述基于光学散斑对所述原始人脸图像进行加密，得到加密人脸图像包括：

获取激光源发出的光束；

将所述光束依次经过第一透镜、第二透镜的扩束后再照亮空间光调制器；

采用照亮后的所述空间光调制器加载所述原始人脸图像，得到波前调制光束；

将所述波前调制光束依次经过第三透镜、第四透镜的扩束后再经过物镜聚焦得到聚焦光束；

将所述聚焦光束输入散射介质，得到随机光学散斑图案；

将所述随机光学散斑图案作为与所述原始人脸图像对应的加密人脸图像。

4. 根据权利要求3所述的基于光学散斑的加密人脸识别系统的方法，其特征在于，所述密文图像解密神经网络的训练过程包括：

获取训练数据集，其中，所述训练数据集包括明文图像和与所明文图像对应的密文图像；

将所述密文图像输入至第一网络中，通过所述第一网络输出解密预测图像；

根据所述明文图像和所述解密预测图像,得到损失函数;

根据所述损失函数,对所述第一网络进行训练,以得到密文图像解密神经网络。

5. 根据权利要求3所述的基于光学散斑的加密人脸识别系统的方法,其特征在于,所述将所述解密人脸图像进行识别,得到人脸识别结果包括:

将所述解密人脸图像输入至所述人脸识别神经网络,得到待识别人脸图像编码数据;

将所述待识别人脸图像编码数据和所述图像编码数据库中存储的若干人脸图像编码数据进行匹配,得到人脸识别结果。

6. 一种智能终端,其特征在于,包括有存储器,以及一个或者一个以上的程序,其中一个或者一个以上程序存储于存储器中,且经配置以由一个或者一个以上处理器执行所述一个或者一个以上程序包含用于执行如权利要求2-5中任意一项所述的方法。

7. 一种非临时性计算机可读存储介质,其特征在于,当所述存储介质中的指令由电子设备的处理器执行时,使得电子设备能够执行如权利要求2-5中任意一项所述的方法。

一种基于光学散斑的加密人脸识别方法和系统

技术领域

[0001] 本发明涉及加密及解密技术领域,尤其涉及的是一种基于光学散斑的加密人脸识别方法和系统。

背景技术

[0002] 随着人们对于公共安全的需求提高,多数公共场合已经安装视频监控装置以及人脸识别装置;但是这些人脸识别装置如果直接存储人脸照片原始数据,容易导致重要隐私数据泄露,并引发一系列的身份盗用事件,造成社会重大经济损失、危害公共安全;因此,学界、工业界对人脸识别数据的加密存储及解密后识别有迫切需求。

[0003] 目前,工业界已经提出了大量基于软件的加密算法,这些软件加密算法广泛应用于隐私数据保护,例如非对称加密算法、高级加密标准等;这些加密算法利用128位、256位等长度的秘钥对明文数据进行加密,以保护数据安全;然而,随着超级计算机计算能力的提升和量子计算理论的发展,这些加密算法的安全性受到了极大的挑战。

[0004] 随着光计算等相关领域的发展,研究者提出了基于硬件实现的光学加密方法;这些方法不依赖于特定算法,而是基于物理光现象对明文进行加密,以实现高维度的快速加密;此外,光学加密具有高安全性、快速加密、低成本的特点,未来的应用前景广阔。

[0005] 光学加密利用了光的多维度衍射、折射、散射等特性,将明文信息进行高维度调制后进行加密,光学加密前后的明文信息与密文信息不具有相关性,破解难度高;此外,唯一可用于解密的秘钥具有超高维度,因此,现代计算机所具有的计算能力并无法破解此种高维度的加密方法;但是,现有的光学加密方法产生的加密图像高度无序,难以提取光学加密后的密文图像特征,限制了光学加密在物体分类和人脸识别等应用场景的发展应用。

[0006] 因此,现有技术还有待改进和发展。

发明内容

[0007] 本发明要解决的技术问题在于,针对现有技术的上述缺陷,提供一种基于光学散斑的加密人脸识别方法和系统,旨在解决现有技术中基于光学加密人脸识别的方法在光学加密时产生的加密图像高度无序,难以提取光学加密后的密文图像特征,导致限制了光学加密在物体分类和人脸识别等应用场景的发展应用的问题。

[0008] 本发明解决问题所采用的技术方案如下:

[0009] 第一方面,本发明实施例提供一种基于光学散斑的加密人脸识别系统,其中,所述系统包括:

[0010] 人脸图像加密模块,用于基于光学散斑对原始人脸图像进行加密,得到加密人脸图像;

[0011] 人脸图像解密模块,用于将所述加密人脸图像输入已训练的密文图像解密神经网络,得到与所述加密人脸图像对应的解密人脸图像;

[0012] 人脸识别模块,用于将所述解密人脸图像进行识别,得到人脸识别结果。

[0013] 在一种实现方式中,所述人脸图像加密模块包括激光源、空间光调制器、散射介质、相机和透镜;其中,所述激光源用于提供照明;所述空间光调制器用于加载明文图像;所述散射介质用于将所述原始人脸图像变成随机光学散斑图案;所述相机用于记录与所述原始人脸图像对应的随机光学散斑图案;所述透镜包括第一透镜、第二透镜、第三透镜和第四透镜;所述透镜用于对光路中的光束大小进行调整。

[0014] 在一种实现方式中,所述人脸图像解密模块为密文图像解密神经网络,其中,所述密文图像解密神经网络由UNet网络和一层基于复数的全连接层组成。

[0015] 在一种实现方式中,所述人脸识别模块包括图像编码数据库、人脸识别神经网络和匹配模块;其中,所述图像编码数据库用于存储若干人脸图像编码数据;所述人脸识别神经网络用于对人脸图像进行编码;所述匹配模块用于将图像编码数据库中的编码数据和通过所述人脸识别神经网络输出的编码数据进行匹配。

[0016] 第二方面,本发明实施例还提供一种基于光学散斑的加密人脸识别系统的方法,其中,所述方法包括:

[0017] 获取原始人脸图像,并基于光学散斑对所述原始人脸图像进行加密,得到加密人脸图像;

[0018] 将所述加密人脸图像输入已训练的密文图像解密神经网络,得到与所述加密人脸图像对应的解密人脸图像;

[0019] 将所述解密人脸图像进行识别,得到人脸识别结果。

[0020] 在一种实现方式中,所述基于光学散斑对所述原始人脸图像进行加密,得到加密人脸图像包括:

[0021] 获取激光源发出的光束;

[0022] 将所述光束依次经过第一透镜、第二透镜的扩束后再照亮空间光调制器;

[0023] 采用照亮后的所述空间光调制器加载所述原始人脸图像,得到波前调制光束;

[0024] 将所述波前调制光束依次经过第三透镜、第四透镜的扩束后再经过物镜聚焦得到聚焦光束;

[0025] 将所述聚焦光束输入散射介质,得到随机光学散斑图案;

[0026] 将所述随机光学散斑图案作为与所述原始人脸图像对应的加密人脸图像。

[0027] 在一种实现方式中,所述密文图像解密神经网络的训练过程包括:

[0028] 获取训练数据集,其中,所述训练数据集包括明文图像和与所说明文图像对应的密文图像;

[0029] 将所述密文图像输入至第一网络中,通过所述第一网络输出解密预测图像;

[0030] 根据所说明文图像和所述解密预测图像,得到损失函数;

[0031] 根据所述损失函数,对所述第一网络进行训练,以得到密文图像解密神经网络。

[0032] 在一种实现方式中,所述将所述解密人脸图像进行识别,得到人脸识别结果包括:

[0033] 将所述解密人脸图像输入至所述人脸识别神经网络,得到待识别人脸图像编码数据;

[0034] 将所述待识别人脸图像编码数据和所述图像编码数据库中存储的若干人脸图像编码数据进行匹配,得到人脸识别结果。

[0035] 第三方面,本发明实施例还提供一种智能终端,包括有存储器,以及一个或者一个

以上的程序,其中一个或者一个以上程序存储于存储器中,且经配置以由一个或者一个以上处理器执行所述一个或者一个以上程序包含用于执行如上述任意一项所述的基于光学散斑的加密人脸识别系统的方法。

[0036] 第四方面,本发明实施例还提供一种非临时性计算机可读存储介质,当所述存储介质中的指令由电子设备的处理器执行时,使得电子设备能够执行如上述中任意一项所述的基于光学散斑的加密人脸识别系统的方法。

[0037] 本发明的有益效果:本发明实施例系统包括:人脸图像加密模块,用于基于光学散斑对原始人脸图像进行加密,得到加密人脸图像;人脸图像解密模块,用于将所述加密人脸图像输入已训练的密文图像解密神经网络,得到与所述加密人脸图像对应的解密人脸图像;人脸识别模块,用于将所述解密人脸图像进行识别,得到人脸识别结果。可见,本发明实施例中通过人脸图像加密模块基于光学散斑对人脸图像进行加密,加密过程中不涉及复杂的数学计算、仅涉及一套结构简单的光学装置,整个加密过程的速度快、成本低,可以实现高安全性、快速和低成本的图像加密,然后通过人脸图像解密模块中的神经网络对加密人脸图像进行解密,实现高保真度的加密图像解密,解密可靠性高,最后通过人脸识别模块将解密图像应用于人脸识别,从而提高加密人脸识别系统的安全性,保护人脸照片隐私数据。

附图说明

[0038] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明中记载的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

- [0039] 图1为本发明实施例提供的基于光学散斑的加密人脸识别系统流程示意图。
- [0040] 图2为本发明实施例提供的优选实施例的光学加密装置的整体示意图。
- [0041] 图3为本发明实施例提供的优选实施例的神经网络解密的整体示意图。
- [0042] 图4为本发明实施例提供的优选实施例的人脸识别方法的整体示意图。
- [0043] 图5为本发明实施例提供的基于光学散斑的加密人脸识别方法流程示意图。
- [0044] 图6为本发明实施例提供的智能终端的内部结构原理框图。

具体实施方式

[0045] 本发明公开了一种基于光学散斑的加密人脸识别方法和系统,为使本发明的目的、技术方案及效果更加清楚、明确,以下参照附图并举实施例对本发明进一步详细说明。应当理解,此处所描述的具体实施例仅用以解释本发明,并不用于限定本发明。

[0046] 本技术领域技术人员可以理解,除非特意声明,这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是,本发明的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件,但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。应该理解,当我们称元件被“连接”或“耦接”到另一元件时,它可以直接连接或耦接到其他元件,或者也可以存在中间元件。此外,这里使用的“连接”或“耦接”可以包括无线连接或无线耦接。这里使用的措辞“和/或”包括一个或更多个相关联的列出项的全部或任一单元和全部组合。

[0047] 本技术领域技术人员可以理解，除非另外定义，这里使用的所有术语（包括技术术语和科学术语），具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是，诸如通用字典中定义的那些术语，应该被理解为具有与现有技术的上下文中的意义一致的意义，并且除非像这里一样被特定定义，否则不会用理想化或过于正式的含义来解释。

[0048] 由于现有技术中，光学加密过程的物理模型过于复杂，难以使用数学公式建立模型进行解密，因此主要采用基于神经网络的方法对密文进行解密。

[0049] 目前，基于光学加密的方法还处于早期的研究阶段；并且由于光学加密后的图像高度无序，因而难以提取光学加密后的密文图像的特征，并将其推广到物体分类、人脸识别等高级应用场合；这是限制光学加密进一步发展应用的主要原因之一。

[0050] 为了解决现有技术的问题，本实施例提供了一种基于光学散斑的加密人脸识别系统，通过系统中人脸图像加密模块基于光学散斑对人脸图像进行加密，可以提升加密的密钥维度，然后通过人脸图像解密模块中的神经网络对加密人脸图像进行解密，最后通过人脸识别模块将解密图像应用于人脸识别，从而提高加密人脸识别系统的安全性，保护人脸照片隐私数据。本发明实施例的系统包括：人脸图像加密模块，用于基于光学散斑对原始人脸图像进行加密，得到加密人脸图像；人脸图像解密模块，用于将所述加密人脸图像输入已训练的密文图像解密神经网络，得到与所述加密人脸图像对应的解密人脸图像；人脸识别模块，用于将所述解密人脸图像进行识别，得到人脸识别结果。

[0051] 示例性设备

[0052] 如图1中所示，本发明实施例提供一种基于光学散斑的加密人脸识别系统，该系统包括：人脸图像加密模块，用于基于光学散斑对原始人脸图像进行加密，得到加密人脸图像；人脸图像解密模块，用于将所述加密人脸图像输入已训练的密文图像解密神经网络，得到与所述加密人脸图像对应的解密人脸图像；人脸识别模块，用于将所述解密人脸图像进行识别，得到人脸识别结果。

[0053] 具体地，人脸识别已经应用越来越广泛，但是如果人脸识别装置直接存储原始人脸图像，会导致重要隐私数据泄露，并引发一系列的身份盗用，造成社会重大经济损失，危害公共安全。因此，对原始人脸图像进行加密可以解决上述问题，目前基于软件的加密算法也会有安全隐患，因此出现基于硬件实现的光学加密，然而现有技术中光学加密后图像高度无序，难以提取光学加密后的密文图像的特征，故本发明设计了基于光学散斑来加密原始人脸图像，解密前的明文图像，光学散斑包含唯一的高密度密钥，可以提升加密系统的安全性。这样，通过已训练的密文图像解密神经网络就可以提取加密人脸图像中的特征，实现对加密人脸图像的解密，得到解密人脸图像，也即解密后的明文图像，最后将解密人脸图像应用到人脸识别模块中进行人脸识别结果，也即判断两个图像是否属于同一个人。

[0054] 在一种实现方式中，如图2所示，所述人脸图像加密模块包括激光源、空间光调制器、散射介质、相机和透镜；在加密过程中，所述激光源用于对整个光学系统提供照明。所述透镜包括第一透镜、第二透镜、第三透镜和第四透镜；所述透镜用于对光路中的光束大小进行调整，在本实施例中为对光束进行扩束，也即激光源发出的光束依次经过第一透镜和第二透镜的扩束后，光束传入到空间光调制器，并将所述空间光调制器照亮。所述空间光调制器加载明文图像（如原始人脸图像），具体为空间光调制器使用原始人脸图像的亮度信息对

传入的激光光束的波前进行调制；经过波前调制后的激光光束依次经过第三透镜和第三透镜的扩束，再经过物镜聚焦后传入散射介质，所述散射介质用于将所述原始人脸图像变成随机光学散斑图案；所述相机用于将该随机光学散斑图案记录下来，并将所述随机光学散斑图案作为加密后的密文图像，在本实施例中为加密人脸图像。

[0055] 在一种实现方式中，所述人脸图像解密模块为密文图像解密神经网络，该如图3所示，密文图像解密神经网络用于对密文图像进行解密。所述密文图像解密神经网络由U型网络(UNet)网络和一层基于复数的全连接层组成，在本实施例中，密文图像解密神经网络由一个四层结构的标准UNet网络和一层基于复数的全连接层组成，所述密文图像解密神经网络经过大量数据训练后再使用时就可以将密文图像恢复成明文图像，输出后的明文图像与加密前的明文图像之间的相似度很高。在本实施例中所述密文图像解密神经网络可以将加密人脸图像恢复成解密人脸图像，解密人脸图像与原始人脸图像的相似度很高，因此，恢复后的解密人脸图像可以被用于人脸识别等其他高级应用场合。

[0056] 在另一种实现方式中，如图4所示，所述人脸识别模块包括图像编码数据库、人脸识别神经网络和匹配模块；其中，所述图像编码数据库用于存储若干人脸图像编码数据；所述人脸识别神经网络用于对人脸图像进行编码，是一个现有技术中的神经网络，在此不再赘述。所述匹配模块用于将图像编码数据库中的编码数据和通过所述人脸识别神经网络输出的编码数据进行匹配。解密人脸图像经过人脸识别神经网络编码后，通过所述匹配模块将通过所述人脸识别神经网络输出的编码数据与已知的图像编码数据库中的编码数据进行一一匹配，当两个编码数据的距离小于预设的阈值(如0.6或者0.5)时，则判断解密人脸图像和编码数据对应的原始人脸图像属于同一个人，否则，则判断解密人脸图像和编码数据对应的原始人脸图像不是同一个人。

[0057] 示例性方法

[0058] 本实施例提供基于光学散斑的加密人脸识别系统的方法，该方法可以应用于加密及解密的智能终端。具体如图5所示，所述方法包括：

[0059] 步骤S100、获取原始人脸图像，并基于光学散斑对所述原始人脸图像进行加密，得到加密人脸图像；

[0060] 实际中，当系统获取到原始人脸图像，由于人脸图像容易被不法分子盗取，造成社会重大经济损失、危害公共安全。故本发明先对原始人脸图像进行加密，加密过程是基于光学散斑，具有高安全性、快速加密和低成本的特点，最终得到加密人脸图像。相应的，所述基于光学散斑对所述原始人脸图像进行加密，得到加密人脸图像包括如下步骤：获取激光源发出的光束；将所述光束依次经过第一透镜、第二透镜的扩束后再照亮空间光调制器；采用照亮后的所述空间光调制器加载所述原始人脸图像，得到波前调制光束；将所述波前调制光束依次经过第三透镜、第四透镜的扩束后再经过物镜聚焦得到聚焦光束；将所述聚焦光束输入散射介质，得到随机光学散斑图案；将所述随机光学散斑图案作为与所述原始人脸图像对应的加密人脸图像。

[0061] 具体地，在加密过程中，获取激光源发出的光束；激光源发出的光束依次经过第一透镜和第二透镜的扩束后，光束传入到空间光调制器，并将所述空间光调制器照亮。所述空间光调制器加载明文图像(如原始人脸图像)，具体为空间光调制器使用原始人脸图像的亮度信息对传入的激光光束的波前进行调制；经过波前调制后的激光光束依次经过第三透镜

和第三透镜的扩束,再经过物镜聚焦后传入散射介质,得到随机光学散斑图案,散射介质为唯一的高维度秘钥,且散射介质具有唯一性和不可复制性,现代计算机所具有的计算能力无法破解此高维度密钥,因此该高维度密钥可以提升加密系统的安全性;基于光学散斑的加密方法不仅可以对人脸图像进行加密,还可以对其他各种类型的图像进行加密,加密过程中安全性由散射介质的维度决定,且此加密维度可以按需扩展,加密安全性远高于传统加密算法;此外,由于加密过程中不涉及大量计算过程,加密速度远快于基于软件的加密算法。该随机光学散斑图案被所述相机记录下来,并将所述随机光学散斑图案作为加密后的密文图像,也即为加密人脸图像。在本实施例中,将20000张人脸图像一张一张地加载到空间光调制器上,被调制过的激光经过散射介质后形成散斑图案,用相机按照加载人脸图像的顺序记录每一幅人脸图像对应的散斑图案;原始的人脸图像即为明文图像,所对应的散斑图案即为经过光学散斑加密的密文图像。

[0062] 得到加密人脸图像后,就可以执行如图5所示的如下步骤:S200、将所述加密人脸图像输入已训练的密文图像解密神经网络,得到与所述加密人脸图像对应的解密人脸图像;

[0063] 具体地,因为密文图像解密神经网络是训练好的,只要将所述加密人脸图像输入,就能得到与所述加密人脸图像对应的解密人脸图像,由于解密人脸图像与初始人脸图像高度相似,故可以用于后续的人脸识别。

[0064] 在一种实现方式中,所述密文图像解密神经网络的训练过程包括如下步骤:获取训练数据集,其中,所述训练数据集包括明文图像和与所述明文图像对应的密文图像;将所述密文图像输入至第一网络中,通过所述第一网络输出解密预测图像;根据所述明文图像和所述解密预测图像,得到损失函数;根据所述损失函数,对所述第一网络进行训练,以得到密文图像解密神经网络。

[0065] 在本实施例中,将20000个明文-密文对分割成三个数据集,其中19800个明文-密文对为训练数据集,100个明文-密文对为验证数据集,100个明文-密文对为测试数据集;使用训练数据集对解密神经网络进行训练,训练过程中使用训练数据集和验证数据集对神经网络进行评估、使得神经网络能够以高保真度将训练数据集和验证数据集的密文图像(加密人脸图像)恢复成明文图像(原始人脸图像)。在进行神经网络训练时,先将训练数据集中的密文图像(加密人脸图像)输入至第一网络中,通过所述第一网络输出解密预测图像;为了使得解密预测图像最后逼近明文图像(原始人脸图像),根据所述明文图像和所述解密预测图像,得到损失函数;损失函数可以为交叉熵损失函数,可以根据所述交叉熵损失函数对所述第一网络进行训练,将所述交叉熵损失函数在所述第一网络中进行反向传播,并更新所述第一网络中的参数。在计算得到所述损失函数后,判断所述损失函数是否小于或等于预设阈值,若所述损失函数小于或者等于预设阈值,则结束训练;若所述损失函数大于预设阈值,则判断所述第一网络的训练次数是否达到预设次数阈值,若所述第一网络的训练次数未达到预设次数阈值,则根据所述损失函数对所述第一网络参数进行修正,若所述第一网络的训练次数达到预设次数阈值,则结束训练,得到密文图像解密神经网络。预设次数阈值以及预设次数阈值可以根据所述视频分类模型的模型精度来确定,在本实施例中,所述预设次数阈值可以为第一网络的最大训练次数,例如,5000次等。密文图像解密神经网络训练和评估完成后,使用测试数据集对训练后的神经网络进行测试,检验解密神经网络对测

试数据集中的密文图像的恢复效果。

[0066] 得到解密人脸图像后,就可以执行如图5所示的如下步骤:S300、将所述解密人脸图像进行识别,得到人脸识别结果。

[0067] 实际中,采用的是现有技术中的人脸识别系统对所述解密人脸图像进行识别,得到人脸识别结果,也即解密图像和人脸识别系统中存储的人脸图像是否吻合。相应的,所述将所述解密人脸图像进行识别,得到人脸识别结果包括如下步骤:将所述解密人脸图像输入至所述人脸识别神经网络,得到待识别人脸图像编码数据;将所述待识别人脸图像编码数据和所述图像编码数据库中存储的若干人脸图像编码数据进行匹配,得到人脸识别结果。

[0068] 在一种实现方式中,所述图像编码数据库存储有若干人脸图像编码数据;所述人脸识别神经网络可以对人脸图像进行编码,是一个现有技术中的神经网络,在此不再赘述。解密人脸图像经过人脸识别神经网络编码后,通过所述匹配模块将通过所述人脸识别神经网络输出的编码数据与已知的图像编码数据库中的编码数据进行一一匹配,当两个编码数据的距离小于预设的阈值(如0.6或者0.5)时,则人脸识别结果为解密人脸图像和编码数据对应的原始人脸图像是同一个人,否则,则人脸识别结果为解密人脸图像和编码数据对应的原始人脸图像不是同一个人。

[0069] 基于上述实施例,本发明还提供了一种智能终端,其原理框图可以如图6所示。该智能终端包括通过系统总线连接的处理器、存储器、网络接口、显示屏、温度传感器。其中,该智能终端的处理器用于提供计算和控制能力。该智能终端的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统和计算机程序。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该智能终端的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种基于光学散斑的加密人脸识别系统的方法。该智能终端的显示屏可以是液晶显示屏或者电子墨水显示屏,该智能终端的温度传感器是预先在智能终端内部设置,用于检测内部设备的运行温度。

[0070] 本领域技术人员可以理解,图6中的原理图,仅仅是与本发明方案相关的部分结构的框图,并不构成对本发明方案所应用于其上的智能终端的限定,具体的智能终端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。

[0071] 在一个实施例中,提供了一种智能终端,包括有存储器,以及一个或者一个以上的程序,其中一个或者一个以上程序存储于存储器中,且经配置以由一个或者一个以上处理器执行所述一个或者一个以上程序包含用于进行以下操作的指令:

[0072] 获取原始人脸图像,并基于光学散斑对所述原始人脸图像进行加密,得到加密人脸图像;

[0073] 将所述加密人脸图像输入已训练的密文图像解密神经网络,得到与所述加密人脸图像对应的解密人脸图像;

[0074] 将所述解密人脸图像进行识别,得到人脸识别结果。

[0075] 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,本发明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/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限, RAM以多种形式可得, 诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink) DRAM(SLDRAm)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0076] 综上所述, 本发明公开了基于光学散斑的加密人脸识别方法和系统, 所述系统包括:

[0077] 人脸图像加密模块, 用于基于光学散斑对原始人脸图像进行加密, 得到加密人脸图像; 人脸图像解密模块, 用于将所述加密人脸图像输入已训练的密文图像解密神经网络, 得到与所述加密人脸图像对应的解密人脸图像; 人脸识别模块, 用于将所述解密人脸图像进行识别, 得到人脸识别结果。可见, 本发明实施例中通过人脸图像加密模块基于光学散斑对人脸图像进行加密, 加密过程中不涉及复杂的数学计算、仅涉及一套结构简单的光学装置, 整个加密过程的速度快、成本低, 可以实现高安全性、快速和低成本的图像加密, 然后通过人脸图像解密模块中的神经网络对加密人脸图像进行解密, 实现高保真度的加密图像解密, 解密可靠性高, 最后通过人脸识别模块将解密图像应用于人脸识别, 从而提高加密人脸识别系统的安全性, 保护人脸照片隐私数据。

[0078] 基于上述实施例, 本发明公开了一种基于光学散斑的加密人脸识别系统的方法, 应当理解的是, 本发明的应用不限于上述的举例, 对本领域普通技术人员来说, 可以根据上述说明加以改进或变换, 所有这些改进和变换都应属于本发明所附权利要求的保护范围。

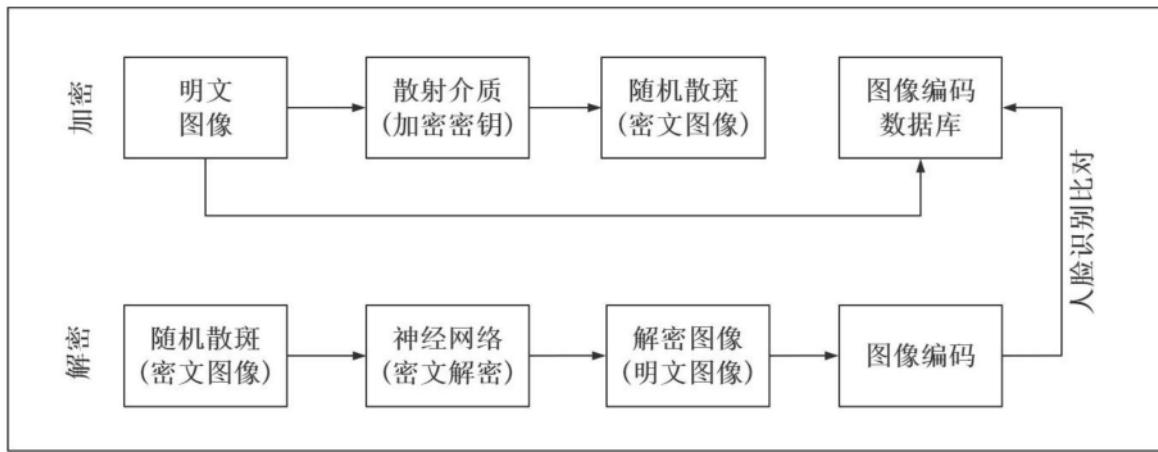


图1

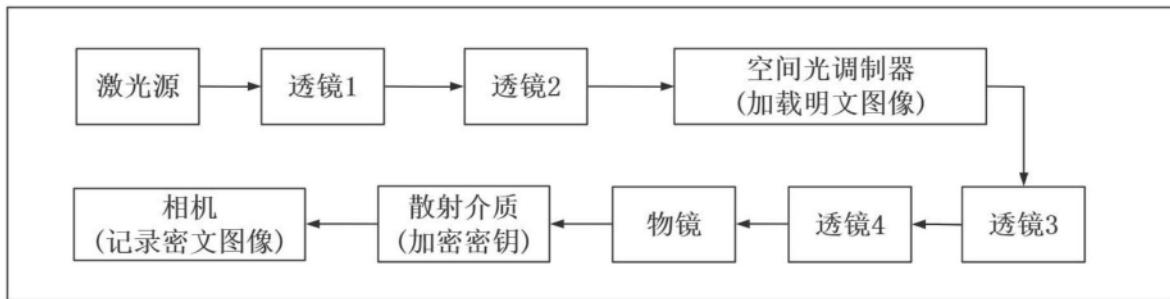


图2

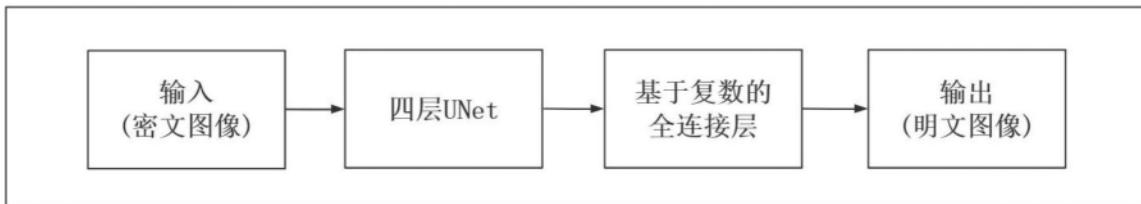


图3

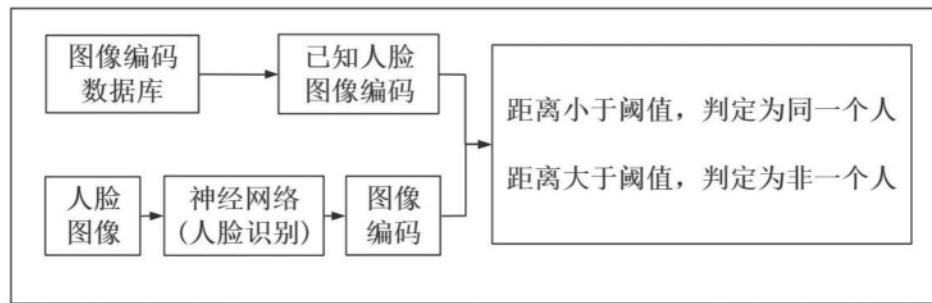


图4

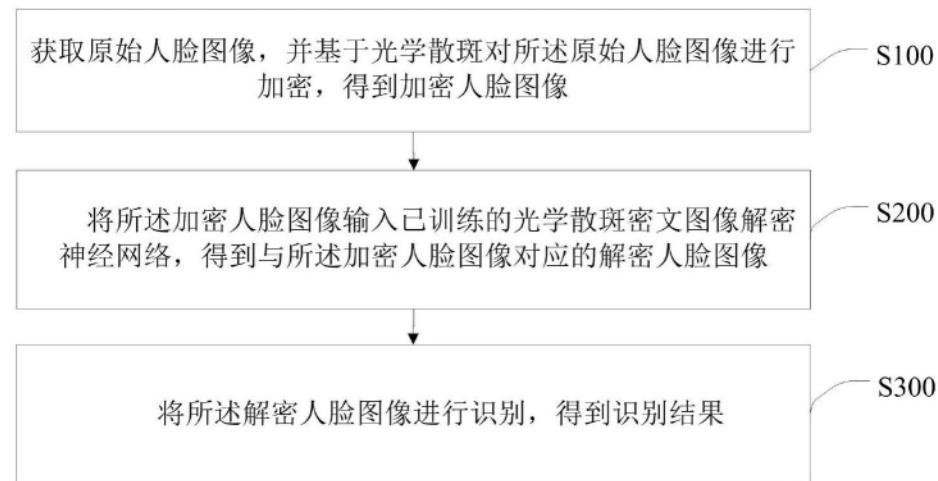


图5

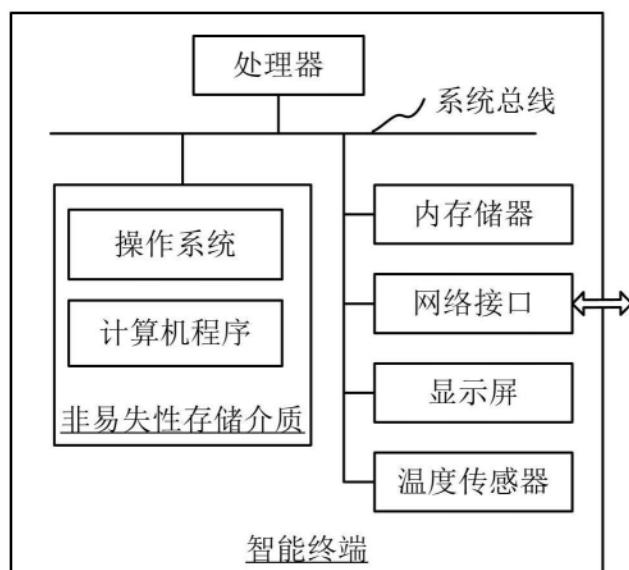


图6